Some Advanced FFmpeg Tricks

Weka: Building ML Models Made Easy

₹120

ISSN-2456-4885

Volume: 11 | Issue: 12 | Pages: 100 | October 2023

OpenSource ForYou

THE COMPLETE MAGAZINE ON OPEN SOURCE

An EFY GROUP Publication

THE POWER OF BLOCKCHAIN



The 'Big Problem' For Blockchain

The Role Of Ethereum In Advancing Open Source Blockchain Technology

The Blockchain And Its Many Uses

Tools For Security Audit And Vulnerability Analysis Of Smart Contracts

Software Freedom Day: Past, Present And Future

An Introduction To Large Language Models

The Community Is Meeting the Industry!



Have you marked the dates on your calendar?

Register Now!

https://opensourceindia.in



www.opensourceforu.com

Wanna Be Your Own Boss?

DO OPEN SOURCE.



Demand for Open Source is sky rocketing. Be it for managing IT infrastructure or development of software--Open Source solutions are what customers are seeking.

All you need to do is develop expertise in an Open Source stack, and then build a team around it!

And, Open Source For You can be your friend and a guide through this journey.

TO READ OUR PRINT EDITION Visit: https://subscribe.efyindia.com

TO READ OUR EZINE EDITION Visit: https://ezine.lfymag.com



WORLD'S LEADING PUBLICATION ON OPEN SOURCE

Looking for marketing solutions to engage with cutting edge techies?
Contact us at growmybiz@efy.in OR call us at +91-9811155335.

India's #1 Event For

R&D and New Product Development

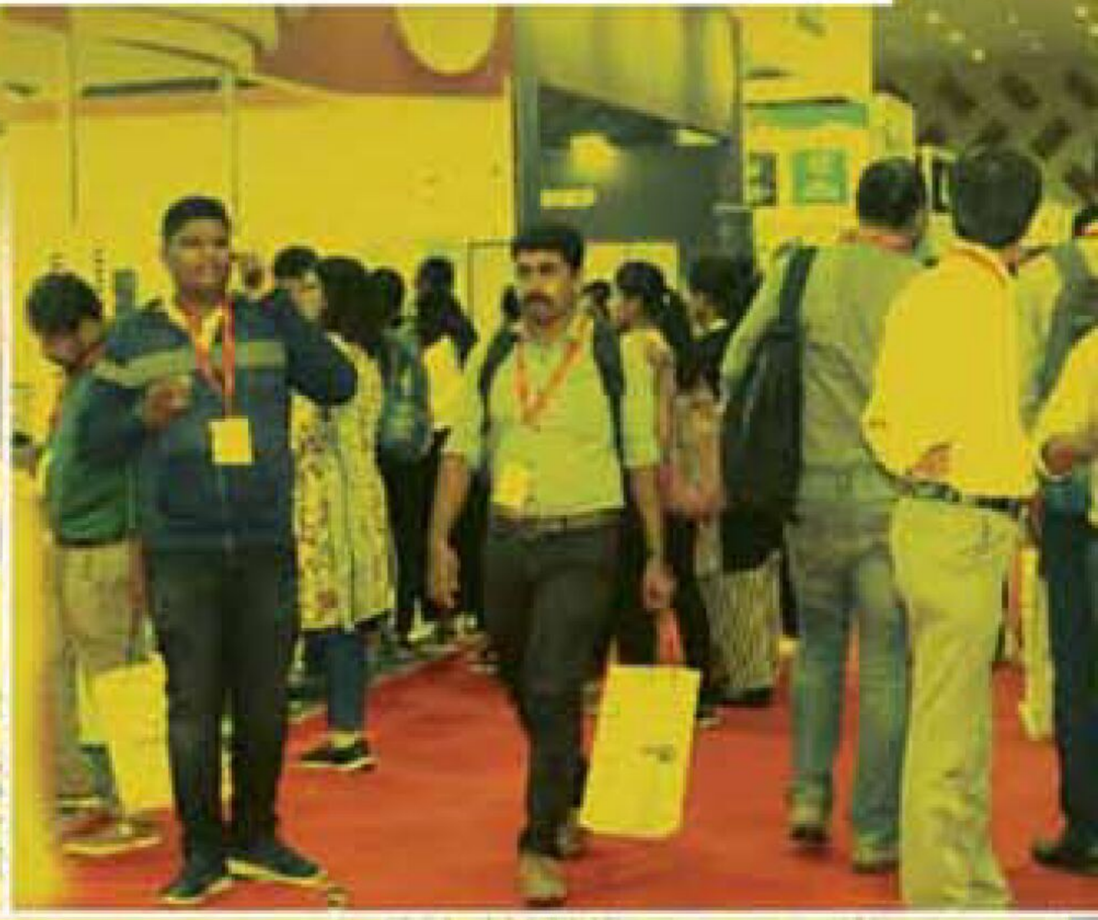
Of Electronics

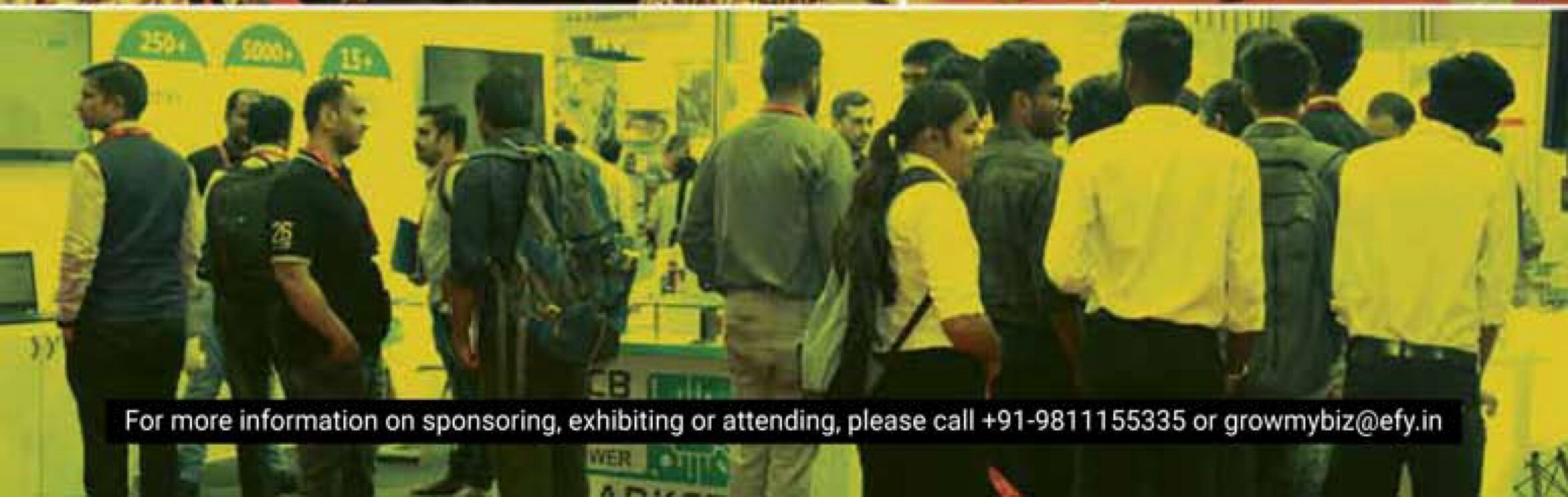
9TH EDITION INDIA ELECTRONICS WEEK 2024

31st Jan - 2nd Feb 2024

KTPO Expo Center |
Whitefield | Bengaluru | India







For more information on sponsoring, exhibiting or attending, please call +91-9811155335 or growmybiz@efy.in

CONTENTS

OCTOBER 2023 | ISSN-2456-4885

FOCUS

28 The ‘Big Problem’ for Blockchain

32 Open Source and Blockchain: Building Trust in a Decentralised World

34 Tools for Security Audit and Vulnerability Analysis of Smart Contracts

60 Blockchain Technology and Generative AI: A Symbiotic Partnership

62 Consortium Blockchain: An Introduction

DEVELOPERS

66 An Introduction to Large Language Models

68 Build Your Own AI Chatbot with OpenAI and Telegram Using Pyrogram in Python

73 The Impact of Deep Learning Models on Visual Data Analysis

ADMIN

89 Do I/O Schedulers Perform Better in Virtual Machines or in Docker Containers?

93 Why Security and Cost go Hand-in-Hand in the Enterprise Cloud

OPEN GURUS

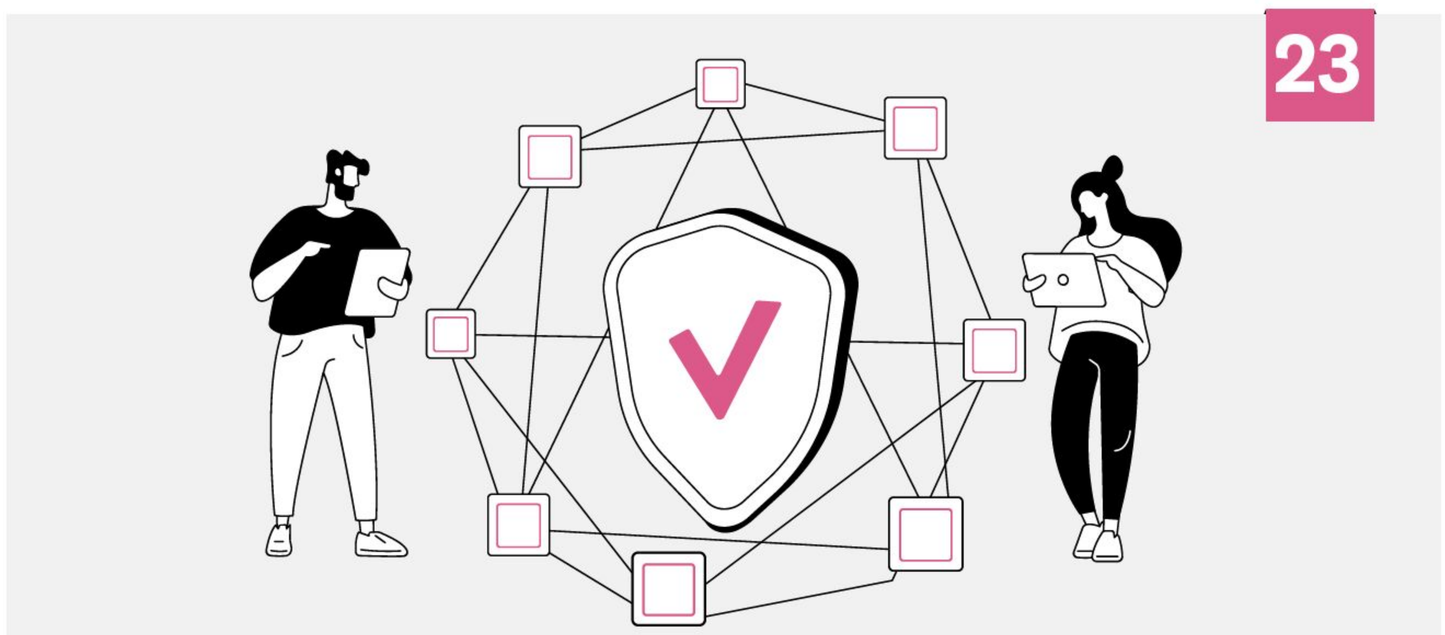
96 Some Advanced FFmpeg Tricks



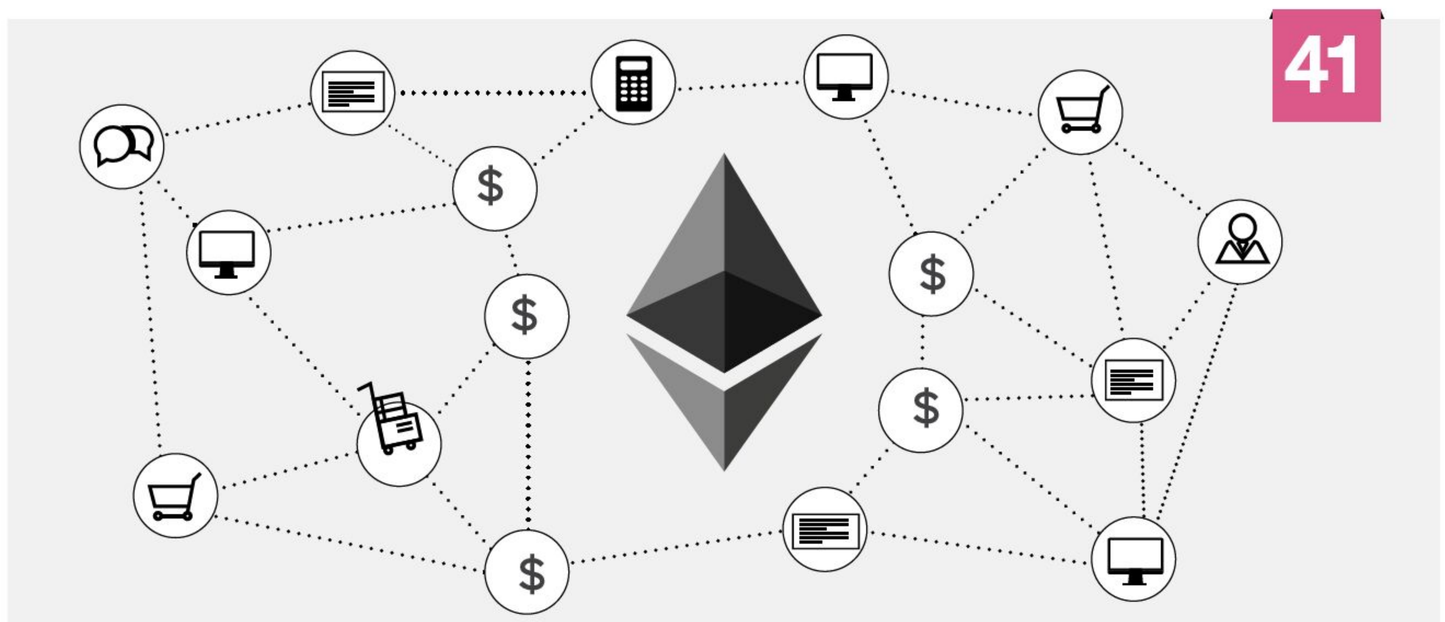
Software Freedom Day: Past, Present and Future



Mastering Enterprise Mobile Security: Safeguarding Your Digital World



Decentralised Applications: Revolutionising the Digital Landscape



The Role of Ethereum in Advancing Open Source Blockchain Technology

REGULAR FEATURES

07 FossBytes

EFYGROUP
YOURS SINCE 1969

Wanna Support Open Source For You?

Subscribe to the Magazine— so that we can keep promoting Open Source.



AMAZING OFFER

Pay for 6 Issues Get 12!

(Buy One Get One Free!)

WORLD'S LEADING PUBLICATION ON OPEN SOURCE

TEAR OUT — **ORDER FORM** — TEAR OUT

Please Tick (✓) Your Choice

☐ **Pay for 12 Issues Get 24 Issues**
and save 50%
(Buy 12 Issues Get 12 Issues Free!)
₹1440

☐ **Pay for 24 Issues Get 48 Issues**
and save 50%
(Buy 24 Issues Get 24 Issue Free!)
₹2880

☐ **Pay for 36 Issues Get 72 Issues**
and save 50%
(Buy 36 Issues Get 36 Issue Free!)
₹4320

To subscribe online, visit
https://tinyurl.com/y5kuv4la
OR
SCAN THIS CODE

Name_____ Organisation_____ Mailing Address_____

_____ City_____

Pin Code_____ State_____ Phone No._____ Email_____

Subscription No. (for existing subscribers only)_____. **I would like to subscribe to the above (✓)marked Open Source For You magazine starting with the next issue.** Please find enclosed a sum of Rs_____ by DD/MO/crossed cheque bearing the No._____ dt._____ in favour of **EFY Enterprises Pvt Ltd,** payable at Delhi. *(Please add Rs 50 on non-metro cheque)*

Please mark one (nearest) relating to your subscription: ☐ Indian Company ☐ MNC ☐ R&D organisation ☐ Engineering institute ☐ College/School ☐ Any other (specify):_____

Send this filled-in form or its photocopy to : **EFY Enterprises Pvt Ltd,** D-87/1 Okhla Industrial Area, Phase 1, New Delhi 110 020 | Ph: **011-40596600** | e-mail: **support@efy.in**

Terms:- # These rates are applicable for new subscribers as well as renewal by existing subscribers. # Can access ezine till your subscription is active # The rates are valid for subscribers within India only. # Please allow 4-6 weeks for processing of your subscription. # The subscription copies will be dispatched through ordinary post only # Subscription Agents will not get agency commission against this scheme # Disputes, if any, are subject to exclusive jurisdiction of competent courts and forums in Delhi/New Delhi only. * Replacement will be made if intimation of damaged / non-receipt of copies is received within 30 days of its publication ** After three months, if you are not satisfied with the magazine, your balance amount will be returned (Not applicable for gift offer)

EDITOR
RAHUL CHOPRA

EDITORIAL, SUBSCRIPTIONS & ADVERTISING
Delhi (HQ)
D-87/1, Okhla Industrial Area, Phase I, New Delhi 110020
Phone: +91-9811155335
E-mail: info@efy.in

MISSING ISSUES
Phone: +91-9811155335
E-mail: support@efy.in

BACK ISSUES
Phone: +91-9811155335
E-mail: support@efy.in

NEWSSTAND DISTRIBUTION
Phone: +91-9811155335
E-mail: efycirc@efy.in

ADVERTISEMENTS
NEW DELHI (HEAD OFFICE)
Phone: +91-9811155335
E-mail: efyenq@efy.in

MUMBAI
E-mail: rmowest@efy.in

BENGALURU
E-mail: rmosouth@efy.in

CHINA
Worldwide Focus Media
E-mail: china@efy.in

GERMANY
pms Plantenberg Media Service GmbH
E-mail: germany@efy.in

JAPAN
Tandem Inc.
E-mail: japan@efy.in

TAIWAN
J.K. Media
E-mail: taiwan@efy.in

UNITED KINGDOM
ASA Media
E-mail: uk@efy.in

UNITED STATES
E & Tech Media
E-mail: usa@efy.in

Printed, published and owned by Ramesh Chopra. Printed at Tara Art Printers Pvt Ltd, A-46,47, Sec-5, Noida, on 28th of the previous month, and published from D-87/1, Okhla Industrial Area, Phase I, New Delhi 110020. Copyright © 2023. All articles in this issue, except for interviews, verbatim quotes, or unless otherwise explicitly mentioned, will be released under Creative Commons Attribution-NonCommercial 3.0 Unported License a month after the date of publication. Refer to http://creativecommons.org/licenses/by-nc/3.0/ for a copy of the licence. Although every effort is made to ensure accuracy, no responsibility whatsoever is taken for any loss due to publishing errors. Articles that cannot be used are returned to the authors if accompanied by a self-addressed and sufficiently stamped envelope. But no responsibility is taken for any loss or delay in returning the material. Disputes, if any, will be settled in a New Delhi court only.

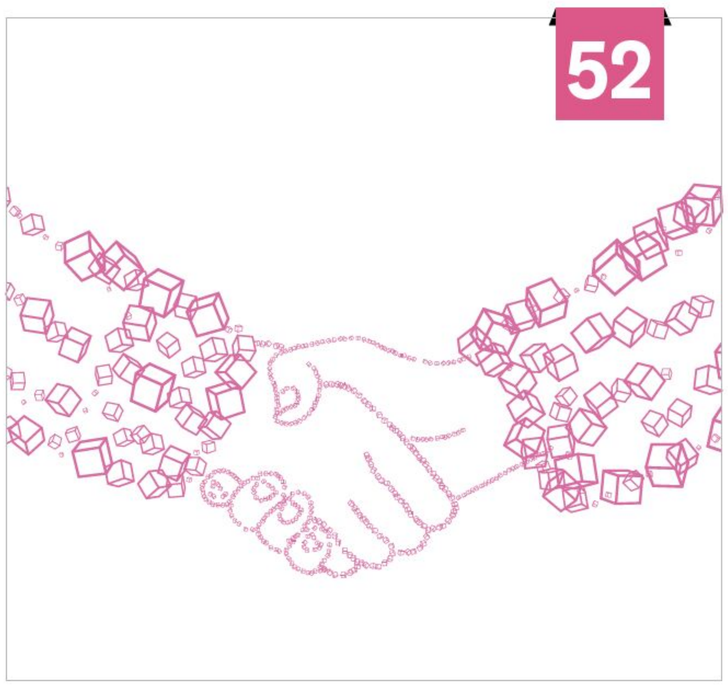
SUBSCRIPTION RATES			
Year	**Newstand Price (₹)**	**You Pay (₹)**	**Overseas**
Five	7200	4320	—
Three	4320	3030	—
One	1440	1150	US$ 120

Kindly add ₹ 50/- for outside Delhi cheques.
Please send payments only in favour of EFY Enterprises Pvt Ltd.
Non-receipt of copies may be reported to **support@efy.in**—do mention your subscription number.

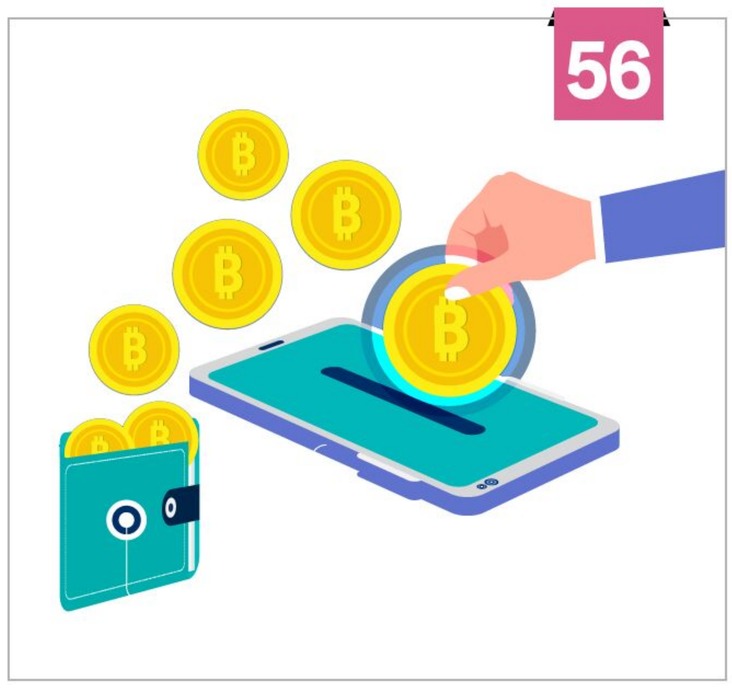
CONTENTS



The Blockchain and its Many Uses



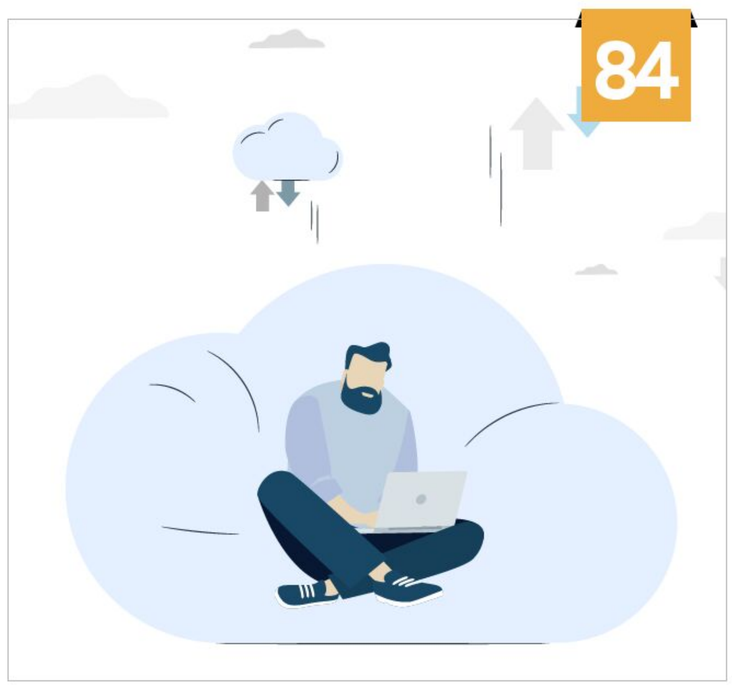
Selecting the Right Blockchain Technology



Cryptocurrency Wallets: Implementing MetaMask for Blockchain Transactions

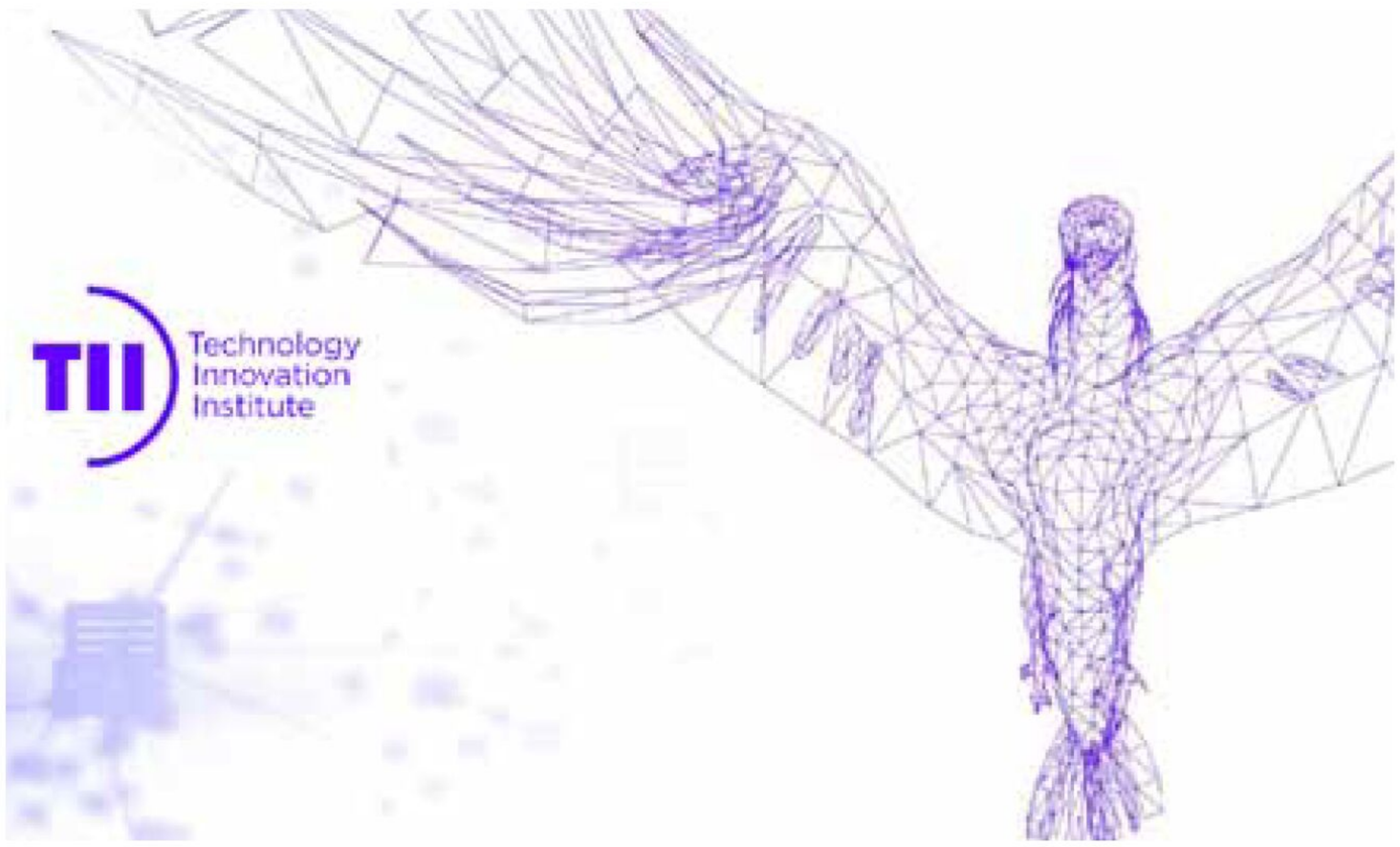


Weka: Building ML Models Made Easy



Migrating to the Cloud? Tick Off this Checklist

Falcon 180B: TII's new open large language model



The Technology Innovation Institute (TII) has unveiled Falcon 180B, an open source large language model that is making waves in the AI community. The new model boasts of a jaw-dropping 180 billion parameters and is trained on 3.5 trillion tokens. It currently reigns supreme on the Hugging Face leaderboard for pre-trained open large language models, and caters to both research and commercial use.

Falcon 180B stands shoulder to shoulder with giants like OpenAI's GPT-4 and Google's PaLM-2, despite being half their size. TII's commitment to high-quality training data shines through its meticulous approach.

This 360GB model is distributed with an Apache 2.0 license. It also has a chat version, is completely free and state-of-the art.

A key strength is that it can handle diverse language tasks, including reasoning, coding, proficiency assessments, and knowledge testing. This is because it's trained on a rich and varied data set that includes web data, conversations, technical papers, and even a fraction of code. Hence, its performance in these tasks matches and often surpasses closed-source competitors like Meta's LLaMA 2.

This open-access model with 180 billion parameters empowers researchers and developers to explore new horizons in natural language processing, and opens the door to innovation across various domains, including healthcare, finance, education, and more.

In short, Falcon 180B's success underscores the value of open source initiatives in AI.

Quetzal-1 satellite project releases open source repository

The team behind the Quetzal-1 satellite project, initially launched in 2020 by students from Universidad Del Valle De Guatemala (UVG), has chosen to release an extensive open source repository, sharing its valuable insights and experience.

Quetzal-1, a CubeSat engineered by UVG students, achieved an impressive 211 days in orbit. Its mission objectives included gathering telemetry data and capturing black-and-white images of Earth. However, initial image quality suffered due to exposure issues.

EDB launches tool for easy Postgres cluster management

EnterpriseDB (EDB), a leader in enhancing Postgres for enterprise use, has unveiled its Trusted Postgres Architect (TPA) as an open source solution for PostgreSQL users. TPA simplifies the setup and management of high availability (HA) Postgres clusters, offering time-saving benefits and reducing the risk of errors.

Historically, HA cluster management has been complex, with potential impacts on performance and data accuracy. EDB aims to address this challenge and make HA clusters more accessible to organisations.

TPA offers a user-friendly structure, enabling enterprises to create and manage HA architectures effortlessly. This facilitates experimentation with cluster setups while maintaining optimal performance and reliability.

It features concise, declarative syntax, enabling users to experiment with trusted architectures for backups, replication, and protection against replication issues.

Combined with EDB Postgres Distributed's Always On architecture, TPA minimises downtime for active-active use cases. EDB backs TPA with its extensive Postgres expertise.

Jozef de Vries, chief product engineering officer of EDB, stated: "TPA embodies EDB's commitment to customer success and supporting the wider Postgres community. It reduces the chance of errors and saves time when deploying production database clusters."

EnterpriseDB's TPA allows organisations to confidently deploy and manage robust database clusters, enhancing operational resiliency and reducing errors in mission-critical applications.

CISA lays out its open source software security roadmap

In a bid to fortify cybersecurity efforts, the US federal Cybersecurity & Infrastructure Security Agency (CISA) has unveiled an intricate roadmap dedicated to the protection of open source software (OSS). The move comes as part of a broader initiative by the Biden administration, which has been fervently advocating for enhanced security measures within the software supply chain.

"CISA recognises the immense benefits of open source software, which enables software developers to work at an accelerated pace and fosters significant innovation and collaboration. With these benefits in mind, this roadmap lays out how CISA will enable the secure usage and development of OSS, both within and outside the federal government," stated CISA in its official document outlining the roadmap.

Within the roadmap, CISA outlines four key priorities -- establishing the agency's role in supporting open source security, enhancing visibility into the utilisation and associated risks of open source, minimising risks to the federal government, and strengthening the overall open source ecosystem.

Dan Lorenc, co-founder and CEO of Chainguard, a supply chain security company, commended CISA for effectively identifying and prioritising the challenges within the realm of open source security. However, he maintained a degree of scepticism about the practical implementation of this strategy.

Lorenc suggested that the government should consider investing in open source projects to support their efforts more substantially. While the roadmap does not presently address this aspect, the government could play a vital role in funding initiatives related to memory safety, vulnerability remediation, and SBOM (Software Bill of Materials) tooling.

One of the mission's primary challenges was a hung I2C bus, leading to battery depletion. An attempt to rectify the situation through a system reset ultimately led to the satellite's failure, attributed to the complete failure of a Lithium-ion battery cell in a low charge state.



The Quetzal-1 team's decision to open source the project is a commendable effort to share its accumulated knowledge. The available resources encompass design documents, satellite and ground station software, as well as the complete telemetry data set. This release serves as a valuable resource for aspiring CubeSat designers, offering lessons learned from Quetzal-1's mission.

Despite the difficulties encountered, Quetzal-1 marked significant achievements, including capturing Central America's first-ever image of Earth from space and establishing radio contact with Earth from orbit. The team's ambitions now extend to Quetzal-2, promising further advancements in CubeSat missions.

Godot Engine introduces Godot Development Fund

The team behind the open source Godot Engine has unveiled the Godot Development Fund—a significant move in securing ongoing financial support for the acclaimed game development platform. This initiative provides a direct channel for anyone to contribute to the engine's growth and development.

At present, the Godot Development Fund sees a monthly influx of €25,591, while Patreon supporters contribute £9,587 each month. The long-term goal is to shift towards their direct funding platform, aiming for cost-effectiveness and the maximisation of funds funnelled directly into Godot's development.

By reducing dependence on large, one-time corporate grants and embracing recurring user-funded contributions and company sponsorships, Godot aims to empower its community while preserving its open source principles. The team states, "This financial independence empowers us to prioritise the needs and interests of our community and the open source principles at the core of our projects. Your help ensures that we can create our journey, uphold our core values, and evolve the engine in ways that benefit our users."

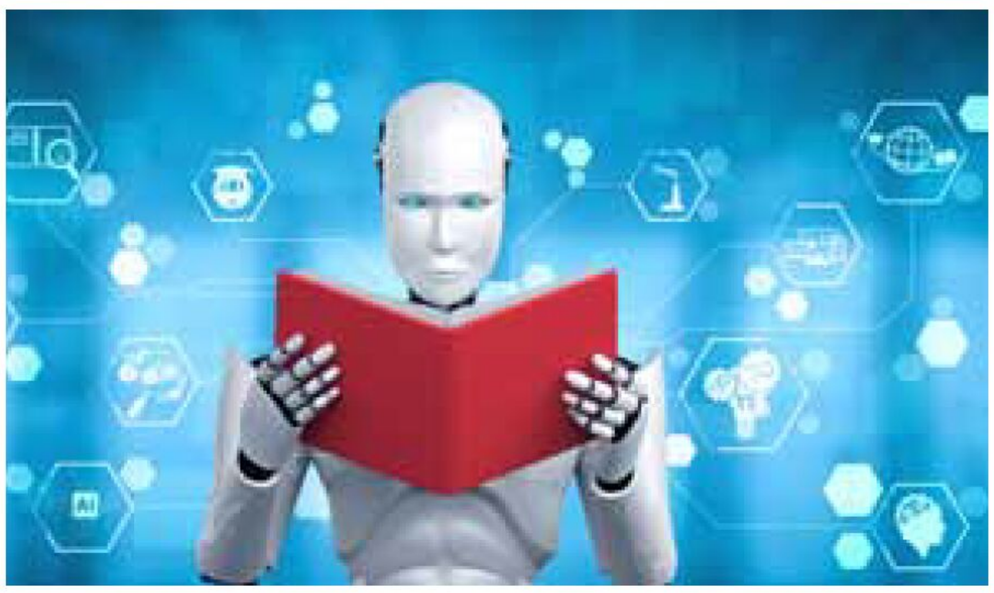


The Godot Development Fund provides a clear path for supporters to directly influence the engine's development while adhering to open source software principles.

In the realm of open source game development, the Godot Engine continues to lead through innovation and community-driven progress. The Godot Development Fund reinforces Godot's position as a pioneering figure in the open source gaming landscape, where community voices guide the engine's evolution.

Accubits' GenZ 70B LLM achieves top global ranking

Accubits Technologies, headquartered in Thiruvananthapuram, India, has taken a giant stride in the world of artificial intelligence (AI) by open sourcing its GenZ 70B large language model (LLM). This collaborative effort with Bud Ecosystem, another Accubits company, has resulted in GenZ 70B achieving the remarkable status of being the top-ranking instruction-tuned LLM on HuggingFace's global leaderboard. Additionally, it stands at a commendable sixth place among open LLMs in all categories.



This 70-billion-parameter fine-tuned LLM represents a significant milestone in the AI landscape. Notably, it is positioned as the largest LLM model in the OpenAI GPT series, making it a key player in the evolving field of generative AI.

Aharsh MS, chief marketing officer at Accubits Technologies, commented on the achievement, emphasising the local significance of GenZ 70B's global recognition. He stated, "An LLM model from India ranking top on a global scale is significant and can be an inspiration for the local developer community."

GenZ 70B is not just a run-of-the-mill language model; it boasts an auto-regressive design with an optimised transformer architecture. To achieve its superior performance, it underwent fine-tuning using the supervised fine-tuning (SFT) method, incorporating data sets from OpenAssistant's instruction fine-tuning and Thought Source's Chain of Thought (CoT) approach. This rigorous fine-tuning has endowed GenZ 70B with enhanced skills and capabilities beyond those of a pre-trained model.

In terms of performance, GenZ 70B scored 7.34 on the MT-Bench benchmark, coming close to the performance of GPT 3.5, despite being 2.5 times smaller. This efficiency is particularly advantageous for real-world commercial applications, where smaller models are often more cost-effective and easier to work with.

Ruby on Rails creator criticises 'open source hooliganism'

Ruby on Rails creator, David Heinemeier Hansson, has expressed his concerns regarding what he calls 'open source hooliganism'. This critique arises from a recent incident involving the TypeScript community's reaction to a decision made by the Turbo team.

Hansson, well-respected in the open source realm, acknowledged the passion displayed by developers for their preferred programming languages and tools. However, he cautioned against crossing the line between passionate advocacy and dogmatic crusading.

The incident in question centres on Turbo's choice to remove TypeScript from their project. While legitimate concerns were raised, most of the debate was dominated by what Hansson termed 'open source hooligans' — individuals with no direct stake in Turbo but fervently defending TypeScript and attacking dissenting voices.

Hansson detailed this situation, citing numerous pull requests requesting TypeScript's reinstatement into Turbo and even a demand for his removal from the

LinkedIn's 'iris-message-processor' boosts escalation management

LinkedIn has unveiled its 'iris-message-processor', an open source project set to improve its Iris escalation management system's performance and reliability. This development offers faster processing speeds—around 4.6 times faster under average loads and an impressive 86.6 times faster under high loads compared to its predecessor.

The 'iris-message-processor' replaces the previous iris-sender subprocess with a fully distributed system, enabling more concurrent processing and direct message sending to vendors. It reduces reliance on the database, no longer using it as a message queue.

Notable improvements include the system's ability to handle large escalations, processing 6000 escalations in under 10 seconds, a significant leap from the previous 30-minute processing time. Even with 50% of nodes dropping simultaneously, it rebalances the cluster in under 30 seconds and processes active escalations in less than three seconds.

This performance boost is achieved by splitting Iris escalations into buckets, assigned dynamically to different nodes within the iris-message-processor cluster. The system's code is written in Go, designed to be efficient and scalable while reducing strain on the database.

LinkedIn has successfully used the iris-message-processor for a year with no outages, consistently surpassing SLOs (service level objectives). It offers a drop-in replacement for the iris-sender, retaining the existing Iris API while delivering substantial performance improvements.

The company has made the iris-message-processor an open source project, making it accessible to the wider community. It operates seamlessly in external environments, potentially replacing commercial incident management systems.

Howso Engine: Doing away with black box AI libraries

Howso, formerly known as Diveplane, has unveiled its open source AI engine, aiming to provide transparency and explainability in a field dominated by black-box AI libraries. The Howso Engine, built on instance-based learning (IBL), promises a fully auditable and accountable approach to AI decision-making.

Co-founder and chief executive, Mike Capps, and co-founder and chief technology officer, Chris Hazard, spoke with *SiliconANGL*E about their mission to reshape AI's role in people's lives. They highlighted the risks of relying on opaque black-box AI systems, where critical decisions impacting individuals' lives lack transparency.

"Chris and I started this company entirely like how do we kill the black box, which is kind of a negative statement," said Capps. "But you know, that approach of 'It's being used improperly,' and decisions are where people's lives are in the balance, whether it's parole, or college or cars, you name it."

The Howso Engine's foundation in instance-based learning sets it apart from traditional neural networks, offering complete explainability. Unlike neural networks, IBL avoids making assumptions about data, making its outcomes and decision processes comprehensible and traceable.

Currently, the Howso Engine focuses on statistical models and structured data, including time series and graph data. However, the company is actively working to expand its capabilities to include text-based data.

While Howso already collaborates with notable organisations like MasterCard Inc. and Duke University Health System to promote transparent AI usage, the decision to open source the engine signals a significant shift in its approach.

project. He described such behaviour as "unhinged open-source hooliganism" and expressed disappointment in some TypeScript community members' reactions.

Drawing parallels with past tech debates, Hansson stressed that defacing open-source repositories and engaging in slanderous behaviour is always unacceptable.

Hansson called on those who care about TypeScript to reflect on the incident, urging enthusiasts to find more constructive ways to express their enthusiasm without resorting to personal attacks or project defacement.

His call for more respectful and constructive discussions serves as a reminder of the importance of civility in open source software development.

Deci releases three generative AI foundation models

Deci, the Israeli deep learning company, has unleashed a trio of generative AI foundation models. Named DeciDiffusion, DeciLM 6B, and DeciCoder, these models have set new records in terms of performance, far outstripping Meta's acclaimed LLaMA and Stable Diffusion algorithms. The Israeli tech firm's open source approach has also shaken up the world of generative AI.

DeciLM 6B, boasting an impressive 5.7 billion parameters, has redefined inference speed, outpacing Meta's LLaMA 2 7B by a staggering 15 times. DeciCoder is a 1 billion parameter code generation model that delivers remarkable inference speed and also maintains or exceeds accuracy standards.

These groundbreaking models owe their success to Deci's proprietary Neural Architecture Search (AutoNAC) technology. Alongside the foundation models, Deci has introduced Infery LLM, an inference software development kit (SDK). This SDK empowers developers to achieve a significant performance boost on existing large language models (LLMs) while preserving the desired level of accuracy.



These developments also have significant cost implications. AI researchers can now reduce their inference compute costs by up to 80% by harnessing Deci's open-source models and Infery LLM. This cost-efficiency extends to the use of widely available GPUs like the NVIDIA A10, making them accessible to a broader range of developers and researchers.

Prof. Ran El Yaniv, chief scientist and co-founder of Deci, highlighted the significance of their solutions, stating, "With Deci's solutions, companies receive both enterprise-grade quality and control, as well as the flexibility to customise models and the inference process according to their precise requirements."

F5 boosts OpenTelemetry project with code contribution

F5, a leading multi-cloud application services and security company, has announced a ground-breaking collaboration with the Cloud Native Computing Foundation's OpenTelemetry project, aiming to revolutionise the world of telemetry data. In a partnership with ServiceNow, F5 has contributed approximately 40,000 lines of code to double the compressibility of the OpenTelemetry Protocol, a move set to reduce telemetry data costs dramatically.

OpenTelemetry, an open source framework, provides a standardised collection of tools for instrumenting, generating, capturing, and exporting telemetry data, including metrics, logs, and traces. This technology has become essential for IT teams to better analyse the performance and behaviour of their solutions. F5's latest

contribution promises to cut costs by half when exporting data from data centres, clouds, and edge locations to a telemetry platform, a significant leap forward in making telemetry more cost-effective.

Laurent Quérel, project lead and distinguished engineer at F5, emphasised the importance of this advancement, stating, "Modern networking solutions, applications, and users generate unfathomably large volumes of data in the course of everyday operations, making compression rates essential to bringing the benefits of comprehensive telemetry to more organisations in a cost-effective manner."

One of the primary benefits of this innovation is the reduction of egress costs related to telemetry traffic by 50%. Organisations that export telemetry data from public clouds to a telemetry aggregation system using this new OpenTelemetry Protocol refinement can expect substantial cost savings.

F5 has also initiated a partnership with ServiceNow Cloud Observability to introduce the OpenTelemetry Arrow Project and reference implementation guidance. This project leverages Apache Arrow, an open source technology used to provide standardised representations of data, to enhance telemetry capabilities further.

Biden administration takes action to bolster open source software security

In a move to bolster cybersecurity defences and prevent future vulnerabilities in open source software, the White House has called for stronger security measures. A two-day summit, held in September this year, convened technology companies, banks, and industry groups. It underscored the Biden administration's commitment to enhancing security standards in the realm of open source software development.



Anne Neuberger, deputy national security adviser for cyber and emerging technology, emphasised the administration's focus on expanding the use of software bill of materials (SBOMs) among companies. SBOMs provide detailed lists of components within a product or program, aiding in vulnerability assessment and remediation.

The summit, held in Washington, D.C., followed a similar meeting at the White House in January 2022, prompted by the disclosure of a critical vulnerability in Log4j, a widely used open source program tracking network activity. The severity of the Log4j vulnerability prompted immediate action over the holiday season to patch the flaw, leaving cybersecurity experts deeply concerned.

Progress has been made since the last summit, including the development of digital certificates for software by the Open Source Security Foundation. These certificates now cover over 17,000 projects, significantly reducing the risk of malicious additions like ransomware and network backdoors infiltrating open source programs.

Omkhar Arasaratnam, general manager of OpenSSF, which hosted the summit, noted, "What we've seen from both the [strategy], as well as the CISA open source roadmap, is that the government is not just declaring outward, 'thou shalt', but it's also taking its own direction and saying in the federal government, 'we shall'."

Microsoft integrates Python's strength with Excel's versatility

Microsoft has announced the public preview of Microsoft Excel's newest feature: the integration of Python directly within Excel. Available to members of the Microsoft 365 Insiders program through Excel for Windows' Beta Channel, this enhancement is set to revolutionise how data professionals interact with Excel.

The integration of Python into Excel presents a transformative approach to data analytics. With the introduction of the PY function, users can now directly input Python code into Excel. This enhances Excel's capabilities and allows users to delve deeper into advanced data visualisations, machine learning, and data cleaning by leveraging Python's extensive libraries. The backing of Anaconda, a prominent enterprise Python repository, further amplifies this integration. As Python in Excel utilises the Anaconda Distribution in Azure, users are provided access to many Python libraries, a move celebrated by Anaconda's CEO, Peter Wang, as a game-changer for Excel users globally.

Prioritising security, all Python operations within Excel are executed on the secure Microsoft Cloud, with the code running in Azure Container Instances, ensuring the utmost user privacy. Collaboration has also been enhanced; teams can share and work on Python-integrated Excel workbooks effortlessly without requiring additional tools.

This initiative, a product of collaboration across various Microsoft teams, symbolises Microsoft's unwavering commitment to the Python community.

For more news, visit *www.opensourceforu.com*

Software Freedom Day: Past, Present and Future

Every year, Software Freedom Day (SFD) celebrates free software across the world. The aim is to increase awareness of free software and its virtues, and encourage its use. This year, SFD was celebrated on September 16. ***Frederick Noronha*** caught up with ***Jurgen Gaeremyn,*** member of the Digital Freedom Foundation (the charity behind Software Freedom Day), to ask some pertinent questions about the history of the event, and its evolution over the years.



Jurgen Gaeremyn,
member of the Digital Freedom Foundation

Jurgen Gaeremyn, member of the Digital Freedom Foundation, wrote in to say: “In June of this year, I offered to help launch Software Freedom Day (SFD) globally. I found your name when searching through the first years of Software Freedom Day, and your account was the oldest one (apart from the founders) I could find in my list. Back in 2005, you were writing for BytesForAll.”

Jurgen says that the SFD team and its supporters in different pockets of the globe are celebrating the 20th edition of Software Freedom Day this year. “Thanks for being one of the very first supporters of SFD, and two decades later still standing for open source software, open data and open culture!”

Seizing the opportunity, I sent across some queries. Here is an excerpt of the exchange.

FN: How has SFD grown or changed over the years (since I last knew it)?

JG: Actually, SFD started back in the time when every self-respecting computer magazine offered a CD with some freebies on it. Back then Matt Oquist decided that burning a CD with actual free software (contrary to the freebies or trial versions on those other CDs) could add much value. He teamed up with Henrik Omma and Phil Harper and they decided to promote this OpenCD project all over the world. Things moved quickly from there.

Software Freedom Day actually reached its peak in 2008, when it was celebrated in at least 563 registered locations all over the world.

In 2010, Frederic Muller took over the initiative and widened the project, reflecting emerging changes. Broadband internet connections were becoming commonplace, and focal points were added — hardware freedom (think of the first Arduino boards that came out around 2011), document freedom (and open standards), and education that was also being impacted more and more through software platforms.

On May 27, 2019, a tragic accident took the life of Patrick Sinz, one of the board members at that moment. This was a heavy blow for the other board members, who were a close team of friends. Then came the global pandemic and organising events in 2020 and 2021 was nearly impossible. Even last year, there clearly still was a lot of reluctance to organise big events.

So now, in 2023, the existing board decided to hand over the project to a new team of volunteers. We started the launch of the 2023 edition of Software Freedom Day in June this year.

For the coming years, we’ll be looking at offering a more centralised and functional online platform where communities can share their content for Software Freedom Day. We’ll also be reaching out to sponsors who will offer tools empowering teams to organise their own events. Combining physical events with online access to presentations and workshops might be the way to go.

Oh and don’t get me started about AI and how open source will be important there too, or we’re off for another hour or two...

FN: How have the celebrations for this year shaped up?

JG: Where the first era was mainly about handing out swag like physical CDs and stickers, today it’s more about building the community and offering online tools that are privacy-respecting.

For example, what are the trade-offs for putting all your documents, photos and personal mails in corporate owned vaults? Are there options to have your private cloud? Explaining how offline tools like LibreOffice on your computer don’t need an internet connection, or showing how to stream not only to the major platforms but also to decentralised content providers might become essential skills.

The Muse Group, for example, has a nice approach to music notation. They have an open source application (Musescore) that is fully featured, and is free to download and modify. To make it commercially viable, they also have an online platform MuseScore.com, where they offer sheet music for download and online music courses. They are actually sponsoring Software Freedom Day this year, and the team writing the best Software Freedom song will be awarded a year of access to this service.

We have connected with some other sponsors too, to send out prizes to SFD teams who excel in a specific field.

FN: What are the challenges the organisers were faced with this year? Can the community help?

JG: Because we were a little late to the game, there wasn’t a lot of build-up to this event. But we always need help from the open source community to make some noise about it, and also start up events locally.

Even if you don’t arrange big events, you could meet up with a class group in the local library to showcase your favourite open source drawing tool. Or maybe there’s a hackerspace in your area that would like to teach how to program home automation using open source tools. Even if you’re on your own, prepare a recording or live stream that you put out. Plenty of ideas — it’s just a matter of finding a few friends and starting something.

There are other small things that can be done too:

- Follow us on social media (we’re on Mastodon, Facebook, Twitter and occasionally also on other platforms) and share.
- Put our interactive banner on your website.
- If you’re a company using or producing open source software, reach out to us at *info@digitalfreedomfoundation.org* if you’d like to sponsor a team (or all teams) in upcoming editions of Software Freedom Day with your tool.

FN: One or two inspiring stories from the past 2-3 years?

JG: That's a tough one... the last few years were pretty rough with Covid. But during these years, I was organising Software Freedom Day in our local hackerspace.

In 2021, I was very inspired by the people from OpenStreetMap, and how they managed to mobilise a worldwide community to create maps that are freely available. We had the lead developer of FreeCAD who came to give an advanced talk on scripting in FreeCAD. He's a professional architect creating all his designs in FreeCAD. Just before that, one of our members gave an introduction on how to use that same program for 3D printing. I was touched by the versatility of FOSS and how different people use it in very different ways.

Last year there was an interesting talk about IoT, and how you could examine an existing device and intercept the traffic to go to your own server instead of to some cloud service.

FN: What is SFD's ultimate goal, and has it evolved over the years, considering that the focus on 'freedom' seems to have somewhat waned over time?

JG: Software freedom is, and has always been, a mindset — it's about believing in the importance of the four freedoms: the right to freely use software, to study it, to share it, and to alter it to your own needs.

While these four freedoms have remained the same, the reasons and accents have shifted. In the beginning of the millennium, it was all about having access to the tools. There were the haves and the have nots. I still remember walking in a Hong Kong market square, where they sold CDs with all the software you could imagine for a few HK$. Obviously illegal, but that was hardly relevant there at that time. It was all about getting equal opportunity.

Nowadays, more and more software come as a (cloud) service — some are free, some pretty expensive. The IoT connects everything to the internet — from doorbells to thermometers, and even light bulbs. The four freedoms are now to be seen in conjunction with our right to privacy and security.

With the recent rise of AI in commercial applications, it will become equally important to have transparency of data sets, weightings, and algorithms if we want to ensure a fairly biased AI. It is also high time to think about decentralisation, prevention of vendor lock-in, open standards, transparency and the freedom to modify into these systems.

FN: What has been the response of India in particular and South Asia in general to SFD?

JG: In Southeast Asia, events have been organised in Kathmandu and Phnom Penh.

It is surprising that the booming country of India is still missing though... Maybe your city can make the difference?

Note: You can connect with Jurgen Gaeremyn on +32496459541 through WhatsApp or Signal, or email him at *jurgen@digitalfreedomfoundation.org*.

END

By: Frederick Noronha

The author is a Goa-based freelance journalist, who has been tracking FOSS (free and open source software), Creative Commons and the Wikipedia issues closely and intensely for a long time.

OSFY Magazine Attractions During 2023-24

Month	Theme
March 2023	Security, Network Management and Monitoring
April 2023	Open Source Programming (Languages and tools)
May 2023	Cloud Special: Everything from management to implementation
June 2023	AI, Deep learning and Machine Learning
July 2023	Database management and Optimisation
August 2023	Mobile/Web App Development, Optimisation and Security
September 2023	DevOps Special
October 2023	Blockchain and Open Source
November 2023	Open Source and IoT and Edge
December 2023	All About Data Management
January 2024	Containers and Managing Containers
February 2024	Open Source on Windows and Best in the world of Open Source (Tools and Services)

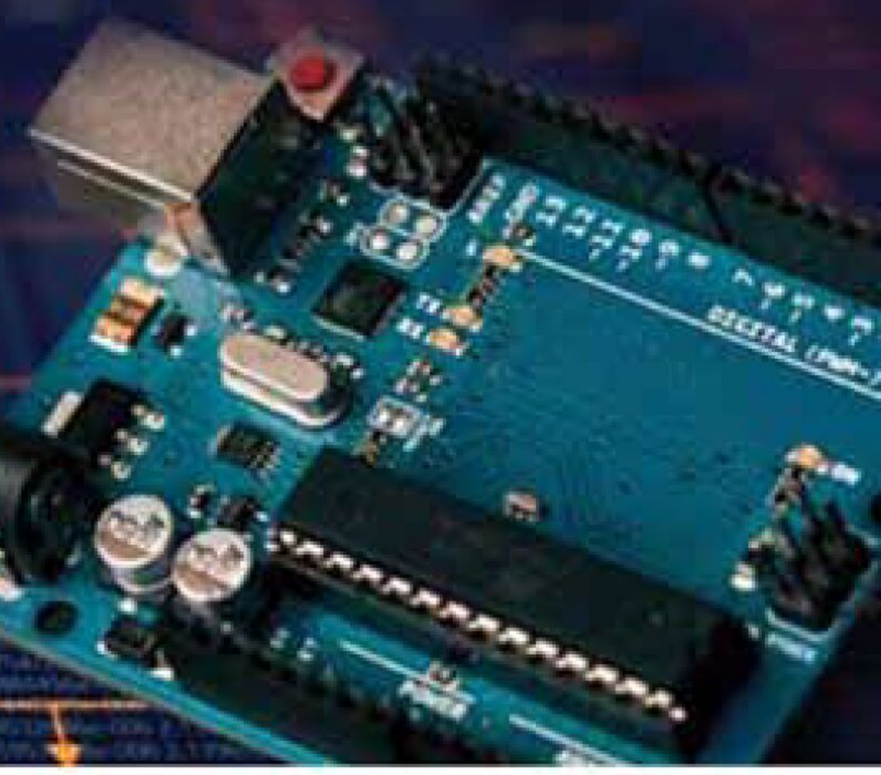
India's #1 Event On Embedded Systems

Co-located with

INDIA ELECTRONICS WEEK

embedded days

31st JAN - 2nd FEB 2024 | KTPO (BENGALURU)



ENABLING SMARTER TECH...

An embedded conference which will focus on latest tech and design challenges related to the fastest growing markets for embedded in India...

TELECOM / 5G
(31 January)



INDUSTRIAL
(1 February)



AEROSPACE & DEFENCE
(2 February)



THE THEMES

AI & ML
Discover how embedded solutions are becoming more intelligent by adopting AI/ML technologies.

IOT
Discover how to develop world-class IoT solutions using state-of-the-art embedded tech.

OPEN SOURCE
Discover how Open Source is enabling better, faster and cheaper development of embedded solutions.

DEV TOOLS
Discover latest development tools that are game changers—before your competition does.

THE EXPO

EXPERIENCE LATEST TECH FIRST-HAND



AI HARDWARE



COMPONENTS & MODULES



DISPLAYS



DEV TOOLS



TEST & DEBUG SOLUTIONS



SMART CONNECTORS

To exhibit, please call +91-9811155335 or growmybiz@efy.in

Mastering Enterprise Mobile Security: Safeguarding Your Digital World

Your smartphone holds a world of data, but is it secure enough? From understanding network technologies to implementing protection measures, this is your guide to safeguarding digital assets.



Mobile devices have become an extension of ourselves, holding a wealth of sensitive information. As technology advances, securing these devices, especially in enterprise settings becomes increasingly vital. Mobile devices have unique characteristics compared to desktops, making their security a bit more challenging. In this article, we will explore various communication methods as well as the security concerns associated with enterprise mobile security.

Mobile devices use electromagnetic waves (zero and one) for communication with each other, but they lack the capability to transfer data over long distances independently. They rely on different methods such as a cellular network (5G is the fifth generation of cellular wireless standards providing capabilities beyond 4G), Bluetooth, Wi-Fi, near field communications, and so on. Let's look into these methods in depth and the security concerns they present.

Cellular networks

Cellular networks, also known as mobile networks, are the primary mode of communication connecting end nodes through service provider networks. Each phone communicates with the service provider by radio waves through a local antenna at a cellular base station or cell site. These cellular networks consist of several components.

Cellular layout: Mobile networks are divided into different geographical areas known as cells. These cells are further divided into hexagonal cells — an antenna covers a cell with certain frequencies. Each cell has a transceiver, a mobile tower that wirelessly connects to mobile devices.

Base station: The base station is placed below the tower. Base stations provide the cell with network coverage and connect with the tower to transmit

voice, data, and other types of content to consumers. The base stations are meant to improve the signal frequency and communication between interconnected devices such as computers or smartphones.

Tower: This is where the antennas and electronic communications equipment are placed to create a cell or adjacent cells. The cell towers distribute the signals generated by the base station.

Mobile tower switching office (MTSO): All base stations and towers in a city are connected via a high-speed link or fibre optics to a mobile telephone switching office (MTSO). Our mobile does not have enough signal power to directly contact a caller residing in another city; hence, it sends a signal to a mobile tower. The mobile tower then sends signals to the MTSO. The MTSO checks our SIM data in its database to find the cell in which the phone is present, and sends a signal to the other city's MTSO. Finally, the MTSO sends signals to the mobile through the mobile tower. The MTSO is normally located in the central cell of a cluster and is generally connected to the public switched telephone network (PSTN).

Public switched telephone network (PSTN): A public switched telephone network is a combination of telephone networks used worldwide, including telephone lines, fibre optic cables, switching centres, cellular networks, satellites and cable systems. The PSTN is a century-old worldwide connected telephone network and lets users make landline telephone calls.

Common security concerns: Here is a critical list of security concerns particularly related to the cellular network.

- Traffic monitoring
- Location tracking
- DDOS attacks
- Access fraud
- Stolen phones
- Subscription fraud

Security measures: The key security measures that can help safeguard against these common security threats are:

- Network traffic monitor and analysis
- Encrypted communication
- Velocity checking
- A subscriber usage-pattern database
- Customer call analysis
- Geographic dispersion checking
- Extensive proprietary anti-fraud algorithms

For more in-depth information about cellular network fraud and solutions, you can refer to *https://csrc.nist.gov/csrc/media/publications/conference-paper/1997/10/10/proceedings-of-the-20th-nissc-1997/documents/031.pdf.*

Wi-Fi

Wi-Fi is the family of wireless network protocols commonly used for local network access. Wi-Fi stands for wireless fidelity. It uses radio frequency to share an internet connection with multiple devices within a certain range via a Wi-Fi router. This router is connected directly to the internet modem and acts as a hub to broadcast the internet signal to all Wi-Fi enabled devices. Wi-Fi repeaters extend the range of the existing network.

Common security concerns: The most relevant security concerns for Wi-Fi networks are:

- Data capture
- On-path attacks
- Denial of service attacks

Security measures: Wired equivalent privacy (WEP) encryption was designed to protect against casual snooping. Later WPS - Wi-Fi protected setup, WPA - Wi-Fi protected access and WAP2 were introduced. All these options are no longer considered secure.

In 2018, WPA3 was announced as a replacement for WPA2, increasing security and enabling secure authentication on wireless routers.

- *WPA3-Personal:* This is a shared key – everyone uses the same key.
- *WPA3-PSK:* The WPA3 session key is derived from PSK using SAE (simultaneous authentication of equals) to provide stronger defences against password guessing. This allows the access provider and station peers to authenticate each other as part of the handshake process while using cryptographic tools to prevent an attacker from performing an offline password cracking scheme.

Li-Fi

Li-Fi, short for light fidelity, offers an innovative way to connect to the internet using light from lamps, streetlights or LED televisions. Li-Fi uses infrared light or LEDs to transmit data. In addition to being cheaper, safer and faster than Wi-Fi, it does not need a router and just requires you to point your mobile or tablet in direct line-of-sight to the light source to surf the web.

Common security concerns: The major security concerns with Li-Fi technology are:

- Jamming
- Spoofing
- Data modification
- Inability to work without light

Security measures: Li-Fi technology is generally considered to be more secure than Wi-Fi, as light cannot pass through walls like radio waves, and it carries more volume of data at a time. Plenty of security features can be embedded in Li-Fi systems in order to make them more secure, such as encryption and monitoring.

Bluetooth

Bluetooth is a short range communications technology intended to replace the cables connecting portable units while maintaining high levels of security. Each device equipped with a Bluetooth chip communicates via spread-spectrum, frequency-hopping, and a full-duplex signal.

An antenna-equipped chip in each device that wants to communicate sends and receives signals at a specific frequency range defined for short-range communication. To communicate, Bluetooth devices pair with each other

to form a personal area network (PAN), also known as a piconet. This process is done through discovery, with one device making itself discoverable by the other device.

Bluetooth is a common mobile connectivity method because it has low power consumption requirements and a short-range signal. One of the most popular communication methods is 802.11 wireless. Point-to-point is a one-to-one connection, involving conversation between two devices. In a point-to-multipoint connection, multiple devices can connect but this doesn't necessarily mean that you can stream media from two devices at a time.

Common security concerns: Some of the most vital security concerns for Bluetooth technology are:

- *Bluejacking:* Sending of unsolicited messages to another device via Bluetooth
- *Bluesnarfing:* Unauthorised access to a Bluetooth-enabled device to steal data from it

Security measures: The security measures that are most effective against these security threats are:

- Update with latest patches
- Monitoring
- Encryption

RFID

Radio frequency identification (RFID) refers to a wireless system comprising two components — tags and readers. The reader is a device that has one or more antennas that emit radio waves and receive signals back from the RFID tag.

There are two types of RFID tags — active and passive tags. An active tag can broadcast a signal over a larger distance because it contains a power source. A passive tag, on the other hand, isn't powered but is activated by a signal sent from the reader.

RFID uses radar technology, and radio energy is transmitted for bi-directional communication.

Common security concerns: Major security concerns hounding RFID technology include:

- Data capture
- Spook reader
- Signal jamming
- Decrypt communication

Security measures: The measures having the most impact on RFID security concerns are:

- Cryptography
- Blocker tags; these prevent unauthorised readers

RFID is commonly used as a geofencing security measure to define a geographic perimeter. When the device enters or exits the perimeter, alerts are sent through this technology.

NFC

Near-field communication (NFC) is a set of standards for contactless communication between devices. NFC chips in mobile devices generate electromagnetic fields. This allows a device to communicate with other devices. NFC is an extension of RFID technology.

Near-field communication transmits data through electromagnetic radio fields to enable two devices to communicate with each other. To work, both devices must contain NFC chips, as transactions take place within a very short distance. NFC-enabled devices must be either physically touching or within a few centimetres of each other for data transfer to occur.

NFC began in the payment-card industry and is evolving to include applications in numerous industries worldwide.

The NFC standard has three modes of operation.

- *Peer-to-peer mode:* Information shared is exchanged between two mobile devices directly.
- *Read/write mode:* An active device receives data from a passive device.
- *Card emulation:* The device is used as a contactless credit card.

It emulates a payment card or other physical card in card readers, magnetic-stripe readers, and contactless card readers used to make payments directly from your mobile device.

Common security concerns: The most relevant security concerns for NFC technology are:

- Remote capture
- Frequency jamming
- On-path attacks
- Loss of NFC device control -- digital pick-pocketing

Security measures: The security measures that most effectively handle NFC security concerns are:

- Encryption
- Up-to-date patching at all times
- Turning it off when not in use

Mobile networks

Mobile networking has evolved significantly since the introduction of the first-generation (1G) mobile network in the 1980s. G refers to generation. Each generation is defined as a set of telephone network standards, which detail the technological implementation of a particular mobile phone system.

1G: 1G was the first generation of wireless cellular technology. It was analogue and supported voice calls only. The maximum speed of 1G was 2.4Kbps.

2G: 2G introduced digital technology and the ability to send SMS (short message service) and plain text-based messages. GSM and CDMA were also introduced during this period. The maximum speed of 2G with general packet radio service (GPRS) was 50Kbps. The maximum theoretical speed was 384Kbps with enhanced data rates for GSM evolution (EDGE).

Before making the major leap from 2G to 3G wireless networks, the lesser-known 2.5G and 2.75G were interim standards that bridged the gap.

3G: 3G enabled web browsing, email, video downloading, picture sharing, and so on. The maximum speed of 3G was around 2Mbps for non-moving devices and 384Kbps for devices in moving vehicles.

4G: 4G applications include amended mobile web access, IP telephony, gaming services,

EFY GROUP
YOURS SINCE 1969

Stay **Connected.**
Stay **Informed.**
Stay **Ahead.**



SUBSCRIBE AND **SAVE**

ORDER FORM

PRINT MAGAZINE	1 YEAR (12 copies each)	3 YEARS (36 copies each)	5 YEARS (60 copies each)
		WITHIN INDIA (IN RUPEES)	
Electronics For You (Rs 100/copy)	840 ☐	2150 ☐	3000 ☐
		SAARC COUNTRIES (IN US$ BY AIR)	
	50 ☐	135 ☐	NA
		OTHER COUNTRIES (IN US$ BY AIR)	
	100 ☐	270 ☐	NA

e-magazine subscriptions within India are available at half the rates mentioned here.
Overseas rates for each e-magazine in US$: 1 year: $12; 3 years: $33; 5 years: $50 only

PRINT MAGAZINE SUBSCRIBERS GET:
- Free e-magazine every month
- Free delivery of print magazine by post
- And much more (check: subscribe@efy.in)
- For delivery by courier, please add Rs 50 for each copy

To subscribe online, visit https://payment.efyindia.com | OR | **SCAN THIS CODE**

Name_____ Organisation_____ Mailing Address_____

_____ City_____

Pin Code_____ State_____ Phone No._____ Email_____

Subscription No. (for existing subscribers only)_____. **I would like to subscribe to the above (✓)marked magazine(s) starting with the next issue.** Please find enclosed a sum of Rs_____ by DD/MO/crossed cheque bearing the No._____ dt._____ in favour of EFY Enterprises Pvt Ltd, payable at Delhi.

Please mark one (nearest) relating to your subscription: ☐ **Indian Company** ☐ **MNC** ☐ **R&D organisation** ☐ **Engineering institute** ☐ **College/School** ☐ **Any other (specify):**_____

Send this filled-in form or copy to : EFY Enterprises Pvt Ltd, D-87/1 Okhla Industrial Area, Phase 1, New Delhi 110 020 | Ph: 011-40596600 | e-mail: support@efy.in

Terms:- # These rates are applicable for new subscribers as well as renewal by existing subscribers # Please allow 4-6 weeks for processing of your subscription.
Please include your pincode for prompt delivery of your copy.

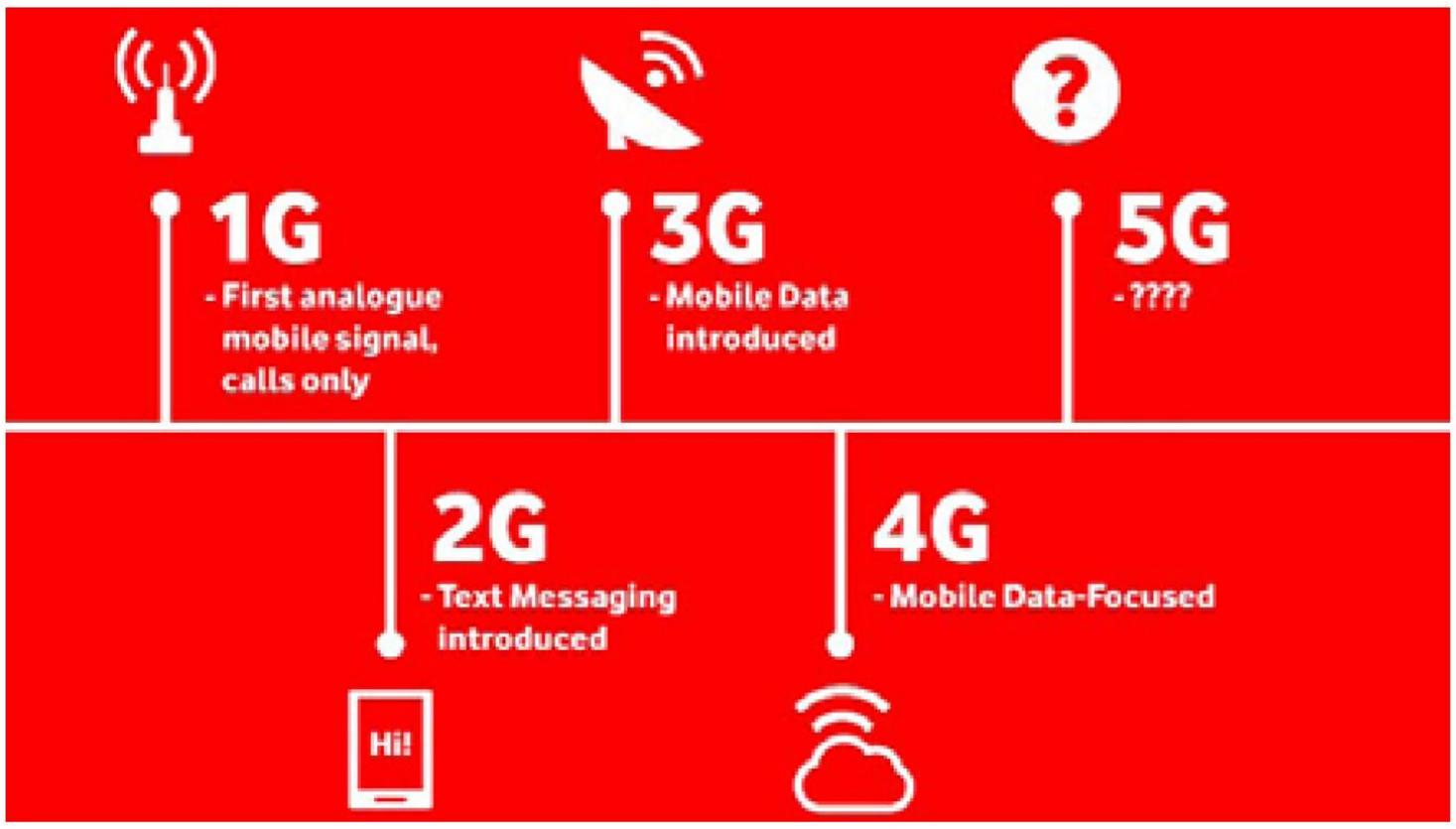


Figure 1: Mobile data speed (Credits: *https://www.techindulge.com/technovation/1g-2g-3g-4g-and-5g-wireless-phone-technology-explained-meaning-and-differences/)*

high-definition mobile TV, video conferencing, 3D television, and cloud computing. The maximum speed of a 4G network when the device is moving is 100Mbps. The speed is 1Gbps for low-mobility communication such as when the caller is stationary or walking.

5G: 5G promises significantly faster data rates, higher connection density, much lower latency, and energy savings, among other improvements. It offers data transfer rates of up to 20Gbps, and allows users to download ultra-high-definition videos and access the internet at lightning-fast speeds. It also offers lower latency, better network coverage, and improved call quality.

Wireless carriers

Wireless carriers are cellular technology companies that provide mobile telecommunications services for supported devices.

CDMA: CDMA stands for code division multiple access. It is a handset-specific technology. CDMA is not very common, and is available in comparatively fewer carriers and countries. These devices are exclusive to Canada, Japan, and the United States.

The CDMA technology does not support transmission of voice and data simultaneously. It is faster, provides better security and comes with built-in encryption.

GSM: The GSM (global system for mobile) standard was launched by AT&T in Finland. Every device uses SIM (subscribers identity module) to communicate with the provider network.

GSM is highly available and globally used. Over 80% of the entire world's mobile networks use it. It uses time-division multiple access (TDMA) and frequency-division multiple access (FDMA). GSM supports the transmission of both voice and data at once. It is slower, less secure, and has no default encryption compared to CDMA.

LTE: Long-term evolution (LTE) is used for faster data transfer and higher capacity. Different variations of LTE networks exist across carriers that use different frequencies. For example, Sprint, T-Mobile, Verizon, and AT&T all have their own bands of LTE.

LTE moves large packets of data to an internet protocol system (IPS). Old methods like CDMA and GSM only transferred small amounts of data.

Both LTE and 4G evolved together, with LTE being the industry standard for the forward edge of the fourth generation's advancement.

4G LTE functionality has two key preconditions: a network that supports the ITU-R (ITU Radiocommunication Sector) standard speeds, and a device powerful enough to match and handle the speeds of that network.

Both GSM and CDMA have switched to LTE as the global 4G standard.

SATCOM: For users who lack traditional landline or cellular coverage, satellite communication (SATCOM) is an option for mobile device use. It uses an artificial satellite to transmit radio signals covering far greater distances and wider areas than most other radio technologies.

Satellite phones function in remote locations as they do not rely on phone transmission lines or cellular towers. Most satellite phones have limited connectivity to the internet, and data rates tend to be slow, but they come with GPS capabilities to indicate the user's position in real time.

Mobile management

Mobile management is all about keeping your devices and data safe — from mobile device management (MDM) that sets access policies to mobile content management (MCM), which secures data.

Mobile device management (MDM): Managing mobile device access and usage in an organisation is a security challenge, where company-owned or user-owned mobile devices are centrally managed. This includes setting policies on apps, camera usage, data, access, and so on. It also focuses on access control features such as screen locks, multi-factor authentication, remote wipe and geofencing.

Mobile content management (MCM): Mobile content management secures the content present on mobile devices; it involves monitoring and restrictions on file sharing, online content viewing, and uploading.

It also entails centralised data management using solutions such as Microsoft Office 365. It implements data loss prevention (DLP) to prevent any sensitive information leakage, encrypts data on the device, and restricts and blocks external or removable drives.

Mobile application management (MAM): Managing mobile apps is challenging, as not all applications are

secure and some may be malicious. MAM ensures that any new application installed is managed through proper channels. This way, only apps with the right permissions are allowed to be installed.

Not all applications are dangerous but those that are not required for business, such as games and social media apps, are denied installation.

Unified endpoint management (UEM): UEM is an evolution of MDM, managing both mobile and non-mobile devices. Through UEM, end users can use different types of devices. Applications can be used across different platforms.

Mobile protection measures

Mobile protection measures are like your device's personal bodyguards, ensuring its safety.

***Remote wipe*:** Managed by MDM, remote wipe removes all the data from the device, usually during theft, necessitating proper data back-up.

Geolocation: This uses location tracking systems for various purposes, including during commute, cross-border alerts and finding lost phones.

Geofencing: This involves implementing restrictions on mobile features when the device is present in a particular location, with authentication and login allowed only within designated areas.

***Screen lock*:** Mobiles are secured using a PIN, passcode, or biometrics, with auto-lock features after a configured time, and data erasure after multiple invalid entries.

Push notification services: This is an information pop-up service on the screen, receiving notifications even when the phone is idle or is using a different application.

Passwords, PINs and biometrics: This involves multi-authentication for mobile devices based on the apps used, managed through MDM, with password rotation, reset and complexity policies.

Context-aware authentication: This helps switching to multi-level authentication when abnormalities are observed, such as access through different locations, different Wi-Fi connections, or paired Bluetooth devices.

***Containerisation*:** This segments storage for business use to avoid data leaks and facilitate easy offboarding, while retaining personal data.

Full device encryption: This ensures data security even after its theft, with keys managed and rotated through MDM.

MicroSD hardware security module (HSM): This provides security services like encryption, key generation, rotation, digital signatures, and encrypted key storage.

SEAndroid (Security Enhancements for Android): This is built using SELinux (Security Enabled Linux) with centralised policy management. It ensures devices are patched with the latest security fixes.

Mobile deployment models

Enterprise mobile device deployment models fall into any of the following categories.

BYOD (Bring Your Own Device): Employees own the device, which can be challenging to secure, and containerisation through MDM can be used to manage corporate data.

COPE (Company Owned/ Personally Enabled): Company buys the device, which is for both professional and personal use. The organisation has full control on the device, including monitoring.

CYOD (Choose Your Own Device): Similar to COPE, these are corporate-owned devices where the user selects the mobile device. This can get tricky in terms of security for certain models.

COBO (Company Owned/ Business Only): Company buys devices and uses them only for official purposes with specific restrictions.

VMI (Virtual Mobile Infrastructure): Apps and data are separated from the mobile device. Data is stored securely in a centralised location to minimise risk.

Mobile security, along with other general security measures, plays a crucial role in ensuring the safety of enterprises and individuals in the rapidly evolving digital landscape. By employing robust mobile management and protection measures, businesses can safeguard sensitive data and mitigate potential threats effectively. END

References

- *https://www.uscybersecurity.net/wp-content/uploads/2019/02/Mobile-Security.jpg*
- *https://whatsag.com/mobile-technology/the-difference-between-a-cell-tower-and-a-base-station.php*
- *https://www.youtube.com/watch?v=1JZG9x_VOwA*
- *https://www.baeldung.com/cs/mobile-networking-generations*
- *https://www.lifewire.com/1g-vs-2g-vs-2-5g-vs-3g-vs-4g-578681*
- *https://www.weboost.com/blog/what-is-4g-lte-and-how-does-it-work#:~:text=LTE%20moves%20large%20packets%20of,it%20helps%20streamline%20your%20service.*
- *https://www.uctel.co.uk/blog/4g-vs-lte-understanding-the-difference-between-4g-and-lte#:~:text=So%20what%27s%20the%20difference%20between,compared%20to%20the%20fourth%20generation.*
- *https://csrc.nist.gov/csrc/media/publications/conference-paper/1997/10/10/proceedings-of-the-20th-nissc-1997/documents/031.pdf*
- *https://www.investopedia.com/terms/n/near-field-communication-nfc.asp*
- *https://www.youtube.com/watch?v=UOGZbq4t_g8*

By: Thangaselvi Arichandrapandian

The author works in a leading bank as AVP. She is a perennial learner and loves the quote: "The more I learn, the more I realise how much I don't know."-*Albert Einstein*

FOCUS

Using Blockchain

The 'Big Problem' for Blockchain



Despite its meteoric rise with the advent of cryptocurrencies, blockchain technology faces a conundrum — its limited adoption across diverse sectors. We delve into this 'big problem' for blockchain, exploring why a technology hailed as revolutionary primarily remains confined to the crypto realm. Challenges, misconceptions, and the potential future of blockchain in a world still grappling with its broader applications are also discussed. *Read more on page.....28*

Open Source and Blockchain: Building Trust in a Decentralised World



The marriage of blockchain and open source has ushered in a new era of innovation, collaboration, and decentralised possibilities. So let's explore what blockchain entails, its diverse types, the dichotomy of public and private blockchains, and why open source is the bedrock upon which the future of blockchain will be built. *Read more on page.....32*

Tools for Security Audit and Vulnerability Analysis of Smart Contracts



Smart contracts are an essential component of blockchain technology, and have helped it transcend typical cryptocurrency and financial transactions. But these contracts do come with a few flaws, making it imperative that they go through a security audit. Among the various tools available for this, Slither ranks high. *Read more on page.....34*

The Blockchain and its Many Uses

The potential for increased security, efficiency, and transparency that blockchain offers is too significant to ignore. It is evolving and disrupting traditional systems, proving that it has real industry altering powers.

Read more on page.....46

Selecting the Right Blockchain Technology

As blockchain continues to evolve, so do your opportunities. This article is a roadmap to informed blockchain decisions and will help you navigate public, private, and hybrid options with precision.

Read more on page.....52

Cryptocurrency Wallets: Implementing MetaMask for Blockchain Transactions

This article introduces and compares popular cryptocurrency wallets. It also tells you how to select one. It then gives a practical demonstration of implementing the MetaMask wallet for blockchain transactions.

Read more on page.....56

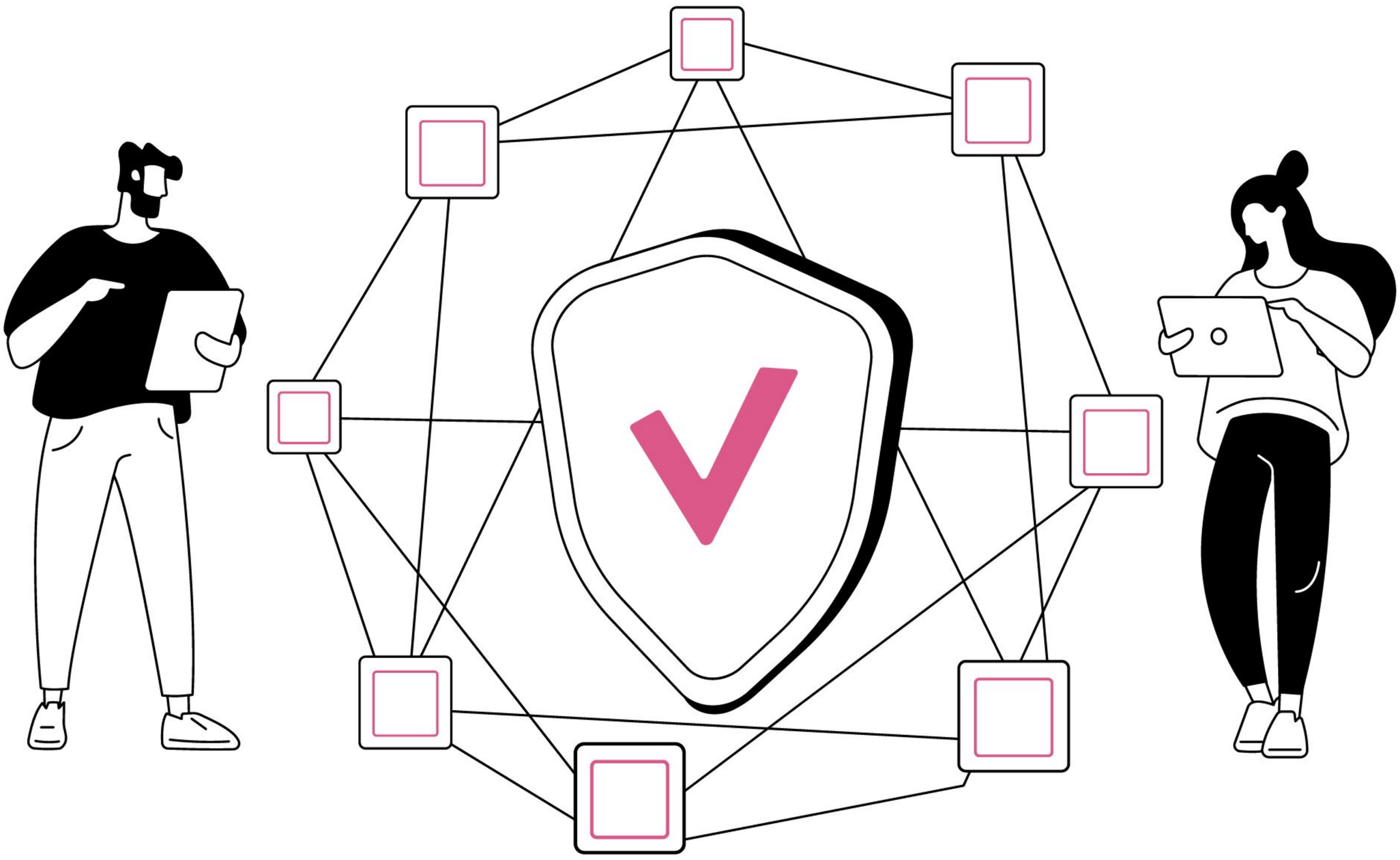
Blockchain Technology and Generative AI: A Symbiotic Partnership

The intersection of blockchain technology and generative AI will usher in a new era of efficiency, security, and creativity in the digital world.

Read more on page.....60

Decentralised Applications: Revolutionising the Digital Landscape

Characterised by enhanced security, transparency, and efficiency, DApps are paving the way for a future where individuals have greater control over their data and interactions. In short, they are changing the way we interact with technology.



Decentralised applications (DApps) are reshaping the way we interact with technology. Unlike traditional applications that rely on central authorities, DApps utilise blockchain technology to create a trustless and transparent environment for users. With the rise of cryptocurrencies and blockchain platforms like Ethereum, the potential for DApps to disrupt various industries is becoming increasingly evident.

What exactly are DApps?

DApps are decentralised applications that operate on a peer-to-peer network of computers, utilising blockchain technology. Unlike traditional applications that are controlled by a central authority, DApps function independently, without any central governing entity. This decentralised nature ensures transparency, security, and immutability, making DApps highly resilient to censorship or malicious activities.

DApps are typically open source, allowing developers to contribute and modify the source code while adhering to predetermined consensus rules. They also employ smart contracts for the execution of predefined protocols, further enhancing their efficiency and trustworthiness. These characteristics differentiate DApps from their centralised counterparts, offering users greater control over their data and enhancing overall security.

The basics of decentralised applications

To understand decentralised applications, we must first grasp the concept of blockchain technology. Traditionally, applications rely on central servers to store and process data, leading to concerns about privacy, security, and single points of failure. Unlike centralised applications, decentralised applications operate on distributed networks that are not controlled by a single entity.

At the heart of DApps lies the blockchain, a distributed ledger that records transactions and interactions between participants. Smart contracts, which are self-executing agreements with predefined rules, automate processes and eliminate the need for intermediaries. This decentralised infrastructure ensures trust, transparency, and security.

Real-world DApp use cases

DApps are finding numerous applications across various industries. Here are some prominent real-world use cases of DApps.

Finance

Decentralised finance (DeFi) applications are gaining significant traction, offering users transparent and inclusive financial services. DApps like Compound, Aave, and Uniswap enable lending, borrowing, and decentralised trading without relying on traditional intermediaries.

Supply chain management

DApps provide an immutable and transparent record of supply chain activities. This enables businesses to track and verify the origin, authenticity, and movement of goods. Projects like VeChain and Origin Trail aim to optimise supply chain processes by leveraging the power of blockchain technology.

Gaming

DApps are disrupting the gaming industry by introducing ownership and interoperability of in-game assets. Games like Axie Infinity and Cryptokitties allow players to own, trade, and monetise virtual assets securely on the blockchain, creating a new paradigm for the gaming experience.

Governance

DApps are empowering decentralised governance models by providing transparent decision-making processes. Projects like Aragon and DAOstack enable token holders to participate in voting, proposal creation, and governance activities, allowing for decentralised and inclusive decision-making.

Advantages of decentralised applications

DApps offer a range of advantages.

Transparency and security

One of the key advantages of DApps is their transparency. Since all transactions are recorded on the blockchain, anyone can verify the integrity of the data. This transparency reduces the risk of fraud and promotes accountability. Moreover, the decentralised nature of DApps makes them resistant to hacking attempts. Unlike centralised databases, which are vulnerable to cyberattacks, the distributed nature of the blockchain adds an extra layer of security.

Elimination of intermediaries

In traditional applications, intermediaries such as banks, payment processors, or centralised exchanges facilitate transactions. These intermediaries often impose additional costs and delays. With DApps, intermediaries are largely eliminated. Smart contracts enable direct peer-to-peer transactions, cutting out unnecessary middlemen. This not only reduces costs but also accelerates the speed of transactions.

User control and ownership

With DApps, users gain greater control over their data and digital assets. Traditional applications often collect and monetise user data without consent. In contrast, DApps allow users to retain ownership of their data and determine how it is used. This shift in control empowers individuals and protects their privacy.

Global accessibility

Decentralised applications have the potential to bridge the global digital divide. Since they operate on the internet, DApps can be accessed by anyone with an internet connection. This opens opportunities for individuals in underserved regions to participate in the digital economy, access financial services, and engage in online transactions.

Challenges and limitations of decentralised applications

While decentralised applications offer numerous advantages, they also face certain challenges and limitations that must be addressed for widespread adoption.

Scalability

One of the primary challenges faced by DApps is scalability. Blockchain networks, especially those utilising proof-of-work consensus algorithms, have limited processing capacity. This results in slower transaction times and higher fees during periods of high demand. To overcome this challenge, various scaling solutions such as Layer 2 protocols, and improved consensus mechanisms are being developed.

User experience

The user experience in decentralised applications is often criticised for being complex and unintuitive. Interacting with DApps typically requires users to manage their private keys and understand the intricacies of blockchain technology. Improvements

in user-friendly interfaces and streamlined processes are necessary to enhance the adoption of DApps among mainstream users.

Regulatory and legal frameworks
As decentralised applications gain popularity, regulatory and legal frameworks are evolving to accommodate this new technological landscape. The decentralised nature of DApps poses challenges for authorities in terms of jurisdiction, compliance, and enforcement. Striking the right balance between innovation and regulation is crucial to ensure the long-term success of decentralised applications.

Energy consumption
Certain blockchain networks, particularly those utilising proof-of-work consensus algorithms, consume significant amounts of energy. This energy consumption has raised concerns about the environmental sustainability of DApps. The development of more energy-efficient consensus algorithms, like proof-of-stake, is a step towards addressing this challenge.

The future of decentralised applications

As the potential of decentralised applications continues to be realised, their impact on various industries is expected to grow significantly. Here are some areas where DApps are making waves.

Finance
Decentralised finance, often referred to as DeFi, is one of the most prominent use cases for DApps. DeFi applications enable users to access financial services such as lending, borrowing, and trading without intermediaries. These applications provide greater financial inclusivity, lower costs, and increased transparency.

Supply chain management
Decentralised applications have the potential to revolutionise supply chain management. By leveraging blockchain technology, DApps can enable end-to-end visibility, traceability, and transparency in supply chains. This can streamline processes, reduce fraud, and enhance consumer trust.

Gaming and digital collectibles
The gaming industry is embracing decentralised applications for the creation of unique digital assets and the facilitation of secure peer-to-peer transactions. Blockchain-based games and marketplaces allow players to truly own and trade in-game items, fostering a vibrant virtual economy.

Social media and content sharing
Decentralised social media platforms are emerging to address issues of privacy and data ownership. These DApps enable users to share content, engage in discussions, and monetise their contributions without relying on centralised platforms that profit from user data.

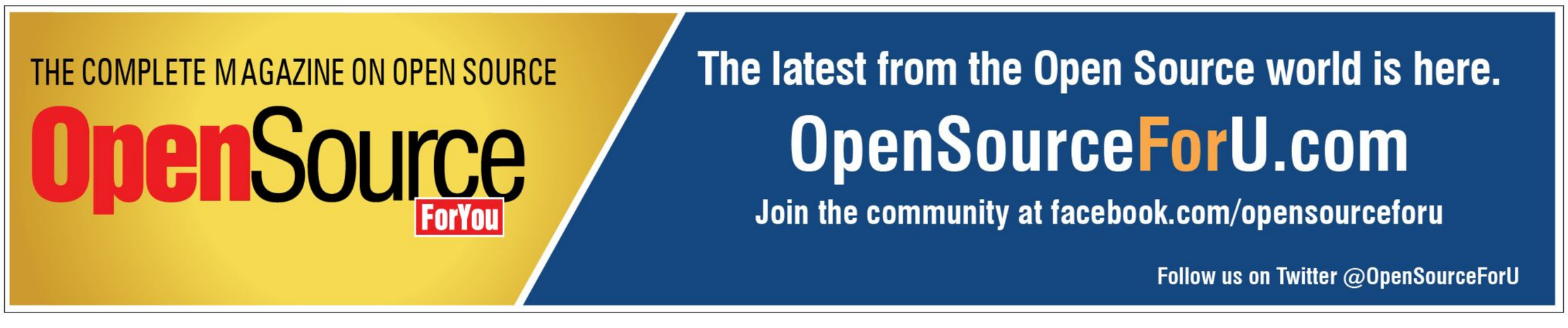
Decentralised applications offer a promising vision of a more transparent, inclusive, and secure digital future. By harnessing the power of blockchain technology, DApps have the potential to transform industries, empower individuals, and reshape the way we interact with technology. Despite the challenges they face, continued innovation and adoption will pave the way for a decentralised revolution. Whether you're a newcomer to the world of decentralised applications or a tech enthusiast, exploring the possibilities and staying informed about their developments will be key in embracing this transformative technology. END

References

- *https://www.gemini.com/cryptopedia/decentralized-applications-defi-dapps*
- *https://www.geeksforgeeks.org/*

By: Neetesh Mehrotra

The author works at Ernst & Young as a senior. His areas of interest are Java development and automation testing.



ACCELERATING DEVELOPMENT AND DEPLOYMENT OF OPEN SOURCE

20th edition









An EFY GROUP EVENT

tracks

- **Community** (India contributes)
- **AI & ML** (Opening up the Tech)
- **IT Infra** (Security, Storage & Cloud)
- **Developers' Meet**
- **DevOps**
- **Data & Bases:** Open Source Rocks!

Asia's #1 Conference on Open Source

20th Edition

OPEN SOURCE INDIA

19-20 October 2023

NIMHANS CONVENTION CENTER, BENGALURU

Register Now!

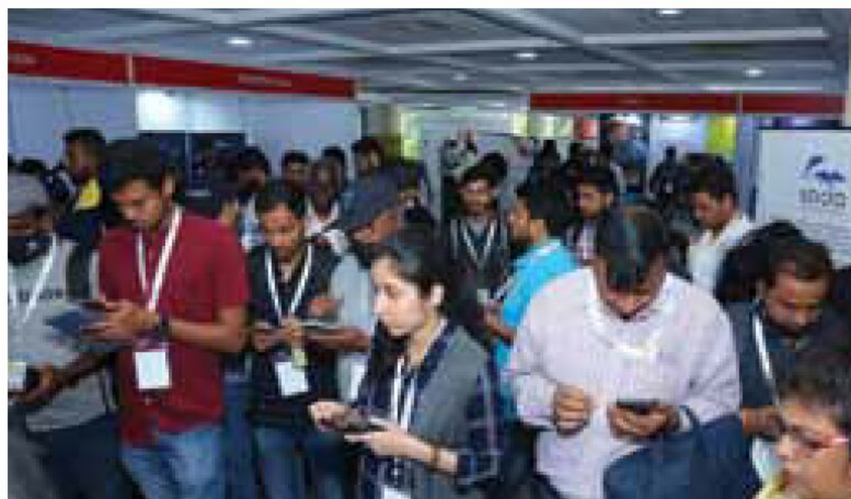
https://opensourceindia.in

www.OpenSourceIndia.in

For more details, call on +91 98111-55335 or write to info@opensourceindia.in

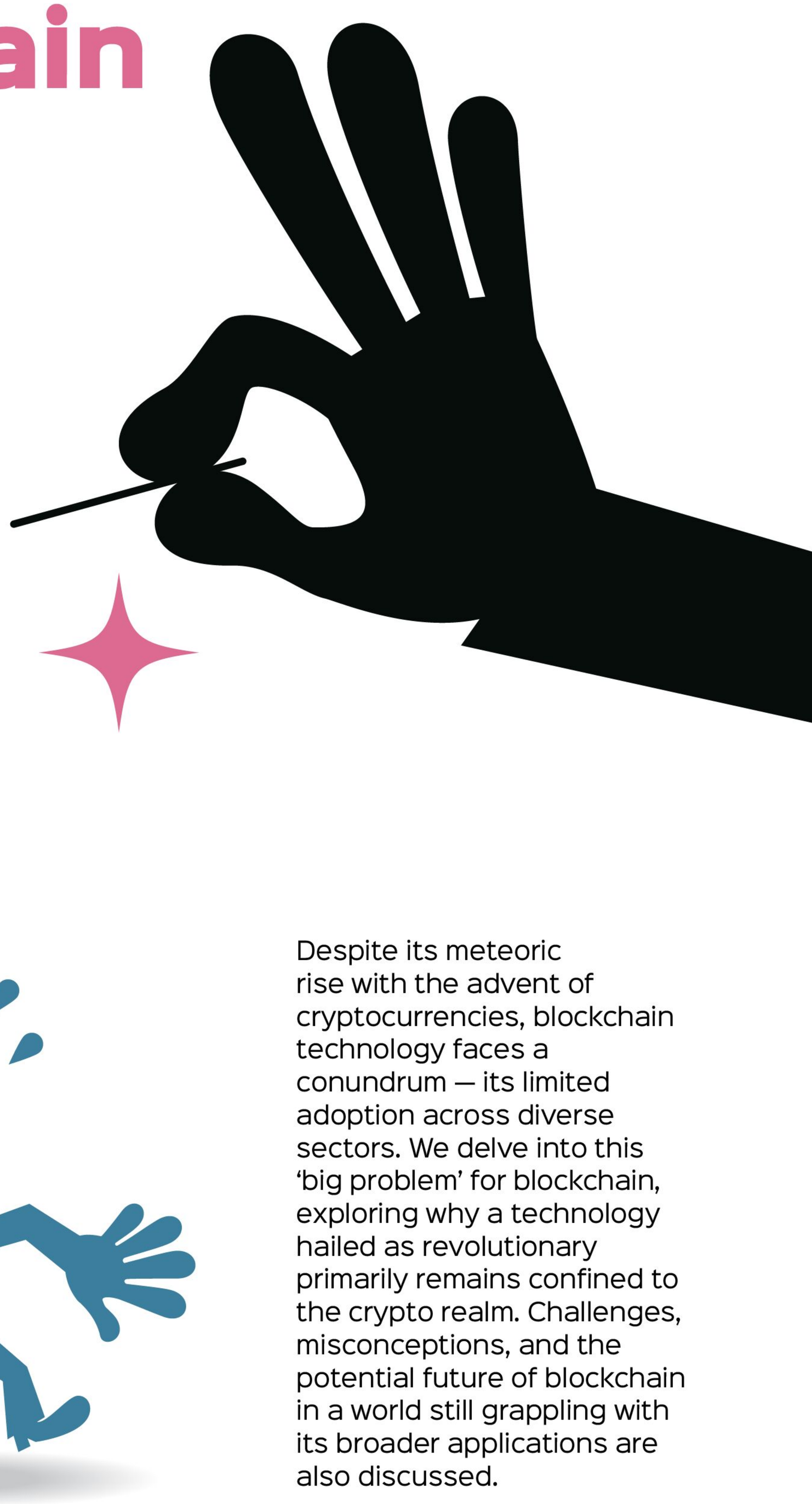






The ‘Big Problem’ for Blockchain





Despite its meteoric rise with the advent of cryptocurrencies, blockchain technology faces a conundrum — its limited adoption across diverse sectors. We delve into this ‘big problem’ for blockchain, exploring why a technology hailed as revolutionary primarily remains confined to the crypto realm. Challenges, misconceptions, and the potential future of blockchain in a world still grappling with its broader applications are also discussed.

Blockchain technology, at its core, is a digital ledger of transactions that is duplicated and distributed across an entire network of computer systems. Every time a new block is added to the blockchain, every computer on the network updates its blockchain to reflect the change. Through this mechanism, blockchain ensures that every transaction is transparent to all users and also remains immutable once added. In essence, it provides a trustworthy record without the need for intermediaries.

The real breakthrough for blockchain technology came with the rise of Bitcoin, the world's first cryptocurrency. Proposed by an unknown entity named Satoshi Nakamoto in 2008, Bitcoin offered a decentralised way to conduct transactions without relying on a central bank or single administrator. This independence from traditional banking and governmental systems was its most alluring charm.

The crypto boom — blockchain's claim to fame

There's no discussing blockchain's journey without mentioning the astronomical rise of cryptocurrencies. As Bitcoin grew in prominence, so did the underlying technology that powered it — blockchain. It didn't take long for venture capitalists and other market savants to realise the potential for making easy money with cryptocurrencies and NFTs.

By 2021, what began as a fringe experiment with Bitcoin had evolved into a global phenomenon with thousands of digital currencies vying for attention. This crypto boom did more than just turn heads; it signalled a seismic shift in how people perceived money, value, and decentralised systems.

Several factors contributed to the crypto explosion.

Distrust in traditional financial systems: Post the 2008 financial crisis, there was growing disillusionment with centralised banking systems and fiat currencies. Cryptocurrencies, being decentralised and transparent, became an attractive alternative for many.

Speculative investment: As stories of early Bitcoin investors becoming millionaires began to circulate, more people dove headfirst into crypto as an investment opportunity, hoping to reap massive returns.

Technological curiosity: For many tech enthusiasts, the underlying blockchain technology was as alluring as the potential profits. The idea of decentralised, transparent transactions without intermediaries was groundbreaking.

New financial solutions: Cryptocurrencies and blockchain introduced innovative solutions to age-old financial problems. Concepts like smart contracts, decentralised finance (DeFi), and non-fungible tokens (NFTs) promised to reshape sectors ranging from lending and borrowing to art and entertainment.

The downfall of crypto and its impact on blockchain

While the crypto boom played a pivotal role in bringing blockchain to the forefront, it also cast a shadow. The very success of cryptocurrencies inadvertently confined blockchain's perception to the realm of digital money. This overshadowing has, to some extent, influenced the challenge blockchain faces in finding its footing in diverse industries outside the world of crypto.

To make matters worse, the cryptocurrency market experienced a major crash in 2021, with the total market capitalisation falling from nearly $3 trillion to less than $1 trillion. This crash was caused by several factors, including rising inflation, rising interest rates, and increased regulatory scrutiny.

One of the biggest scandals that contributed to the crash was the collapse of the cryptocurrency exchange FTX. FTX was a major player in the crypto market, and its collapse caused a wave of panic selling. The scandal surrounding FTX involved allegations that the company was insolvent and that it had engaged in market manipulation.

This triggered the Securities and Exchange Commission (SEC) to act and the crypto crackdown began. The SEC issued several enforcement actions against crypto companies, alleging that they had violated securities laws. These enforcement actions further shook the confidence of investors in the crypto market.

The crypto crash of 2021 had quite a few remarkable consequences. First, it caused a significant loss of wealth for investors. Second, it led to increased regulatory scrutiny of the crypto market. Third, it damaged the reputation of cryptocurrencies and made it more difficult for crypto companies to raise capital. It was a major setback for the cryptocurrency industry, but moreover, it was a major setback for blockchain technologies.

As funding for crypto projects seized, blockchain projects focused on other domains also felt the impact.

According to a report by *CB Insights*, venture capital funding for blockchain companies fell by 88% in the first half of 2022 compared to the same period in 2021. The report also found that the number of blockchain deals fell by 60% in the same period. The lack of clear use cases for blockchain technologies outside of the crypto industry made it difficult for investors to see the potential return on investment for these projects.

The theoretical use cases for blockchain outside of crypto and finance

Before we jump into the current state of blockchain, it is necessary to summarise some of the potential problems it could theoretically solve, outside of crypto and finance. These are the potential use

cases that have been talked about for nearly a decade now.

Supply chain management: Blockchain can be used to track the movement of goods and materials through a supply chain. This can help to improve efficiency, transparency, and traceability.

Healthcare: Blockchain can be used to store and share medical records in a secure and private way. This can help to improve patient care, and to reduce fraud and errors.

Government: Blockchain can be used to create secure and transparent records of government transactions. This can help to improve accountability and transparency, and to reduce corruption.

Other industries: Blockchain is also being explored for use in other industries, such as insurance, real estate, and media.

The current state of blockchain technology outside of crypto and finance

Outside of cryptocurrencies, most of which are directly or indirectly under the investigation of SEC, not much has happened for blockchain technology. The total locked value (TVL) of decentralised financing went from an all-time high of $248 billion in 2022 to less that $40 billion in 2023, and NFTs cooled off almost as fast as they had heated.

I did a survey of large scale applications of blockchain technologies in 2023 and I am afraid I could not find much to talk about. Keep in mind that this is my own personal research and therefore it's not conclusive. I might have missed an application or two, but overall, large scale applications (not related to crypto and finance) currently running on blockchain technology are next to non-existent.

Current applications of blockchain across the world

IBM Food Trust: IBM Food Trust is a blockchain-based platform that tracks the movement of food products through the supply chain. Launched in 2021, this platform is used by food producers, retailers, and distributors to ensure the safety and authenticity of food products.

Walmart: Walmart is experimentally using blockchain technology to track the movement of produce through its supply chain at a limited capacity. Not much has been spoken about this project since its inception in 2022.

Estonia: Estonia is using blockchain technology to record land ownership and manage elections. It is one of the most advanced countries in the world in terms of its use of blockchain technology.

United Arab Emirates: The United Arab Emirates is using blockchain technology experimentally to track the movement of goods and materials through its ports.

The 'big problem' for blockchain

For most blockchain experts, the big problem to solve is the 'blockchain triad', as coined by Vitalik Buterin, wherein every blockchain application has to choose between focusing on decentralisation, security or scalability but cannot have all three without compromising on at least one.

But I would like to argue for a bigger 'big problem' for blockchain — adaptability. Outside of Bitcoin, which seems to be the only technology to find its grounding in a proper use case and an application, blockchain is struggling. We are yet to put theory into practice when it comes to blockchain and this is becoming clearly evident with every passing day.

Probable reasons for the blockchain adoption abyss

As a researcher, I can only share potential reasons for the lack of adoption of blockchain technology based on observational data. This is by no means an exhaustive list of reasons, and I welcome any feedback and criticism on the points that I have raised here.

Complexity and understanding: Not only does blockchain suffer from bad PR due to crypto and NFTs, it also has a problem with outreach. Most people, including the ones invested in blockchain technology, do not understand how the technology works and what makes it uniquely useful. A survey by *Statista* in 2022 found that only 39% of Americans have heard of blockchain. Of those who have heard of it, only 16% said they have a good understanding of it.

Lack of investment by big tech: Although tech startups disrupt industries more often than big tech, it is often the big tech companies that throw money behind such companies and projects to fuel the disruption. A classic example is Microsoft with OpenAI. Unfortunately, such a thing has not happened in the case of blockchain. Despite there being no shortage in blockchain startups, big tech companies such as Google, Microsoft and Meta have not been very forthcoming in investing in these projects. In fact, the world of big tech has been suspiciously silent on the whole blockchain saga. There are multiple reasons for this.

- *The crypto contagion:* The most valuable asset of a big tech company is its stock price. Protecting the value of its stock is the first priority for the CEOs of such companies. Therefore, getting into a technology that has direct ties with the crypto space can be potentially damaging for the stock price.
- *Lack of regulatory clarity:* Even if an interesting project worth investing were to come up, it is difficult for cryptocurrencies to not play some form of a role in that project. Given the lack of regulatory clarity from the SEC, as it stands today, the future of blockchain projects can be highly speculative. Big tech likes due diligence when

it comes to regulatory issues for obvious reasons.

- *Blockchain is not a one-fit-all model:* Unlike a technology like AI, blockchain is not a one-fit-all model. It caters to a specific set of use cases that mostly revolve around security. So, while the technology might be attractive, it doesn't mean that every tech company has a potential need for it.
- *Problems with integration:* To integrate blockchain into a pre-existing system, a ground up rebuild of the entire system is required. Imagine having a house without any plumbing. Now, to lay pipes, you will have to break all the floors and every wall in the house. It is easier to just break the house and rebuild it from scratch. But what if it wasn't a house but a 1000 acre palace with 100s of rooms? That's basically the conundrum for big tech companies. Even if they found an application for blockchain in their preexisting products, they are just too big to be rebuilt from the ground up.

Regulatory concerns and VC funding: As already discussed, there is a lack of clarity as to where SEC stands on most crypto projects. Crypto projects are inherently linked to blockchain projects outside of crypto. Every technology requires VC trust in order to thrive as they are the ones who put their money on the line to fund speculative projects. With blockchain, there can be no trust unless there is regulatory clarity. Therefore, the money is running dry, demotivating any further innovation in this space.

The blockchain triad: As stated earlier in the article, the blockchain triad is an existential problem with current blockchains. A technology as pristine as Bitcoin, too, is not immune to this problem. Bitcoin focuses on security which then raises issues with scalability on level 1. Developers bandage this problem by building layer 2 blockchains over the layer 1, but that adds up complexity and compromises on decentralisation and security. Research is still ongoing as to how this problem can be mitigated, but for now, the problem remains.

The looming quantum conundrum: As the world edges closer to realising the potential of quantum computing, the very foundation of blockchain technologies is under threat. Quantum computers, with their ability to perform complex calculations at unprecedented speeds, have the potential to crack cryptographic algorithms that keep blockchains secure. Traditional cryptographic methods, like the ones employed in many cryptocurrencies, rely on problems that are computationally hard for classical computers to solve, such as factoring large numbers. However, quantum algorithms, like Shor's algorithm, can solve these problems efficiently. If large scale, practical quantum computers become a reality, they could decrypt blockchain records and forge transactions, effectively dismantling the trust and security that underpin blockchain systems. This quantum conundrum underscores the need for post-quantum cryptographic methods if blockchain technologies are to survive in a post-quantum world.

A potential 'X-chain' that supersedes blockchain altogether: While blockchain has been lauded for its potential to revolutionise sectors from finance to supply chain, it's not impervious to being supplanted. Emerging advancements, such as artificial intelligence (AI), offer enhanced data analysis and decision-making capacities, which might render some blockchain applications redundant. Quantum computing, as discussed, poses a direct threat to blockchain's cryptographic security. Furthermore, concepts like the 'Blockchain Triad' (which advocates a synthesis of blockchain, AI, and the Internet of Things), hint at a future where blockchain isn't the standalone star but merely a part of a more intricate technological matrix. As history has shown, no technology is sacrosanct. If a more efficient, secure, and scalable solution emerges, it could relegate blockchain to the annals of technological history, much like its predecessors.

Some of the reasons why blockchain is struggling can be addressed rather quickly. For instance, if the SEC moves fast and makes the regulations for blockchain technologies clearer, it can instantly boost the VC trust leading to reflow of funding in the space. This could have a chain effect with big tech trusting the technology and taking steps for adopting blockchain, which could then help startups build disruptive technologies using blockchain. However, there are also some existential threats to blockchain, the solutions for which are currently unclear. Issues such as quantum conundrum and Blockchain Triad are problems that could lead to people developing a newer more advanced technology that renders the concept of blockchain moot.

Personally, I feel blockchain is a great technology with a lot of potential to offer. The rise of Bitcoin is a testament to that. But for blockchain to thrive as a technology at large, the 'big problem' needs to be addressed by the tech community. END

By: Mir H.S. Quadri

The author is a research analyst with a specialisation in artificial intelligence and machine learning. He is the founder of Arkinfo, which focuses on the research and development of tech products using new age technologies. He shares a deep love for analysis of technological trends and understanding their implications. Being a FOSS enthusiast, he has contributed to several open source projects.

Open Source and Blockchain: Building Trust in a Decentralised World

The marriage of blockchain and open source has ushered in a new era of innovation, collaboration, and decentralised possibilities. So let's explore what blockchain entails, its diverse types, the dichotomy of public and private blockchains, and why open source is the bedrock upon which the future of blockchain will be built.



At its core, blockchain is a digital ledger that records transactions in a secure, transparent, and immutable manner. Picture it as a chain of blocks, each containing a set of transactions. These blocks are linked together in chronological order, forming an unbreakable chain. The brilliance of blockchain lies in its decentralised nature; no single entity has complete control over the network. Instead, it's maintained by a network of computers, or nodes, that work collaboratively to validate transactions through consensus mechanisms like proof of work (PoW) or proof of stake (PoS).

Let's take a practical example to understand this better. Imagine you're buying a piece of jewellery. With traditional methods, it's hard to verify if the gemstone in that necklace is really as rare as is claimed. Enter blockchain. In a blockchain-powered supply chain, each step of the gemstone's journey, from the mine to the store, is recorded in the blockchain. So, when you scan a QR code on that necklace, you get a detailed history of where the gemstone was sourced, cut, and even its authenticity certificates. This level of transparency builds trust—something that was difficult to achieve before.

Overview of how blockchain works

Now, let's take a closer look at the fundamental mechanics of blockchain.

Blocks: Think of a blockchain as a chain of blocks, where each block is like a page in a ledger. It contains a list of transactions. For instance, in a cryptocurrency blockchain like Bitcoin, a block may record all the recent transactions that took place, including who sent how much Bitcoin to whom.

Nodes: Blockchain is not maintained by a central authority; instead, it's a distributed network. This means there are many computers (nodes) connected to the network, each having a copy of the entire blockchain. These nodes work collectively to validate transactions and add them to the blockchain.

Consensus mechanism: The key to blockchain's security is its consensus mechanism. This is how the network ensures that all nodes agree on the validity of transactions. In Bitcoin, the most well-known consensus mechanism is proof of work (PoW). Miners, the participants in the network, solve complex mathematical puzzles to validate transactions. Once a puzzle is solved, the new block is added to the chain, and the miner is rewarded with some cryptocurrency. This process requires significant computational power, making it extremely difficult for anyone to manipulate the blockchain.

Types of blockchains

Blockchain technology comes in various types, each designed for specific purposes. Here's an overview of the three main types.

Public blockchains: Public blockchains are open to anyone, making them entirely decentralised. These blockchains are maintained by a global network of nodes, and anyone can join, participate, and validate transactions. Public blockchains offer a high degree of transparency and security. They are ideal for applications where trust among participants is paramount, such as cryptocurrencies.

Private blockchains: Private blockchains, as the name suggests, restrict access. They are used primarily within organisations for internal purposes. Access to a private blockchain is controlled, typically by a central entity or group of entities. This results in faster transaction processing and greater privacy compared to public blockchains.

Consortium blockchains: Consortium blockchains strike a balance between public and private blockchains. They are governed by a pre-selected group of organisations or nodes. Consortium blockchains are semi-decentralised, combining the controlled access of private blockchains with the collaborative features of public blockchains. They are often used in industries where multiple organisations need to collaborate while maintaining some level of trust and privacy.

Use cases and examples of each type

These use cases explore the real-world impact of blockchain's versatility. Let's take a look at how they shape industries and redefine trust.

Public blockchain use cases

- **Bitcoin**, the pioneer of cryptocurrencies, operates on a public blockchain. It allows anyone to participate in the network, verify transactions, and earn rewards (in the form of new Bitcoins) for contributing computational power. Bitcoin's primary use case is as a digital currency, enabling peer-to-peer transactions without the need for intermediaries like banks.
- **Ethereum** is another well-known public blockchain, but its use cases go beyond digital currency. Ethereum introduced smart contracts, which are self-executing contracts with the terms directly written into code. These contracts run on the Ethereum blockchain and enable automated and secure execution of agreements. For example, digital artists can create a smart contract that ensures they receive a percentage every time their artwork is resold, empowering creators in the digital realm.

Private blockchain use case

- **Hyperledger fabric** is a prominent example of a private blockchain framework. It's designed for use within organisations and consortiums. Hyperledger fabric offers enhanced privacy and scalability while maintaining control over the network. Use cases for this framework include supply chain management, where companies need to securely share information about the movement of goods without exposing sensitive data to the public.

Consortium blockchain use case

- **R3 Corda** is a consortium blockchain platform designed for businesses and financial institutions. It allows multiple parties to collaborate while preserving confidentiality. Corda is used in scenarios like trade finance, where banks, corporations, and regulators need to exchange information and assets securely. For instance, it can facilitate the transfer of ownership of goods as they move through a supply chain while ensuring that only authorised parties have access to relevant data.

Importance of open source for blockchain

Open source and blockchain are kindred spirits, both embodying transparency, collaboration, and community-driven innovation. Open source means the source code is freely available for inspection, modification, and enhancement by anyone. In the blockchain realm, this philosophy is pivotal. Consider Ethereum, a decentralised platform that allows developers to build and deploy smart contracts. Its open source nature ensures that the platform evolves based on collective intelligence, promoting security and adaptability.

Open source blockchain use cases

Open source blockchain technology has unlocked a treasure trove of real-world applications. Let's dive into some examples.

Supply chain authentication with VeChain: VeChain, an open source blockchain platform, partners with companies to verify the authenticity and origin of products. For instance, luxury brand products can be traced from creation to the store, assuring buyers that they're receiving genuine items.

Decentralised identity with Sovrin: Sovrin, an open source blockchain network, addresses the challenges of managing digital identities. It enables individuals to control their personal information securely, reducing the risks of data breaches and identity theft.

Energy trading with Powerledger: Powerledger leverages blockchain to enable peer-to-peer energy trading. Home owners with solar panels can sell excess energy to their neighbours, promoting sustainable energy usage.

Continued to page...65

Tools for Security Audit and Vulnerability Analysis of Smart Contracts

Smart contracts are an essential component of blockchain technology, and have helped it transcend typical cryptocurrency and financial transactions. But these contracts do come with a few flaws, making it imperative that they go through a security audit. Among the various tools available for this, Slither ranks high.



Blockchain technology has emerged as a revolutionary solution with versatile applications beyond its initial association with cryptocurrencies. Its decentralised and tamper-resistant nature offers a range of real-world use cases that go beyond financial transactions.

With the implementation of smart contracts, the blockchain environment provides high-end and fully secured applications for assorted domains including e-governance, real estate, finance, logistics, and many others. Smart contracts are transforming the real estate industry by automating property transactions. They facilitate seamless and secure buying, selling, and renting of properties, with ownership transfers occurring only when payment conditions are met.

Key use cases and applications of blockchain

Imagine a world where transparency is a given, fraud is rendered nearly impossible, and trust between parties is inherent. That's the world blockchain technology is shaping.

- ***Supply chain management:*** Blockchain provides end-to-end transparency and traceability in supply chains. Each step of a product's journey can be recorded on the blockchain, ensuring authenticity and preventing fraud. This is particularly important in industries where provenance, such as the origin of luxury goods or food products, is critical. Smart contracts ensure automatic execution of agreements when predefined conditions, such as the arrival of goods at a specified location, are met. This real-time tracking minimises fraud, reduces paperwork, and streamlines logistics processes.
- ***Decentralised finance (DeFi):*** Smart contracts have become the foundation of the DeFi movement. They power lending and borrowing platforms, decentralised exchanges (DEXs), automated market makers (AMMs), and yield farming

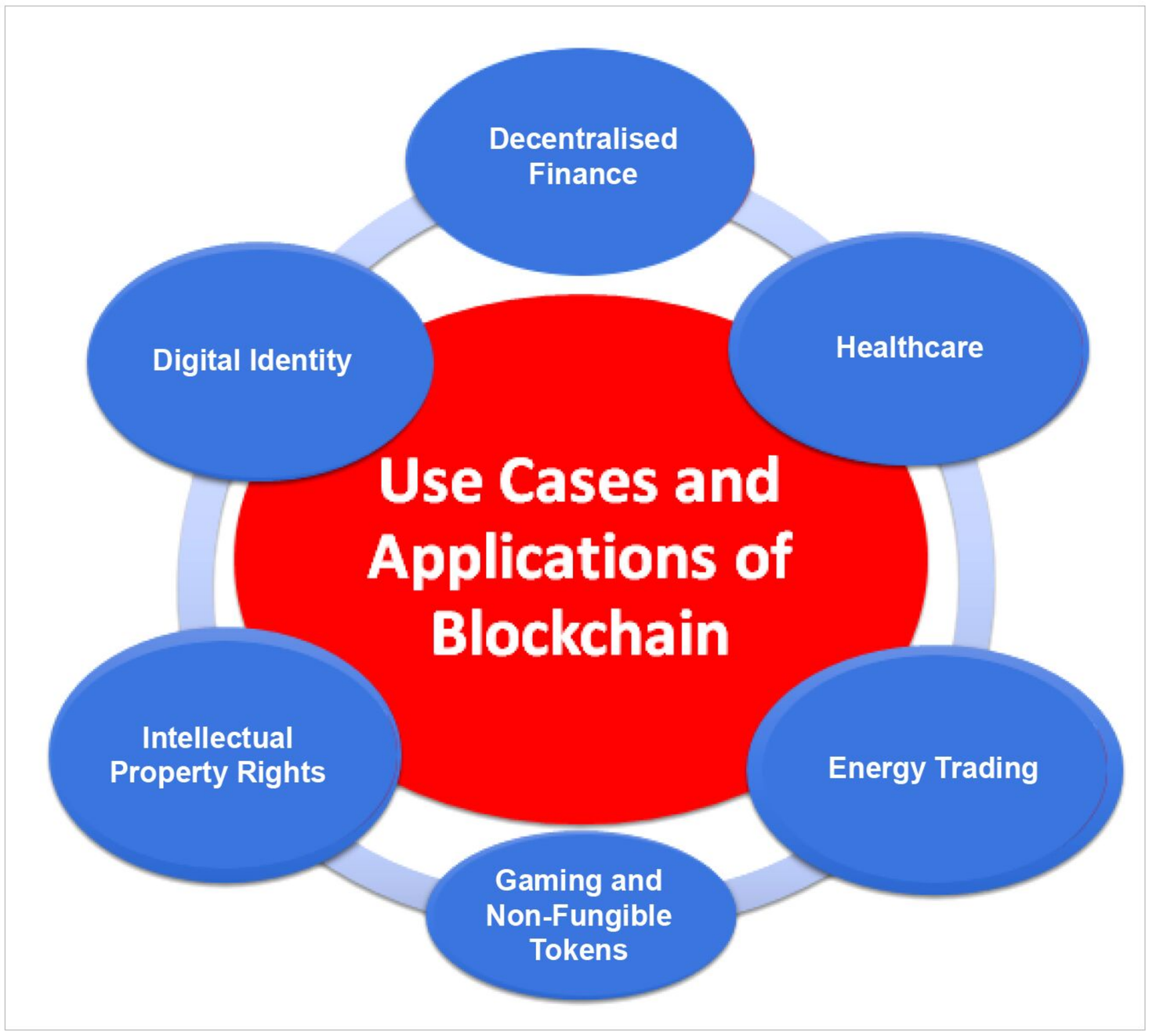


Figure 1: Key applications and use cases of blockchain

protocols. These applications enable users to engage in financial activities without intermediaries, enhancing transparency, reducing costs, and offering a wide range of financial services.

- ***Healthcare:*** Blockchain can securely store and share patients' medical records across healthcare providers. This ensures data accuracy, privacy, and reduces administrative inefficiencies. Patients have more control over their data, granting access only to authorised parties.
- ***Voting systems:*** Blockchain-based voting systems offer secure and transparent elections. Each vote is recorded as a transaction, preventing tampering and ensuring the integrity of the electoral process. This can help enhance voter trust and reduce instances of fraud. Decentralised voting systems use smart contracts to conduct transparent and tamper-resistant elections.
- ***Digital identity:*** Blockchain can create self-sovereign identities that users control. This could replace traditional identification methods, allowing individuals to manage and share their personal information securely while reducing identity theft and data breaches.
- ***Energy trading:*** Blockchain enables peer-to-peer energy trading, where individuals with solar panels can sell excess energy to their neighbours. This decentralised approach can make energy distribution more efficient and environment-friendly.
- ***Intellectual property rights:*** Blockchain can be used to prove ownership and protect intellectual property rights. Digital assets like artwork, music, and patents can be securely registered and tracked on the blockchain, preventing unauthorised use.
- ***Cross-border payments:*** Blockchain-based remittance services offer faster, cheaper, and more secure cross-border transactions. Traditional banking intermediaries are bypassed, reducing fees and delays. Smart contracts simplify cross-border transactions by automating currency exchange and payment execution. This eliminates intermediaries, reduces fees, and accelerates the transfer process.
- ***Gaming and non-fungible tokens:*** The ability of blockchain to prove ownership has led to the rise of blockchain-based gaming and digital collectibles. Players can truly own in-game assets, and unique digital items can be bought, sold, and traded securely. Smart contracts are at the heart of blockchain-based gaming and NFT platforms to enable the creation, ownership, and trading of unique digital assets.

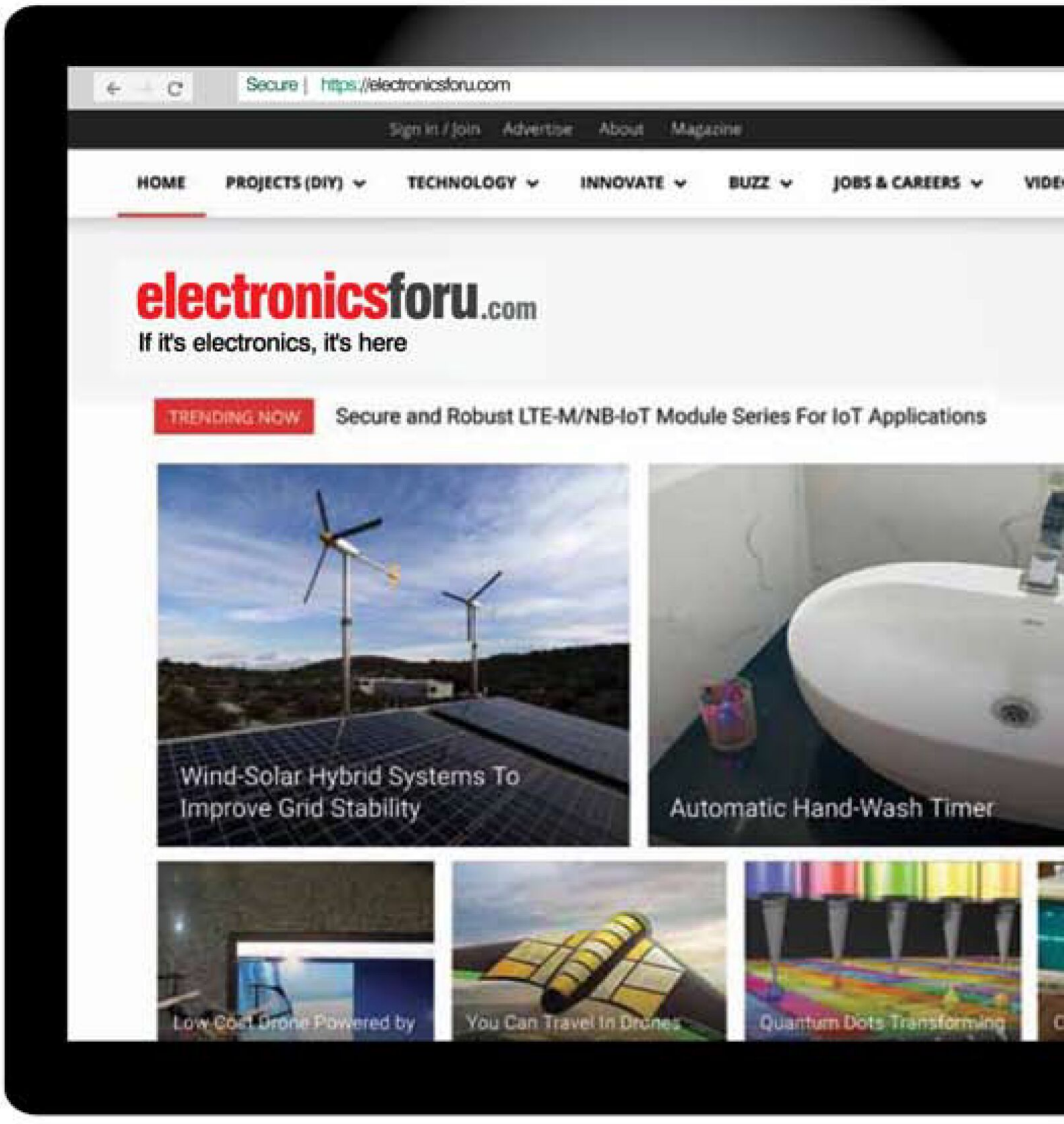
Smart contracts and decentralised applications

Smart contracts have emerged as a cornerstone of innovation within decentralised applications (DApps). The integration of smart contracts brings a multitude of benefits to various sectors, revolutionising how decentralised applications operate and interact with users.

Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They automatically execute when predefined conditions are met, reducing the need for intermediaries and streamlining processes in areas like real estate, insurance, and legal agreements.

While smart contracts offer numerous advantages, they also come with challenges, including coding vulnerabilities and legal considerations. As the technology evolves, careful planning, code auditing, and integration within a comprehensive DApp ecosystem are vital for harnessing the full potential of smart contracts.

Your favourite website has



electronicsforu.com

THANKS TO YOU—OUR ONLINE NETWORK IS

FACTS & FIGURES

- 4 websites (two more coming soon)
- Five major Facebook communities
- Seven major LinkedIN groups & pages
- Million-plus active users (monthly)
- Million-plus reach through Facebook
- Fifty-thousand-plus industry connections through LinkedIN

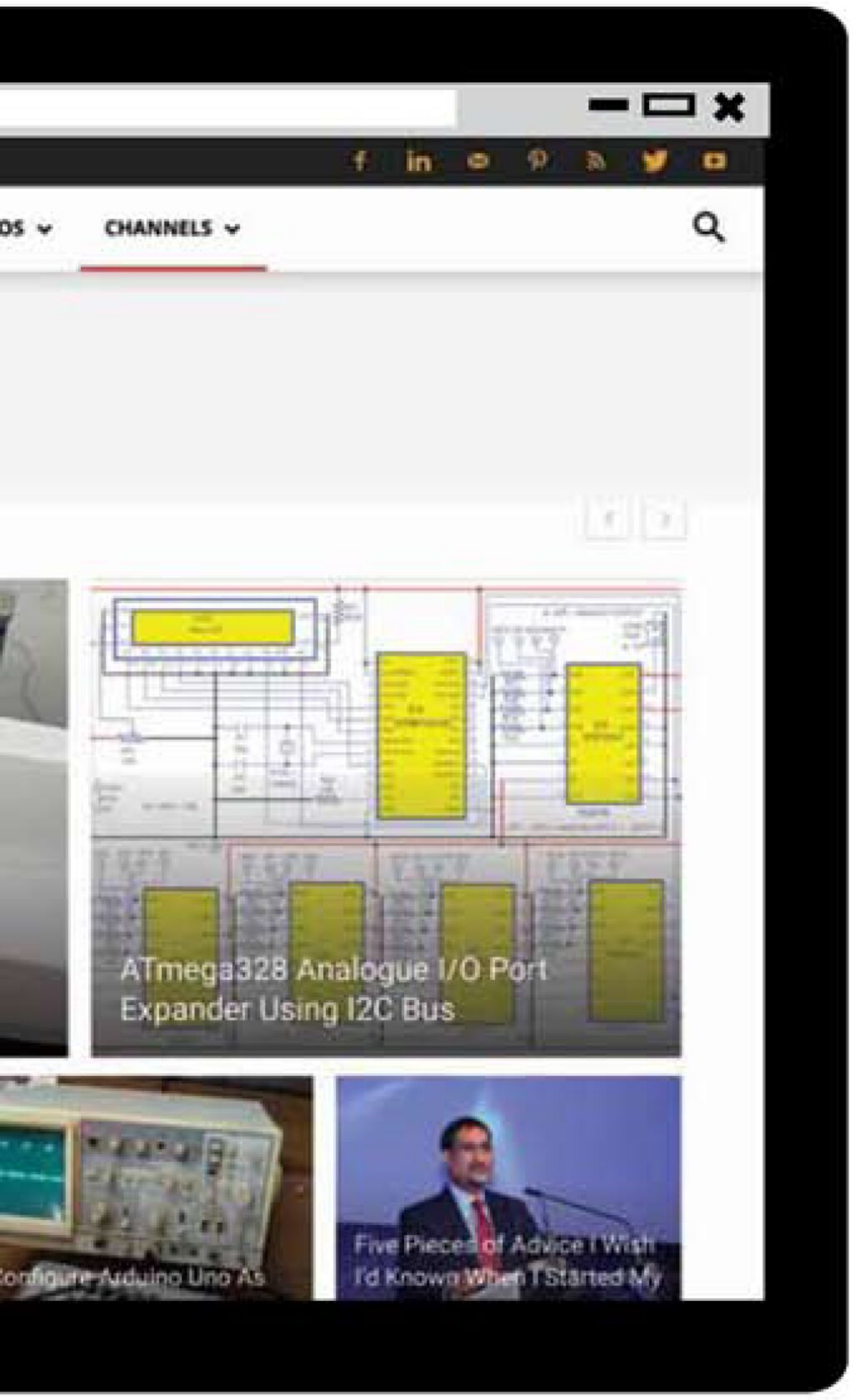
READERS

- You can access all content for FREE
- You can subscribe to newsletters for FREE --on most websites
- Register on our websites to get free invites to technical webinars and seminars

EXPERTS

- Experts who want to share their knowledge through articles, DIY Projects, etc are welcome
- We also welcome experts who want to share their knowledge through webinars or seminars
- You can contact us at editop@efy.in

fast growing peers now...





The Latest in IOT.
A platform for enablers, creators and providers of IOT solutions.



India. Electronics. Directory.
Enabling commerce between buyers & sellers of electronics in India.



Business. Electronics. India.
Everything you want to know about India's electronics industry.

Amazing DIY Projects. Latest Tech trends.

The hang-out for electronics enthusiasts.

AMONGST THE WORLD'S TOP 5 AND GROWING!

INDUSTRY

- You can advertise for as little as US$ 100 per month
- Special combo offers for advertisers in our print publications
- We've now enabled flexible CPM-based advertising
- You can advertise on the platform of your choice (based on your target audience)
- We invite press releases at efy-edit-team@efy.in
- Press releases are published free of cost, subject to discretion of the editorial team

RESPONSE GUARANTEED SOLUTIONS

We now also act as marketing partners for our clients and drive entire marketing for them, where we charge them on basis of results and not efforts!

CONTACT US: Shrikant Rao • growmybiz@efy.in • +91-98111 55335

Need for security audit and vulnerability analysis of smart contracts

Smart contracts, while offering immense potential to revolutionise industries, are not immune to vulnerabilities and flaws that can lead to significant financial losses, breaches of privacy, and disruptions of services. Conducting thorough security audits and vulnerability analyses is essential to ensure the integrity and reliability of these self-executing pieces of code. Let's find out why.

- ***Immutability of smart contract code:*** Smart contracts are designed to be immutable once deployed on the blockchain. This means that any errors or vulnerabilities present in the code can't be easily rectified without deploying a new contract. Thus, a rigorous security audit before deployment is crucial to catch and address potential issues.
- ***Financial impact:*** Many smart contracts deal with financial transactions, such as decentralised finance (DeFi) protocols and token sales. Vulnerabilities in such contracts can be exploited by malicious actors to syphon funds or manipulate the contract's behaviour, resulting in substantial financial losses.
- ***Economic incentives for hackers:*** The decentralised nature of blockchain networks and the potential for financial gain make smart contracts attractive targets for hackers. Exploiting vulnerabilities can yield significant rewards, incentivising cybercriminals to search for weaknesses.
- ***Lack of central authority:*** Traditional software development benefits from central authorities and regulatory bodies that can enforce security standards. In contrast, the decentralised and permissionless nature of blockchain means that security measures need to be embedded in the code itself.
- ***Complexity and interconnectedness:*** Smart contracts can interact with multiple other contracts and external data sources. This complexity increases the attack surface and the likelihood of unforeseen vulnerabilities emerging from interactions between different components.
- ***Inadequate testing*:** Smart contracts require specialised testing methodologies. Traditional software testing may not be sufficient due to the unique features of blockchain technology. Security audits help identify issues that might be missed by conventional testing approaches.
- ***New technology, new risks:*** Blockchain technology and smart contracts are still relatively new, and security best practices are continually evolving. Conducting regular security audits helps keep up with the latest security standards and practices.
- ***User trust*:** Users of decentralised applications rely on the security and reliability of the underlying smart contracts. Any breach or vulnerability can erode trust, causing users to lose confidence in the technology and the services built on it.
- ***Legal and reputational risks:*** Security breaches not only result in financial losses but also expose projects to legal liabilities and reputational damage. This can have long-lasting consequences on the success and adoption of the project.
- ***Preventative approach:*** A proactive approach to security, through audits and vulnerability assessments, is more cost-effective than attempting to recover from an exploit or breach after it occurs.

In short, security audit and vulnerability analysis of smart contracts is a critical component of responsible blockchain development. It safeguards the integrity of transactions, protects user assets, and upholds the reputation of projects.

There are several free and open source security audit tools available for auditing blockchain smart contracts

Table 1: Security audit tools for smart contracts

Audit tool	URL	Usage patterns
Slither	*github.com/crytic/slither*	Finds vulnerabilities in Solidity smart contracts. It offers a range of detectors for various security issues.
Mythril	*github.com/ConsenSys/mythril*	Analyses Ethereum smart contracts. Detects common vulnerabilities and provides actionable insights to improve security of contracts.
Securify	*github.com/eth-sri/securify2*	Audits Ethereum smart contracts. It uses formal verification techniques to identify security vulnerabilities and potential attack vectors.
Oyente	*github.com/melonproject/oyente*	Ethereum smart contract analyser that focuses on identifying vulnerabilities such as reentrancy attacks, transaction-ordering dependence, and more.
SmartCheck	*github.com/smartdec/smartcheck*	Static analysis tool for Ethereum smart contracts. Finds security issues by scanning the contract's source code.
Solhint	*github.com/protofire/solhint*	Enforces best practices and coding standards to improve contract security.

(Table 1). These tools help identify vulnerabilities and potential security issues in your smart contracts.

Installation and working with Slither for security audit and vulnerability testing

Slither is a powerful and versatile tool that aids in identifying vulnerabilities and improving the security of Ethereum smart contracts. Its features make it an essential component of the development toolkit for those working in the blockchain space.

Slither is an open source tool designed to analyse Ethereum smart contracts for security vulnerabilities and issues. It's widely used by developers and auditors to ensure the safety and reliability of smart contracts.

Key features of Slither

Slither is like a shield against code vulnerabilities. Let's delve deeper into some of its key features and witness how it helps secure smart contract development.

Static analysis: Slither performs static analysis on smart contracts, which means it analyses the code without executing it. This helps identify potential vulnerabilities and issues without the need to deploy the contract on the blockchain.

Vulnerability detection: One of Slither's primary functions is to detect a wide range of vulnerabilities and weaknesses in smart contracts. These vulnerabilities can include issues like reentrancy attacks, unchecked send calls, integer overflows, and more.

Custom rules: Slither allows users to define custom rules and checks that are specific to their project's requirements. This flexibility enables developers to target specific patterns or issues that might not be covered by default rules.

Integration with build process: It can be integrated into the development workflow, often as part of the continuous integration (CI) pipeline, to automatically analyse contracts whenever changes are made to the codebase. This ensures that potential issues are caught early in the development process.

Interactive reports: Slither generates comprehensive reports that detail the identified vulnerabilities and issues. The reports provide insights into the location of the issue, its severity, and possible solutions. This information assists developers in understanding and fixing the problems.

Gas estimations: For Ethereum smart contracts, gas costs are a critical consideration. Slither provides gas estimations for various execution paths within the contract, helping developers understand the potential gas expenses of their code.

Support for multiple languages: While Slither is mainly designed for Solidity, the primary programming language for Ethereum smart contracts, it also supports other languages that compile to Ethereum bytecode, such as Vyper.

Continuous updates: The tool is actively maintained by the community, which means it receives regular updates to improve its detection capabilities and support the evolving landscape of smart contract security issues.

To install Slither, use pip installer:

```
pip install slither-analyzer
```

After completing the installation, you can verify it as follows:

```
slither --version
```

Once Slither is successfully installed, it can be used to analyse Solidity smart contracts for security vulnerabilities.

For example, to analyse a Solidity file named 'MyContract.sol', you can navigate to its directory and then run:

```
slither MyContract.sol
```

Slither will analyse the contract and provide you with a report of any potential security issues it detects.

Let's say there is a Solidity smart contract named 'SimpleToken.sol':

```
pragma solidity ^0.8.0;
contract SimpleToken {
  mapping(address => uint256) public
balances;

  constructor() {
    balances[msg.sender] = 1000;
  }
  function transfer(address to, uint256
amount) public {
    require(balances[msg.sender] >=
amount, "Insufficient balance");
    balances[msg.sender] -= amount;
    balances[to] += amount;
  }
}
```

To perform an audit using Slither, follow these steps:

- Open a terminal window.
- Navigate to the directory containing your Solidity contract.
- Run Slither on your contract

```
> slither SimpleToken.sol
```

Slither will analyse your Solidity code and provide a report on the potential security issues it detects.

```
Slither static analysis report

Summary :
 High : 0
 Medium : 0
 Low : 0
 Informational : 1

Detectors :
 UninitializedState : uninitialized
state variables
  · contracts/SimpleToken.sol : L3 : 3
| SimpleToken | balances
```

In this example, Slither's uninitialised state detector detected that the balances mapping is uninitialised

in the constructor. The developer of the smart contract should initialise it properly in the constructor to avoid potential issues.

Another example code of Slither for audit of Solidity code is:

```
pragma solidity ^0.8.0;

contract Fundraiser {
  mapping(address => uint256) public
balances;

  function contribute() public payable
{
    balances[msg.sender] += msg.value;
  }
  function withdraw(uint256 amount)
public {
    require(balances[msg.sender] >=
amount, “Insufficient balance”);
    balances[msg.sender] -= amount;
    (bool success, ) = msg.sender.
call{value : amount}(“”);
    require(success, “Transfer
failed”);
  }
}
```

In the following output, Slither's 'UncheckedSend' detector detected that there is an unchecked use of the call function for sending funds. This can potentially lead to issues if the recipient of the funds is a contract with a fallback function that throws an exception or reverts. It's recommended to use the transfer function instead of a call to handle fund transfers safely.

Slither static analysis report

```
Summary :
 High : 1
 Medium : 0
 Low : 0
 Informational : 0

Detectors :
 UninitializedState : uninitialized
state variables
  · contracts/Fundraiser.sol : L3 : 3 |
Fundraiser | balances

 UncheckedSend : usage of unchecked
send
  · contracts/Fundraiser.sol : L14 : 11
| Fundraiser | call()
```

With the growing adoption of blockchain across industries, ensuring the robustness and security of smart contracts is crucial. Researchers can explore advanced vulnerability detection methods, automated fingerprinting of vulnerabilities, and integration of AI and machine learning to enhance accuracy. Addressing scalability challenges, real-time monitoring, regulatory compliance, privacy-enhancing techniques, and community engagement through bug bounties are pivotal areas of focus. This will help establish secure and resilient blockchain ecosystems that drive innovation and inspire trust. END

By: Dr Gaurav Kumar

The author is associated with various academic and research institutes for delivering expert lectures and conducting technical workshops on the latest technologies and tools.

Continued from page...65

The essence of open source is collaboration, and the blockchain sphere thrives on it. Developers from across the globe contribute to projects, resulting in innovative features, robust security, and rapid iterations. Take Bitcoin, for instance. Its codebase is open for anyone to review and propose changes. This collaborative approach has led to various implementations, each catering to specific needs. Such vibrant ecosystems exemplify the power of collective expertise.

Challenges and the future of blockchain

While open source and blockchain create a harmonious symphony, challenges persist. Scalability, interoperability between different blockchains, and governance are areas that demand careful navigation. Additionally, as blockchain evolves, it intersects with emerging technologies like the Internet of Things (IoT), forging novel possibilities. The future beckons towards a more interconnected and efficient world.

Consider the healthcare sector. Integrating blockchain with IoT devices can create a network where patients' medical data is securely stored and shared with healthcare providers. This ensures accurate and real-time patient records, streamlining treatment processes and minimising errors.

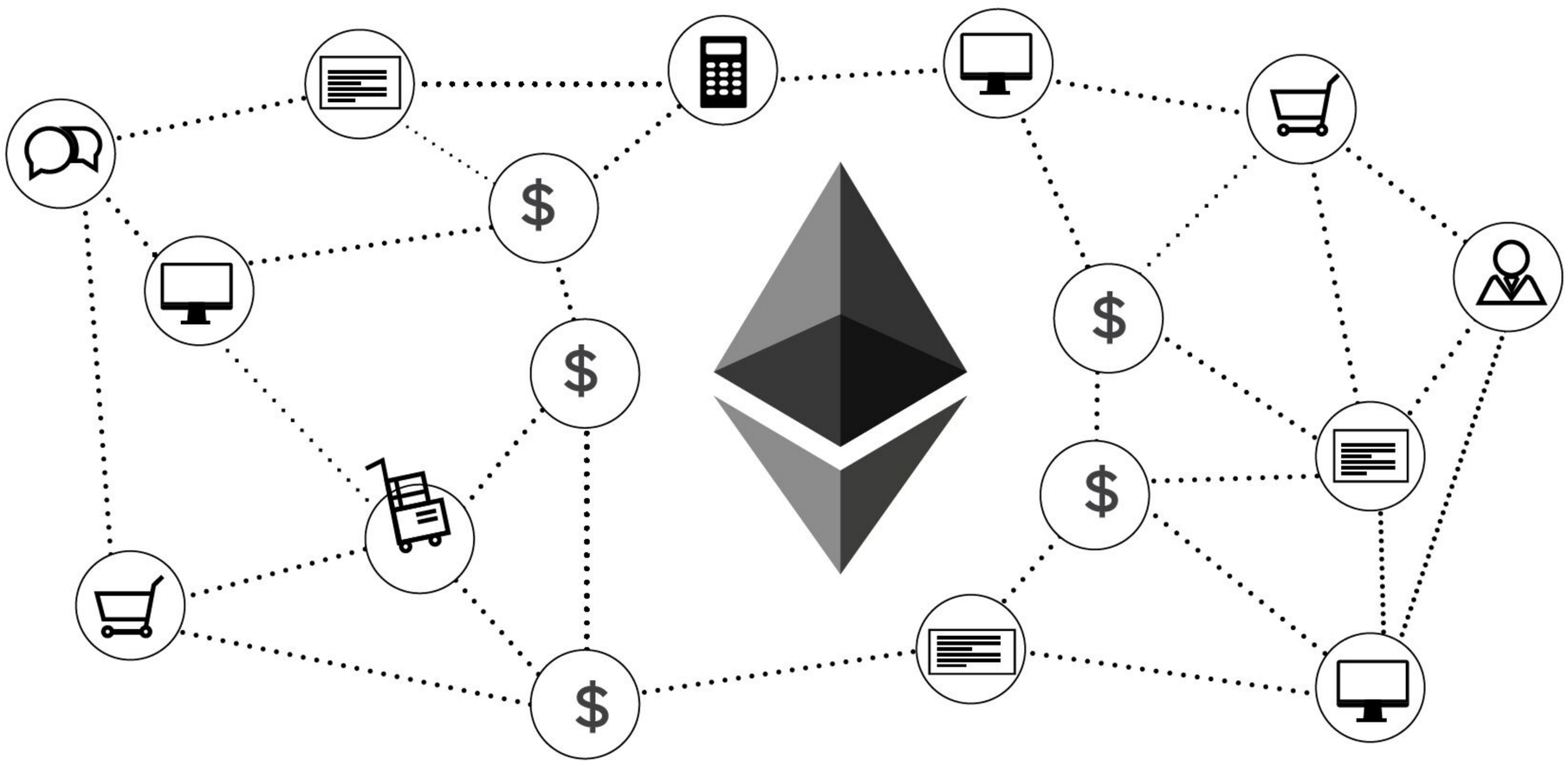
Blockchain technology, with its potential to redefine trust, transparency, and security, finds its perfect ally in open source philosophy. Innovation flourishes when barriers are torn down and knowledge is shared openly. With every block added to the chain and every line of open source code contributed, we take strides towards a decentralised, collaborative future—one where technology serves humanity in ways we're just beginning to comprehend. END

By: Meghraj Singh Beniwal

The author is the founder of Schooling for Next Generation, a tech enthusiast and Android hobbyist. He is a test automation analyst working in Virginia in the US.

The Role of Ethereum in Advancing Open Source Blockchain Technology

Ethereum's journey embodies the essence of open source development in blockchain. Its impact is undeniable, inspiring global innovation and shaping the ethos of decentralised collaboration. Its legacy illuminates the boundless potential of open source blockchain technology.



In a world of innovation, open source blockchain technology knows no limits. Let's explore Ethereum's transformative journey, revealing the core principles that fuel its groundbreaking role. This expedition offers profound insights into Ethereum's influence on the wider blockchain ecosystem and a glimpse into the uncharted territories of open source blockchain technology.

The significance of open source development in blockchain

Before diving into Ethereum's remarkable journey, it's essential to recognise the profound significance of open source development in the blockchain industry. Open source principles are the lifeblood of blockchain innovation. They enable diverse communities of developers, researchers, and enthusiasts to come together, collaborate, and collectively drive the development of blockchain projects. The power of open source lies in its transparency, inclusivity, and the accelerated pace of innovation it fosters. In the context of blockchain, these principles empower the creation of decentralised, trustless networks poised to disrupt a myriad of industries.

Ethereum's role in advancing open source blockchain technology

Ethereum has played a transformative role in advancing open source blockchain technology. At its core, Ethereum introduced the concept of smart contracts, revolutionising how transactions and agreements are executed. These self-executing contracts automate processes, reducing the need for intermediaries and enhancing trust in digital transactions. Ethereum's commitment to open source development further reinforces its impact. Its transparent codebase invites global participation, fostering a diverse community of developers and advocates. Ethereum improvement proposals (EIPs) provide a structured framework for collaborative innovation, ensuring that the platform evolves with input from all stakeholders.

Beyond its platform, Ethereum's influence resonates across the blockchain space. Decentralised finance (DeFi) and non-fungible tokens (NFTs) have thrived on Ethereum, reshaping financial services and ownership. Ethereum's DeFi and NFT ecosystems have expanded the horizons of blockchain applications, showcasing its far-reaching impact. Additionally, Ethereum's prominence has accelerated the

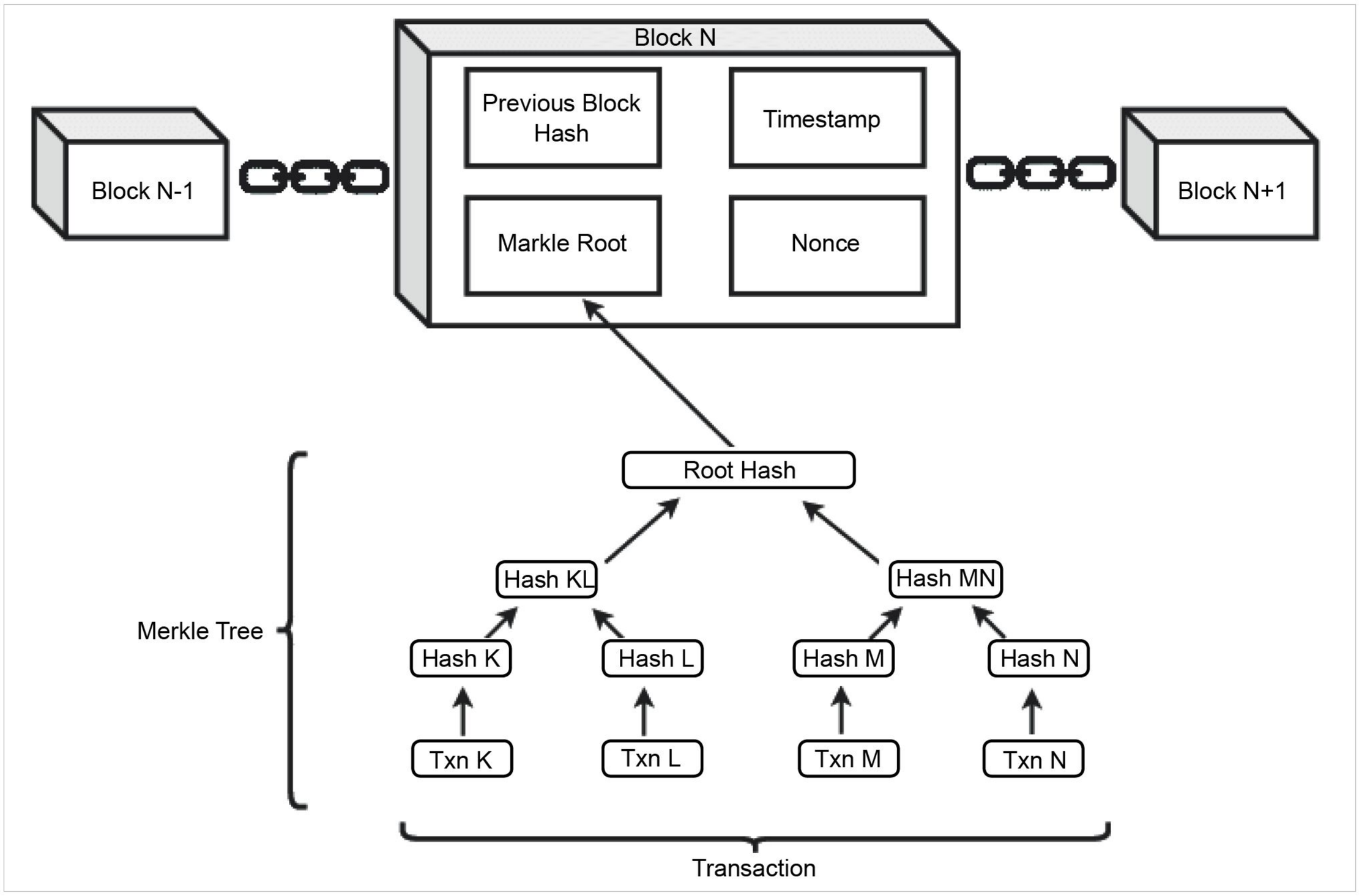


Figure 1: Structure of an Ethereum blockchain (Credit: *researchgate.net*)

development of interoperability solutions, bridging different blockchains and promoting seamless asset transfers.

The genesis of Ethereum

Ethereum traces its origins to the visionary mind of Vitalik Buterin in 2013. Recognising the limitations of Bitcoin, Buterin penned the Ethereum whitepaper, envisioning a blockchain that could go beyond mere digital currency. He visualised a versatile and open platform that could support smart contracts and a wide array of decentralised applications.

Buterin's vision ignited a call to action, rallying a global community of developers, including figures like Gavin Wood and Joseph Lubin, who shared his belief in Ethereum's potential. In 2015, Ethereum's genesis block marked the official beginning of a new era in blockchain technology, where developers could build decentralised applications that extended far beyond the boundaries of digital currency. This genesis moment unleashed a wave of innovation and inspired a worldwide movement.

The genesis of Ethereum serves as a testament to the power of visionary thinking, open source collaboration, and the boundless possibilities of blockchain. It not only birthed a blockchain but sparked a global movement, inspiring developers, entrepreneurs, and blockchain enthusiasts to reimagine what decentralised technology could achieve. Ethereum's journey from a whitepaper to a thriving ecosystem is a testament to the enduring impact of bold ideas and the transformative potential of blockchain technology on a global scale.

Ethereum's open source philosophy

Ethereum's foundation is built upon a bedrock of open source philosophies. From its inception, Ethereum championed transparency, collaboration, and community involvement as fundamental tenets. The source code of Ethereum's client software, such as Geth and Parity, is accessible to the public, inviting scrutiny and contributions from developers worldwide. This unwavering commitment to transparency ensures the Ethereum network remains secure and free from hidden vulnerabilities.

However, Ethereum's dedication to open source transcends mere code accessibility. It fosters a global community of developers and advocates who work harmoniously to continually enhance the platform. This community values inclusivity, welcoming developers of all backgrounds to contribute their expertise to the network's growth. It is this spirit of collaboration that defines Ethereum's open source philosophy.

Ethereum's contribution to the blockchain space is perhaps most profound in the realms of smart contracts and decentralised applications (DApps). These innovations have not only redefined how we interact with blockchain but have also democratised access to decentralised technology.

Smart contracts

Ethereum introduced the groundbreaking concept of smart contracts. These self-executing contracts are coded agreements with the terms and conditions directly written into the blockchain. Unlike traditional contracts, smart contracts automatically execute actions when predefined conditions are met, without the need for intermediaries. Ethereum's innovation was to make smart contracts a fundamental part of its blockchain, thus enabling decentralised, trustless agreements.

```
// Example of a simple Ethereum smart contract
// This contract allows two parties to enter into a bet, and
the winner receives the funds

pragma solidity ^0.8.0;

contract SimpleBet {
    address public player1;
    address public player2;
    bool public isGameFinished;

    constructor() {
        player1 = msg.sender;
        isGameFinished = false;
    }
    function enterGame() public payable {
        require(msg.sender != player1 && !isGameFinished,
"Invalid entry");
        player2 = msg.sender;
    }
    function finishGame(address winner) public {
        require(msg.sender == player1 || msg.sender ==
player2, "Not a participant");
        require(!isGameFinished, "Game already finished");
        payable(winner).transfer(address(this).balance);
        isGameFinished = true;
    }
}
```

Development of DApps

Ethereum's open source framework provided the fertile ground necessary for the development of DApps. These applications run on the Ethereum blockchain, utilising smart contracts for various purposes, including financial services, gaming, supply chain management, and more. Ethereum's open source nature, along with the accessibility of its code and development tools, lowered the entry barriers for developers worldwide.

Developers could leverage Ethereum's open source codebase to create DApps that could interact with smart contracts seamlessly. Ethereum's decentralised and transparent infrastructure allowed for innovative solutions to be built on top of it, disrupting traditional industries and paving the way for a new wave of decentralised services.

```
// Example of a simple decentralized application (DApp)
interacting with an Ethereum smart contract using Web3.js

const Web3 = require('web3');
const web3 = new Web3('https://mainnet.infura.io/v3/YOUR_
INFURA_PROJECT_ID');

const contractAddress = '0xYourSmartContractAddress';
const contractABI = [...]; // ABI of your smart contract

const contract = new web3.eth.Contract(contractABI,
contractAddress);

async function placeBet() {
    // Interact with the smart contract to place a bet
    await contract.methods.enterGame().send({ from:
'0xYourAccountAddress', value: web3.utils.toWei('1', 'ether')
});
}
async function declareWinner() {
    // Interact with the smart contract to declare a winner
    await contract.methods.finishGame('0xWinningPlayerAddre
ss').send({ from: '0xYourAccountAddress' });
}
```

Ethereum as a platform for innovation

Ethereum has served as a fertile breeding ground for a multitude of innovative projects and solutions within the blockchain ecosystem. Noteworthy endeavours like MakerDAO, Uniswap, and CryptoKitties have thrived on the Ethereum platform. These projects have redefined financial services, decentralised exchanges, and digital collectibles, demonstrating the versatility and potential of blockchain technology.

Ethereum's open source nature has encouraged developers to push the boundaries of what is possible. The platform's extensible architecture and active development community have created an environment where experimentation and innovation flourish, driving the blockchain industry forward.

Open source development on Ethereum

A defining characteristic of Ethereum is its decentralised development community. The Ethereum ecosystem does not discriminate; it embraces the contributions of anyone with the passion and skills to participate in its growth. This inclusivity

is a testament to Ethereum's unwavering commitment to open source principles, where the best ideas rise to the top, regardless of their origin.

Ethereum improvement proposals (EIPs) provide a structured framework for proposing and discussing changes to the Ethereum network. This open dialogue ensures that all stakeholders have a voice in shaping the platform's future, fostering a sense of ownership and collective responsibility among the Ethereum community.

Challenges and solutions

Ethereum's open source journey has been marked by innovation and adaptability in the face of significant challenges. Here, we address some key challenges Ethereum has encountered and the inventive solutions it has embraced.

Scalability challenge: Ethereum faced scalability issues due to increased usage, leading to slow transaction confirmations and high gas fees.

Solution: Ethereum 2.0 (Eth2) is a comprehensive solution, transitioning from proof of work (PoW) to proof of stake (PoS) to increase scalability. Shard chains enable parallel processing, alleviating scalability concerns.

High gas fees challenge: Surging demand resulted in high gas fees, hindering user and developer interactions.

Solution: Layer 2 scaling solutions, like Optimistic Rollups and zk-Rollups, offer cost-effective off-chain processing while maintaining mainnet security.

Network congestion challenge: Network congestion led to slow transactions, impacting user experience.

Solution: Eth2 and shard chains distribute transactions, reducing mainnet congestion for smoother performance.

Security and scalability balance challenge: Balancing security and scalability was complex, with some solutions posing security risks.

Solution: Eth2 seeks to balance security and scalability by transitioning to PoS, enhancing security, and introducing shard chains for scalability.

Compatibility and transition challenge: Transitioning to PoS while maintaining compatibility was challenging.

Solution: Tools and bridges are being developed to facilitate a smooth transition from PoW to PoS, ensuring application and asset migration.

Developer experience challenge: Complex development and high gas costs affected developer productivity.

Solution: Initiatives like the Ethereum Developer DAO, Layer 2 solutions, and sidechains enhance the developer experience.

Adoption and education challenge: Widespread adoption and education on blockchain technology remained a challenge.

Solution: Educational initiatives, hackathons, and developer support foster understanding and adoption of blockchain technology.

Ethereum 2.0: A leap forward

Ethereum 2.0 marks a monumental leap forward in Ethereum's mission to advance open source blockchain technology. This comprehensive upgrade is designed to tackle some of the most pressing issues that Ethereum has faced. By transitioning to PoS and implementing shard chains, Ethereum 2.0 promises to deliver heightened scalability, reduced energy consumption, and enhanced network security. It represents Ethereum's commitment to continuous improvement and innovation.

Ethereum's impact on the wider blockchain ecosystem

Ethereum's open source model has acted as a catalyst for innovation within the broader blockchain ecosystem. Its influence can be observed in several key ways.

- ***Transparency and trust:*** Ethereum's commitment to open source development has established a foundation of transparency and trust. This ethos has encouraged other blockchain projects to adopt similar principles, enhancing their credibility within the community.
- ***Collaborative ethos:*** Ethereum's vibrant and collaborative community has inspired developers and teams from other blockchain projects to embrace open collaboration. The spirit of working together, sharing knowledge, and building on each other's successes has become a hallmark of Ethereum's influence.
- ***Cross-pollination of ideas:*** Ethereum's groundbreaking concepts, such as smart contracts and decentralised applications (DApps), have sparked a wave of innovation throughout the blockchain space. Many projects have drawn inspiration from Ethereum's success and incorporated similar functionalities into their own platforms.
- ***DeFi and NFT proliferation:*** Ethereum's DeFi and NFT ecosystems have had a profound impact on the blockchain industry. Other projects have followed suit, creating decentralised financial solutions and digital assets marketplaces, and expanding the possibilities for blockchain applications.
- ***Interoperability initiatives:*** Ethereum's prominence has accelerated the development of interoperability solutions. Projects like Polkadot, Cosmos, and Aion aim to bridge the gap between different blockchains, enabling seamless asset transfers and collaboration between ecosystems.
- ***Decentralised governance:*** Ethereum's experiments with decentralised governance, as seen through proposals and decisions made by the Ethereum community, have inspired other projects to explore similar governance models. This has led to the democratisation of decision-making within blockchain communities.
- ***Global innovation hub:*** Ethereum has become a global epicentre for blockchain innovation. Its open source

framework invites developers from diverse backgrounds to participate, resulting in a rich tapestry of blockchain applications, protocols, and experiments.

The future of Ethereum and open source blockchain

The future of Ethereum and open source blockchain technology holds immense promise and potential. As Ethereum 2.0 continues to roll out and mature, it is poised to become an even more scalable and sustainable blockchain platform.

- ***Ethereum 2.0 evolution:*** Ethereum 2.0, with its transition to proof-of-stake (PoS) consensus, shard chains, and improved scalability, promises a more efficient and eco-friendly blockchain. This evolution will enable Ethereum to process a higher number of transactions per second, reducing congestion and lowering energy consumption.

```
// A simple Solidity smart contract example
// This contract allows users to store and retrieve data on
the Ethereum blockchain

pragma solidity ^0.8.0;

contract StorageContract {
    string private data;

    function storeData(string memory _data) public {
        data = _data;
    }

    function retrieveData() public view returns (string
memory) {
        return data;
    }
}
```

- ***Decentralised finance (DeFi) growth:*** DeFi, built predominantly on Ethereum, is likely to continue its explosive growth. Ethereum's role as the backbone of DeFi applications will drive financial innovation, potentially reshaping traditional finance systems.

```
// A simple JavaScript example of interacting with a DeFi
smart contract on Ethereum using Web3.js

const Web3 = require('web3');
const web3 = new Web3('https://mainnet.infura.io/v3/YOUR_
INFURA_PROJECT_ID');
const contractAddress = '0xYourContractAddress';
const contractABI = [...]; // ABI of your DeFi smart contract
const contract = new web3.eth.Contract(contractABI,
contractAddress);

async function checkBalance(accountAddress) {
    const balance = await contract.methods.
balanceOf(accountAddress).call();
    console.log(`Account balance: ${balance} tokens`);
}
checkBalance('0xYourAccountAddress');
```

- ***Non-fungible tokens (NFTs) expansion:*** NFTs, which have gained mainstream attention, will continue to flourish on Ethereum. The platform's infrastructure will support the creation and trading of unique digital assets across various industries, from art and gaming to real estate.

```
// A simple Solidity smart contract example for creating an
NFT on Ethereum

pragma solidity ^0.8.0;

import "@openzeppelin/contracts/token/ERC721/extensions/
ERC721Enumerable.sol";
import "@openzeppelin/contracts/access/Ownable.sol";
contract MyNFT is ERC721Enumerable, Ownable {
    using SafeMath for uint256;
    using Address for address;

    constructor() ERC721("MyNFT", "NFT") {}

    function mint(address to, uint256 tokenId) public
onlyOwner {
        _mint(to, tokenId);
    }
}
```

In conclusion, Ethereum's remarkable journey from its inception to its current status as a groundbreaking open source blockchain platform exemplifies the pivotal role of open source development in the blockchain industry. Its unyielding commitment to transparency, collaboration, and innovation has not only transformed the blockchain landscape but has also inspired countless developers and projects worldwide. Ethereum is a shining beacon of open source collaboration in the blockchain space, shaping the future of decentralised innovation and offering a glimpse into the boundless possibilities of open source blockchain technology. END

By: Dhaval Gajjar

The author is the CTO of Textdrip and the CEO of Pranshtech Solutions and WeTechnolabs Solutions. With a passion for technology and innovation, he explores the ever-evolving world of digital solutions, sharing insights and expertise to drive progress in the tech industry.

The Blockchain and its Many Uses

The potential for increased security, efficiency, and transparency that blockchain offers is too significant to ignore. It is evolving and disrupting traditional systems, proving that it has real industry altering powers.



Blockchain is a disruptive technology that digitises, decentralises, secures and incentivises the validation of transactions across industries. This technology has the potential to improve security, processes and systems in every domain where accurate, tamper-proof record-keeping is essential.

Trust: Blockchain is a decentralised, peer-to-peer network that records transactions to blocks, which are written to the distributed ledger based on consensus between all the participants in the network. The ledger is distributed to all the nodes and is not centralised. These factors foster trust among the participants.

Transparency: The data recorded on the blockchain ensures all the participants in the network have the distributed ledger copy; no party can maliciously change the data in the ledger, as the transaction is committed to the blockchain once all parties come to a consensus (based on applicable consensus algorithm).

Elimination of intermediaries: Blockchain technology eliminates the need for intermediaries. Once blockchain technology is adopted, consensus algorithms transparently record and verify transactions, eliminating the need for manual verifications by any third party. Cryptography helps in eliminating third-party intermediaries as keepers of trust.

Automation: With transactions executing almost immediately and significantly reducing the processing times (sometimes from days to hours), old time-consuming processes are replaced by automated verification and validation.

Key characteristics of blockchain technology

- ***Digital:*** Digitises all the information on the blockchain, thus eliminating the need for manual documentation.
- ***Distributed:*** Blockchain distributes control among all peers in the transaction chain, creating a shared infrastructure within an enterprise system. Participants independently validate information without centralised authority. There is no single point of failure because of distributed system operation. Even if one node fails, the remaining nodes continue to operate, ensuring no disruption.
- ***Immutable:*** All the transactions are immutable in the blockchain. Encryption is done for every transaction covering time, date, participants, and hash to the previous block.

- ***Chronology:*** Each block acts like a repository that stores information pertaining to a transaction, and links to the previous block in the same transaction. These connected blocks form a chronological chain providing a trail of the underlying transaction.
- ***Consensus based:*** A transaction on the blockchain is executed only if all the parties on the network unanimously approve it. Consensus-based rules can be altered to suit various circumstances.
- ***Digital signature:*** Blockchain enables exchange of transactional values using unique digital signatures that rely on public keys. Public keys are decryption code known to everyone on the network. Private keys are codes known only to the owner to create proof of ownership. This is very critical to avoid fraud in records management.
- ***Consistent:*** Blockchain data is complete, consistent, timely, accurate, and widely available.
- ***Persistence:*** No invalid transactions are admitted. It is nearly impossible to delete or roll back transactions once they are included in the blockchain. Cryptographically, the blocks created are sealed in the chain. It is impossible to delete, edit or copy already created blocks and put them on the network. This ensures a high level of robustness and trust.
- ***Anonymity:*** Each user can interact with the blockchain with a generated address, which does not reveal the real identity of the user.

Principles of blockchain

- ***Integrity:*** Blockchain technology uses a distributed verification system for transactions that does not centralise power. Integrity is required during the decision rights of blockchain users and a network's incentive structures. The use of complex algorithms and consensus among users ensures that once agreed upon, there is no tampering with transaction data. Data stored on blockchain acts as a single version of truth for all parties involved, reducing the risk of fraud.
- ***Decentralisation:*** Blockchain distributes power among different members. This means no single person or system can ever tamper with it. It is robust and resistant to attacks and fraud due to a distributed power system.
- ***Peer-to-peer:*** All blockchain transactions are peer-to-peer. This means that at least two parties are involved. The best way to understand this is to compare a standard credit card transaction with the first practical use of blockchain. The benefits of the peer-to-peer aspects of the blockchain are that the two people involved in a transaction can both verify if the transaction is correct, without the need for any other party to be involved.
- ***Cryptographic system:*** Blockchain lends its cryptography a level of authenticity and integrity.
- ***Equal rights:*** Rights are reserved in a transparent manner. Blockchain users know exactly what rights they are entitled to and that they are equal and fair in the best way possible.

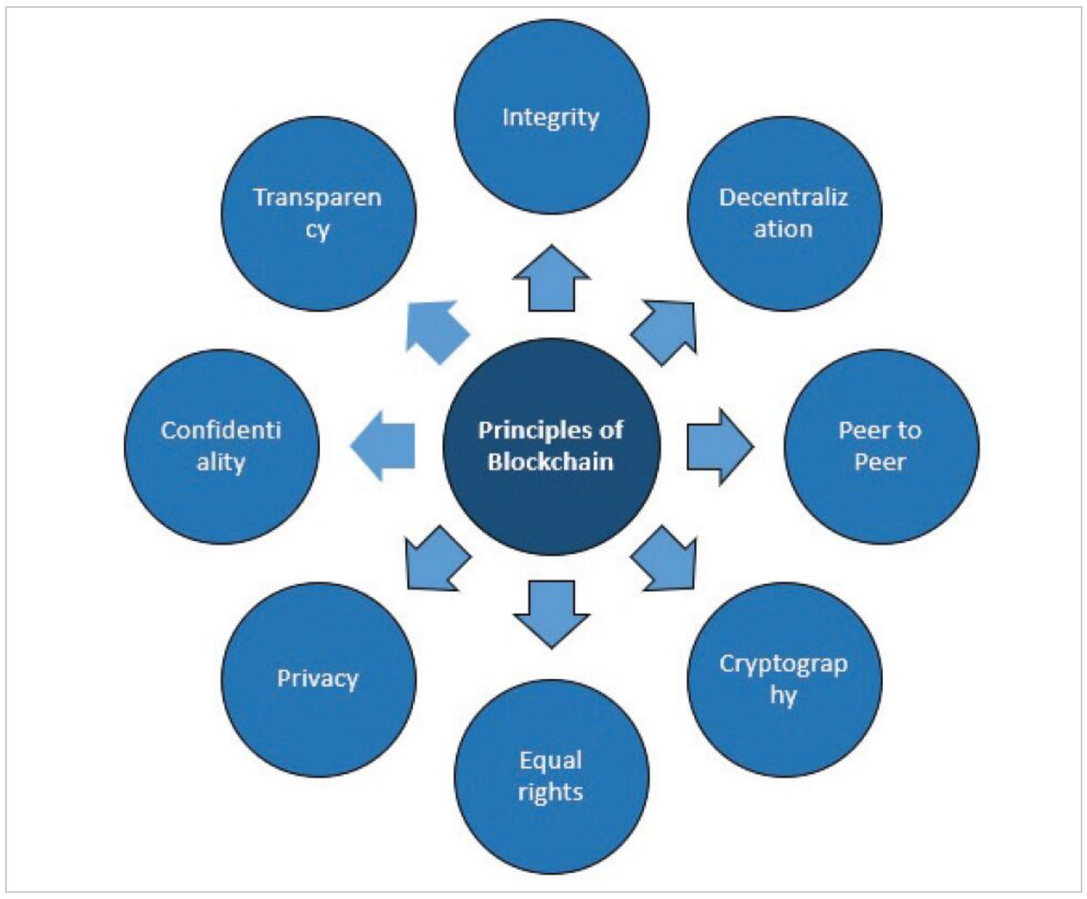


Figure 1: Principles of blockchain

- ***Privacy:*** Blockchain establishes a separate virtual identity for its users to protect their privacy, both online and offline. The identity uses a series of numbers, much like code, that are difficult to profile. Hence, blockchain fosters trust by eliminating the need for any real (or seemingly real) identity. It protects the identity of its users so that they can participate in the digital economy freely and fairly with integrity.
- ***Confidentiality:*** Blockchain provides confidentiality by enabling users of a ledger to see authorised transactions only.
- ***Transparency:*** Blockchain shares the ledger to all nodes and uses consensus algorithms to reach consensus among them. Consensus algorithms also ensure the ordering and execution of the transactions.

Figure 2 shows the logical application architecture of the blockchain system with key components and layers.

Blockchain services layer acts as a gateway for reaching out to the blockchain infrastructure. It consists of various services related to identity management, key management, cryptography, machine learning (ML) and business intelligence (BI). Identity, key, and cryptographic services are critical for data integrity. BI and ML are used for analysis and reporting purposes.

Distributed ledger stack consists of the core distributed ledger technology stack. Blockchain building, transaction execution and consensus happen in this layer. The components in this stack may vary depending on the distributed ledger product chosen. However, the common sub-components are consensus algorithms, data storage, and transactions management and other relevant services.

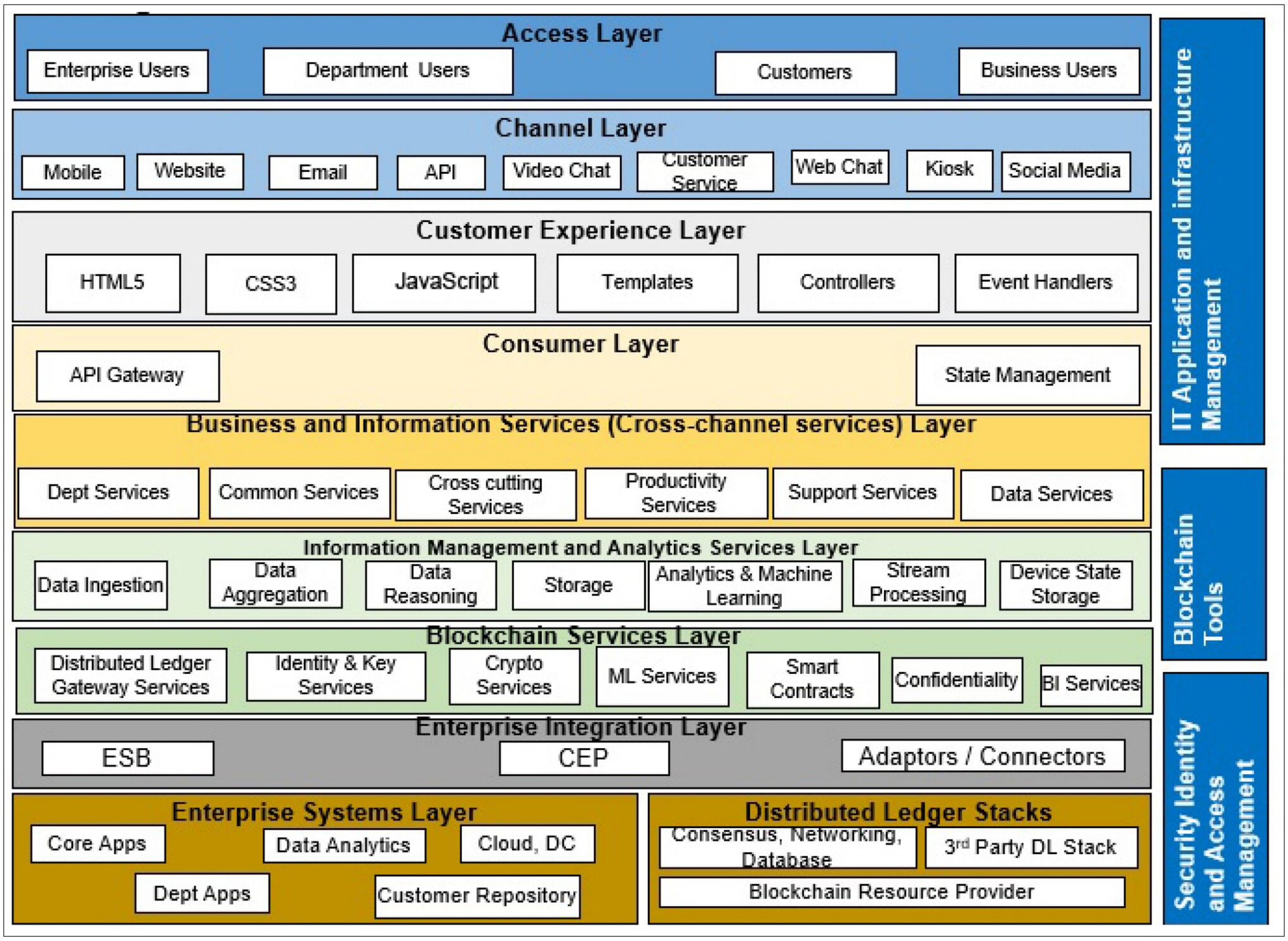


Figure 2: Blockchain logical reference architecture

Real world use cases of blockchain technology

Government

In government, linking the data between various departments with blockchain ensures that the data is realised in real-time. Blockchain technology could improve transparency and check corruption in governments worldwide.

- ***Registration:*** By securing a unique and non-corruptible record on a blockchain and validating changes to the status of that record across owners, a reliable property record can be created, whether for a piece of land that heretofore had no owner or as a link between stovepiped systems. A decentralised, standardised system for land registration records could reduce the number of intermediaries required, increase trust in the identity of transacting parties, increase process efficiencies, and decrease time and cost to process.
- ***Election:*** Citizens can cast votes the same way they initiate other secure transactions and validate that their votes were cast—or even verify the election results. Solutions are being worked on to blend secure digital identity management, anonymous vote-casting, individualised ballot processes, and ballot casting confirmation verifiable by the voter. Potential cost savings can be achieved through blockchain-enabled voting.
- ***Finance:*** Online identity has always been a time-consuming and costly process. Financial services like loans, mortgages, and insurance have always required a higher level of security, checking, authentication and authorisation. This meant that checking official government identity documents was a required step. One of the benefits of the blockchain is that it has the potential to cut out the intermediaries and provide every organisation/department in the network access to the same source of the right information. Blockchain technologies make tracking and managing digital identities secure and efficient, resulting in reduced fraud. Users are able to choose how they identify themselves and with whom their identity is shared.
- ***Town planning:*** Having property records on the blockchain makes it possible that prospective buyers shall

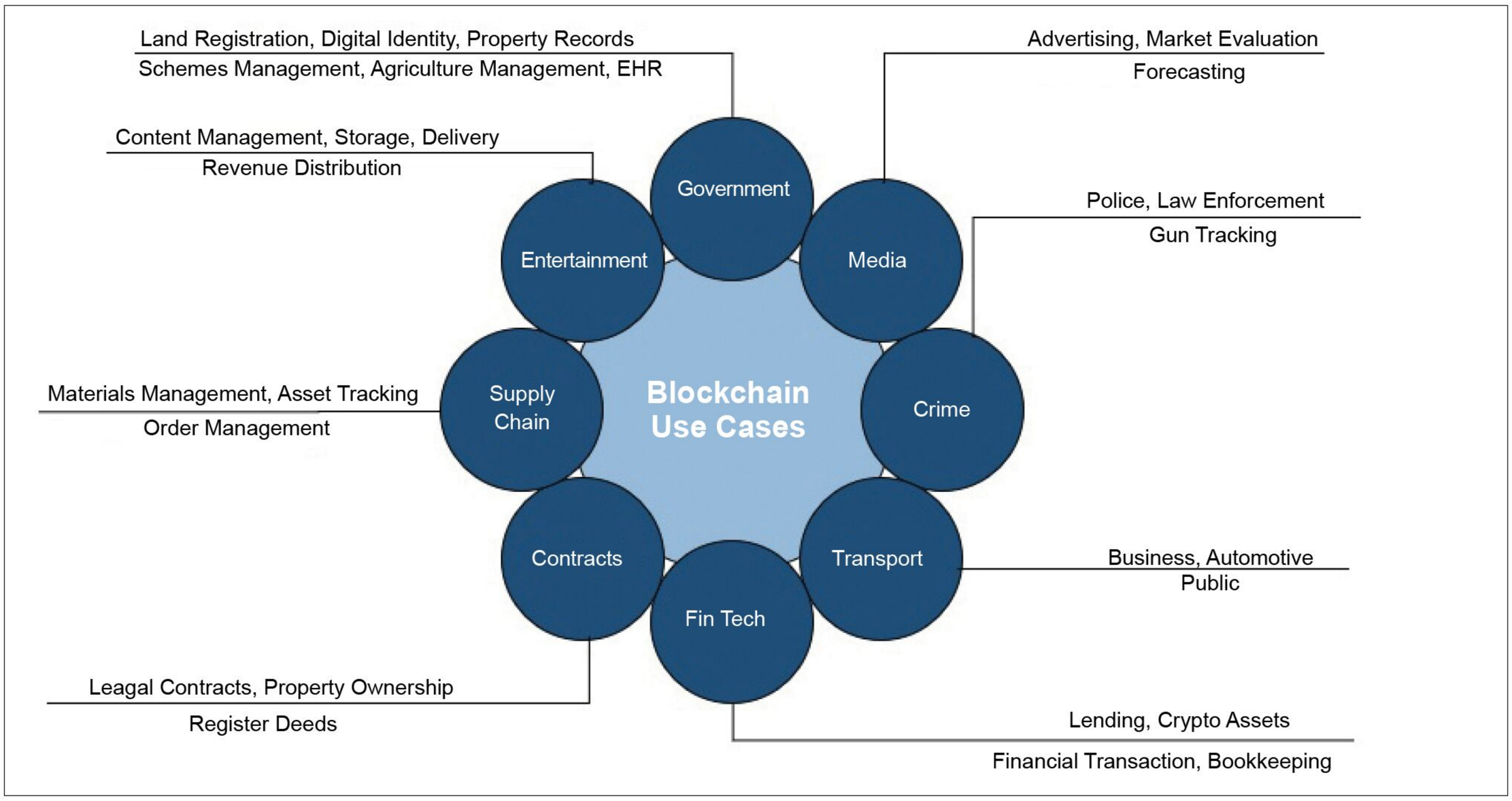


Figure 3: Blockchain use cases

verify the owner of a house quickly and easily.

- ***Revenue:*** Blockchain enables seamless cross-referencing of documentation across multiple government entities. All documentation is automatically verified by the relevant entities. The inherent features of blockchain (digital identity) make it impossible to make changes to the ledger.
- ***Managing entity:*** Business unit incorporation and governance is possible with the use of digital signatures and programmable business rules. It also enables approvals and validations of the entity and its application on the blockchain. The distributed ledger technology (DLT) allows multiple parties to digitally sign for authorisation and approve a transaction and documents.
- ***Grants:*** An integrated blockchain solution enables seamless customer onboarding with automated disbursements of loans and grants. Transactions on the ledger are auditable in real-time providing greater transparency for regulators. Highly secured digital signatures make sure transactions get executed only when the relevant entities provide their signature.
- ***Agriculture:*** Integrated agriculture management system (IAMS) with a blockchain infrastructure ensures immutability of data and a way to trace historical agricultural data, as agricultural products move from production sources to the consumer. IAMS with a blockchain infrastructure helps diversify current agricultural management practices in a way that engages the public through ownership of the agricultural production process. Other possible applications include the use of blockchain technology to record and manage agricultural land records as well as agriculture insurance.
- ***Healthcare:*** Digitisation of health records is a significant task in the public health sector, which is huge, complex and associated with ethical issues. Medical records are scattered and erroneous, with inconsistent data handling processes. Sometimes, hospitals and clinics are forced to work with incorrect or incomplete patient records. Blockchain technology can help create a secure and flexible ecosystem for exchanging a patient's electronic health records. This technology can also make the space more transparent by creating a basis for critical drugs, blood, organs, etc. In addition, by putting all medical licences on a blockchain, fraudulent medical practitioners can be prevented from practising, and chemists can be prevented from selling spurious drugs.
- ***Education:*** Student records, faculty records, educational certificates, etc, are key assets in the education domain and are shared with multiple stakeholders; so it is imperative to ensure that they are trustworthy. All these records can be maintained with the application of blockchain technology. Blockchain can also simplify certificate attestation and verification.

Media

Media is a multi-billion dollar industry that is evolving every year. However, it is currently not consumer- or creator-friendly due to intermediaries taking advantage and making tons of revenue in the process. With blockchain, the

whole landscape can change and become more accessible to consumers as well as content creators.

Advertising: Advertisers can use blockchain to place their ads and earn revenue in millions of dollars. With blockchain-powered browsers, it is now possible for consumers to turn off the advertising and protect their privacy at the same time.

Market evaluation/forecasting: Blockchain can speed up market forecasting to an entirely new level, as it can hold a massive amount of data that can be used in conjunction with machine learning or artificial intelligence.

Crime management

Blockchain can help enforce the law and ensure that crime remains at an all-time low.

- ***Police/law:*** The blockchain maintains integrity of data and helps in storing all the evidence. In addition, it is distributed without worrying about tampering. It adds the necessary layer of security that adds trust to law enforcement.
- ***Gun tracking:*** With blockchain, we can have a system where each gun can be accounted for. Each weapon that leaves the factory can be tracked to help stop illegal gun usage and export. Once stored, the information can be retraced whenever needed. A gun used in a crime can be traced back to its original owner or its origins can be known instantly.

Transportation

The transportation industry can be transformed by blockchain adoption. It lowers processing and administrative costs, minimises disputes, improves overall transportation speed, and much more.

- ***Business transportation:*** Blockchain allows easy data coordination using DLT. Smart contracts can be used to automate most of the transportation pipeline, or to create a custom solution to enable transportation for fragile and sensitive products easily. The whole network can scale to include more transportation vehicles, products, and information.
- ***Automotive:*** With self-driving cars already out and shipping, it is now high time for the automotive industry to make use of the blockchain. The revolution has already started. The IOTA (Internet of Things Application) blockchain has already shown a proof-of-concept for how its Tangle DLT can work for autonomous cars.
- ***Public transport:*** Public transportation always demands improvement. With blockchain, things can change drastically.

Fintech

Right now, tons of fintech start-ups are working to provide a better solution by using blockchain.

Blockchain is the greatest disrupter to the global financial services system of this generation. Banking systems and principles, underlying banking transactions, and bookkeeping are complex and challenging. With a blockchain-based solution in place, complex processes that once took weeks to reconcile can be completed in a few minutes.

Existing ledger accounting in the financial services sector is usually in the form of a centralised and private database, not too different from the paper based versions used a long time back. With blockchain, the ledger moves to an open and distributed record shared across the participant nodes in the blockchain. Each node maintains its own version of the ledger, and the network must collectively agree on the authenticity and correctness of transactions before carrying out an update.

Contracts

Contracts help to set up requirements for taking up a job, for payment and any other tasks that require two parties. They can be related to music, land, property, etc.

- ***Inheritances:*** Smart contacts empower digital inheritance, which means to transfer digital assets to someone.
- ***Legal contracts:*** Legal contracts can take advantage of smart contracts. However, they must adhere to the blockchain law.
- ***Property and land:*** Blockchain can provide a suitable means to register deeds, property ownership, and so on. This will remove any frauds, and any change of deed is brought to the notice of the owner. In addition, the information can be backtracked with full transparency and security.

Supply chain management

In supply chain, blockchain technology can be used to store and record all the transactions and exchanges of ownership, right from the extraction of raw materials to delivery to the customer. It helps to identify where the materials were sourced, the type of labour used, and the exact position of the goods at any given moment.

In supply chain management, blockchain technology enables enterprises to:

- Verify materials
- Identify asset quantity as the assets move through the supply chain
- Coordinate orders and shipment notifications
- Verify the constitution of materials
- Increase scalability, security, and innovation
- Link physical materials to serial numbers, bar codes, and digital tags
- Share important information about the manufacturing process, assembly, delivery, and vendors

Entertainment

Blockchain is also changing the entertainment industry in several ways.

- ***Entertainment industry:*** The future of entertainment is in the hands of the blockchain. Blockchain will change how content is created and consumed.

Feature	Open source product	Remarks
Public blockchain	Ethereum, Ripple, Litecoin, etc	Permissionless blockchain; participants are anonymous and proof of work as consensus algorithm; requires mining
Private blockchain	Hyperledger projects, Exonum, OpenChain, MultiChain	Permissioned blockchain; identity of the participants is known before; no need of mining and native cryptocurrency to pay for mining
Federated blockchain (consortium)	R3, EWF, etc	Group of companies or individuals coming together to make decisions for the best benefit of the whole network. Such groups are also called consortiums or a federated blockchain
Smart contracts in general programming languages	Hyperledger, Ethereum	Ethereum does not directly support Java; it does so with the help of a framework called web3j
No mining and native cryptocurrency	Hyperledger, Corda, Openchain	Typically, public blockchains require mining (as part of proof of work) to add a block to the chain. Miners will be rewarded using native cryptocurrency
Pluggable consensus algorithms	Hyperledger, Corda, OpenChain	Support for pluggable consensus used for different applications
Pluggable ordering service	Hyperledger	Support for pluggable ordering service used for different applications
Pluggable membership service	Hyperledger	Support for pluggable membership used for onboarding new users onto the network

- ***Music industry:*** Blockchain will make it easier to share music and use smart contracts to do so. The smart contracts will ensure that the revenue is distributed to the parties according to the agreement. It will also remove intermediaries.

Benefits of blockchain

- Greater transparency; transaction histories are becoming more transparent using blockchain technology
- Enhanced security; there are several ways that blockchain is more secure than other record-keeping systems
- Elimination of error handling through real-time tracking of transactions with no double spending
- Improved traceability
- Trusted record-keeping and shared trusted process
- Increased efficiency and speed, reduction of settlement time to mere seconds by removing intermediaries
- Reduced cost and complexity, material cost reduction through the elimination of expensive proprietary infrastructure
- Full automation of transactional processes, from payment through settlement

Blockchain is not recommended for:

- High performance (millisecond) transactions
- Small organisations (no business network)
- Database replacement
- Messaging solutions
- Transaction processing replacement

Table 1 shows various open source blockchain products and their critical characteristics.

In summary, blockchain provides better security during transactions of any value. This unique and universal technology helps to streamline and automate nearly all customer services and legal contracts, while increasing the transparency and effectiveness of an enterprise. However, more work is needed for using blockchain technology to minimise enterprise costs, improve security in an era of cyber uncertainty and enhance customer delivery. END

Acknowledgements

The author would like to thank Santosh Shinde of BTIS, Enterprise Architecture division of HCL Technologies Ltd for giving the required time and support in many ways to write this article as part of architecture practice efforts.

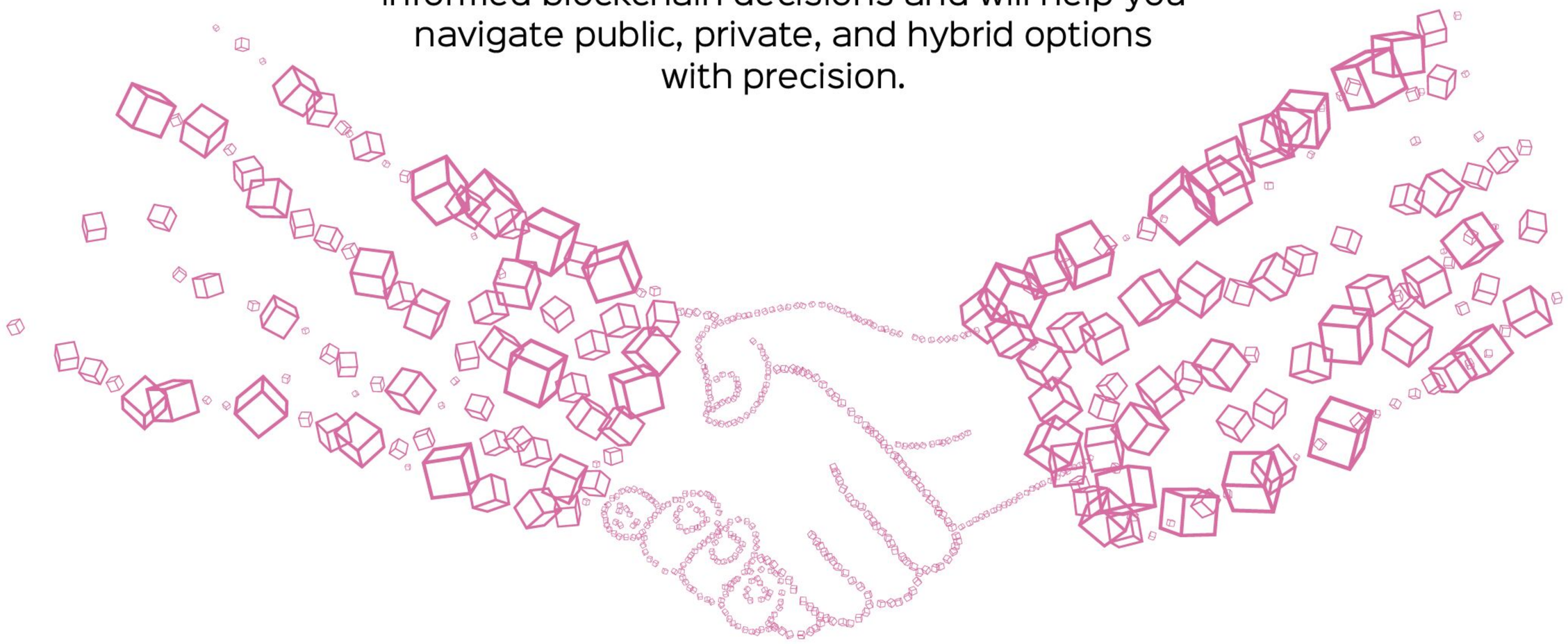
By: Dr Gopala Krishna Behara

The author is an enterprise architect in the BTIS Enterprise Architecture division of HCL Technologies Ltd. He has a total of 27 years of experience in the IT industry.

Disclaimer: The views expressed in this article are that of the author and HCL does not subscribe to the substance, veracity, or truthfulness of the said opinion.

Selecting the Right Blockchain Technology

As blockchain continues to evolve, so do your opportunities. This article is a roadmap to informed blockchain decisions and will help you navigate public, private, and hybrid options with precision.



A blockchain is a decentralised and distributed digital ledger that records transactions across multiple computers in a way that ensures security, transparency, and immutability. Understanding the distinctions among various blockchain platforms is crucial when embarking on a blockchain project. Before diving deep into the crux of selecting the blockchain platform for your project, let us recap some fundamentals of blockchain and its types.

Brief overview of how blockchain works

While venturing deeper into the blockchain landscape, it's essential to understand how this technology's inner workings shape the choices in the world of decentralisation. Here is a brief overview.

Blocks: Transactions are grouped together into blocks. Each block contains a list of transactions and a reference to the previous block, forming a chain of blocks.

Decentralisation: Instead of being stored on a single central server, the blockchain ledger is maintained by a network of computers (nodes) distributed around the world. This decentralised nature prevents a single point of failure and makes the system more resilient.

Consensus mechanisms: To validate and add new blocks to the chain, a consensus mechanism is used. The most well-known consensus mechanism is proof of work (PoW), which requires miners to solve complex mathematical puzzles to verify transactions. Other mechanisms like proof of stake (PoS) and delegated proof of stake (DPoS) exist as well.

Immutability: Once a block is added to the blockchain, it's nearly impossible to alter the information within it. This immutability is achieved through cryptographic hashing and the decentralised nature of the network.

Transparency: The entire transaction history is publicly available on the blockchain, offering a high level of transparency.

Security: The decentralised and distributed nature of blockchain, along with cryptography, enhances security. Changing a single block would require altering subsequent blocks on every node, which is computationally infeasible.

Blockchain use cases

Blockchain technology has transcended its roots as the backbone of cryptocurrencies, and has evolved into a versatile tool with myriad applications. It now has applications beyond cryptocurrencies.

Supply chain management: Blockchain can provide transparency and traceability in supply chains, verifying the origin and movement of goods.

Smart contracts: These are self-executing contracts with the

terms directly written into code. They automatically execute and enforce agreements when predefined conditions are met.

Identity verification: Blockchain can be used to securely manage digital identities and reduce the risk of identity theft.

Voting systems: Blockchain can enhance the security and transparency of voting systems, reducing the potential for fraud.

Healthcare: Patient records can be securely stored and shared among healthcare providers using blockchain, ensuring data accuracy and privacy.

Real estate: Blockchain can streamline property transactions, reducing paperwork and improving efficiency.

Financial services: Blockchain has the potential to revolutionise traditional financial systems by enabling faster, more secure, and cheaper cross-border transactions.

Whether you're considering launching a decentralised application (DApp), managing digital assets, or exploring supply chain solutions, selecting the right blockchain platform is a pivotal decision.

Public blockchains and private blockchains

A fundamental distinction in the world of blockchain is the division between public blockchains and private blockchains.

The choice between public and private blockchains depends on the specific needs of your project or organisation. Public blockchains excel in scenarios where decentralisation, openness, and transparency are paramount, while private blockchains offer control and privacy. The emergence of hybrid blockchains provides even more flexibility.

We'll delve into the nuances of these two blockchain variants and explore their use cases, benefits, and trade-offs.

Public blockchains: The power of permissionlessness

Permissionless public blockchains are perhaps the most iconic face of blockchain technology. They epitomise decentralisation and openness. Here's what characterises them.

Accessibility for all

Permissionless public blockchains are open to anyone, anywhere. Participation requires no prior approval or vetting. This inclusive nature enables global participation, fostering a truly decentralised ecosystem.

Transparency and trustlessness

Transactions on permissionless public blockchains are transparent and immutable. They're recorded on a public ledger that anyone can access and verify. Trust is established not through intermediaries but through cryptographic algorithms and consensus mechanisms.

Prime examples

Two of the most renowned examples of permissionless public blockchains are Bitcoin and Ethereum. Bitcoin introduced the world to the concept of a decentralised digital currency, and Ethereum pioneered smart contracts, enabling programmable, self-executing agreements.

Use cases

Permissionless public blockchains are ideal for applications where trust, censorship resistance, and decentralisation are paramount. They are often used for digital currencies, DApps (decentralised applications), and scenarios where transparency is critical, like voting systems and public records.

Private blockchains: Control and privacy

Permissioned private blockchains, on the other hand, introduce a layer of control and privacy into the blockchain landscape. Here's what defines them.

Controlled access

Access to a permissioned private blockchain is restricted. Participants are known and typically vetted, ensuring a degree of trust among network members. These blockchains often cater to consortiums, businesses, or organisations.

Enhanced privacy

Privacy is a key feature of permissioned private blockchains. Unlike their public counterparts, transactions on these networks are not necessarily visible to all participants. They provide a level of confidentiality that can be crucial in enterprise settings.

Use cases

Permissioned private blockchains find applications in contexts where privacy, regulatory compliance, and control are vital. Industries like finance, healthcare, and supply chain management use them to streamline processes, secure data, and meet legal requirements.

Hybrid blockchains: The best of both worlds

In some cases, a middle ground is sought through hybrid blockchains. These blockchains combine features of both public and private blockchains. They offer selective transparency and access control, making them adaptable to various use cases. Hybrid blockchains are an excellent solution when there's a need for shared data among multiple parties while maintaining a degree of confidentiality.

Blockchain platforms

Open source blockchain projects provide transparency, flexibility, and often have active developer communities. There are several available. Table 1 lists some notable open source blockchain platforms and projects.

These are just a few examples of open source blockchain projects, and there are many more in various stages of development. When choosing an open source blockchain platform, consider

Table 1: Popular open source blockchain platforms and projects

Ethereum (ETH) Ethereum is one of the most well-known open source blockchain platforms for creating decentralised applications (DApps) and smart contracts. It uses the Ethereum virtual machine (EVM), and has a large and active development community.
Hyperledger Fabric Hyperledger Fabric is an open source permissioned blockchain platform hosted by the Linux Foundation. It is designed for enterprise use cases, emphasising privacy, scalability, and modular architecture.
Hyperledger Sawtooth Hyperledger Sawtooth is another open source blockchain platform under the Hyperledger project. It focuses on simplicity and modularity, and is suitable for building custom blockchains.
Corda (R3 Corda) Corda is an open source blockchain platform designed for financial institutions. It emphasises privacy and supports interoperability between different Corda networks.
Stellar (Stellar Development Foundation) Stellar is an open source blockchain platform for cross-border payments and tokenisation. It focuses on fast and low-cost transactions, particularly for financial inclusion.
NEO (NEO blockchain) NEO is an open source blockchain platform that supports smart contracts and digital assets. It provides support for multiple programming languages, making it developer-friendly.
Cardano (IOHK - Input Output Hong Kong) Cardano is an open source blockchain platform known for its academic research-driven approach. It aims to provide a secure and scalable infrastructure for smart contracts and DApps.
Tezos (Tezos Foundation) Tezos is an open source blockchain platform with a strong focus on governance. It allows token holders to participate in protocol upgrades and decision-making.
Avalanche (Avalanche Foundation) Avalanche is an open source blockchain platform known for its flexibility and customisability. It offers subnets and custom blockchains for various use cases.
Bitcoin (Bitcoin Core) Bitcoin is the original open source blockchain project, focusing primarily on digital currency. Bitcoin Core is the reference implementation of the Bitcoin protocol.
Polkadot (Web3 Foundation) Polkadot is an open source, interoperable blockchain platform that connects different blockchains. It allows for the creation of parachains with unique features.
Cosmos (Interchain Foundation) Cosmos is an open source project designed to create an internet of blockchains. It facilitates interoperability between blockchains and has a modular architecture.
IOTA (IOTA Foundation) IOTA is an open source distributed ledger technology (DLT) project that focuses on the Internet of Things (IoT) and feeless microtransactions. It uses a directed acyclic graph (DAG) called the Tangle.

your project's specific requirements, community support, and the platform's suitability.

Factors to consider when choosing a blockchain platform

Selecting the right blockchain platform is a pivotal decision, whether you are considering launching a decentralised application (DApp), managing digital assets, or exploring supply chain solutions. The key factors to consider when choosing the blockchain platform are:

Define your use case

Begin by clearly defining the purpose of your blockchain project. What specific problem are you trying to solve, and what functionalities do you need from the blockchain? Different use cases may require vastly different platforms.

Consensus mechanism
Understand the consensus mechanism employed by the blockchain platform. Each mechanism, whether proof of work (PoW), proof of stake (PoS), or others, has its advantages and trade-offs. PoW, for instance, offers high security but consumes substantial energy.

Scalability
Assess the scalability of the blockchain platform. Will it handle the anticipated transaction volume? Consider aspects like block size, block time, and the network's ability to accommodate growth.

Security
Evaluate the platform's security features. Look for a blockchain with a strong track record and mechanisms to thwart attacks, such as 51% attacks. Security is paramount, especially for applications involving sensitive data.

Smart contract support
If your project involves smart contracts, ensure the platform supports them. Examine the available programming languages and tools for writing and deploying smart contracts.

Interoperability
Consider whether the platform facilitates interoperability with other blockchains or existing systems. Blockchain networks increasingly need to communicate with each other and integrate into the broader tech ecosystem.

Privacy features
If your project demands privacy, seek platforms with features like zero-knowledge proofs or confidential transactions. These can shield sensitive data while still benefiting from blockchain technology.

Regulatory compliance
Be aware of the regulatory landscape in your region. Choose a blockchain platform that aligns with relevant regulations. Some platforms incorporate compliance features.

Token and asset support
If tokenisation is part of your plan, verify that the platform supports it and whether it offers standardised token protocols like ERC-20 (for Ethereum). Asset management tools should also be considered.

Ecosystem and partnerships
Examine the blockchain's ecosystem. Are there active projects, DApps, or industry partnerships that align with your goals? A robust ecosystem can foster growth and adoption.

Costs
Consider the costs associated with using the blockchain, including transaction fees and hosting expenses. Ensure it aligns with your budget.

Performance and throughput
Assess the blockchain's performance, including transaction throughput and confirmation times. A platform must meet your project's performance requirements.

User experience and documentation
Examine the user-friendliness of the platform and the availability of comprehensive documentation and developer resources. A well-documented platform can expedite development.

Long-term viability
Consider the blockchain's long-term viability and roadmaps. Ensure it is actively maintained and has plans for future enhancements.

Testing and prototyping
Before fully committing, consider building a prototype or conducting tests to evaluate the platform's suitability for your project.

Legal and compliance consultation
If your project involves legal and compliance complexities, consult legal experts well-versed in blockchain to ensure full compliance with applicable regulations.

Community and expert input
Leverage the insights of the blockchain community and experts. Forums, conferences, and online communities can provide valuable perspectives.

Choosing the right blockchain platform is a multifaceted task. It's not a one-size-fits-all technology, but rather a versatile tool that can be tailored to meet your project's unique requirements. It could involve disrupting industries with decentralised applications or securely managing sensitive enterprise data.

We should not forget that blockchain technology is continuously evolving. We need to stay informed about new developments, emerging platforms, and updates in the blockchain space. With careful consideration and due diligence, we can select a blockchain platform that aligns with our project's objectives and sets the stage for success in the decentralised world. END

By: Renganathan D.
The author is a Google cloud certified architect at HCL Technologies Ltd.

Disclaimer: This article expresses the views of the author and not of the organisation he works in.

Cryptocurrency Wallets: Implementing MetaMask for Blockchain Transactions

This article introduces and compares popular cryptocurrency wallets. It also tells you how to select one. It then gives a practical demonstration of implementing the MetaMask wallet for blockchain transactions.



A cryptocurrency wallet is a digital tool that allows individuals to store, manage, and interact with their cryptocurrencies. Cryptocurrency wallets play a crucial role in the blockchain ecosystem, as they are essential tools for collecting, storing, and transacting cryptocurrencies. These wallets come in various forms, each with its characteristics and use cases. Different cryptocurrency wallets commonly used in the blockchain space are shown in Figure 1.

How to choose the right cryptocurrency wallet

Choosing the right cryptocurrency wallet depends on your specific needs, security concerns, and level of expertise. For long-term storage of significant cryptocurrency holdings, hardware wallets are recommended. Mobile and desktop wallets may be more suitable for everyday transactions and quick access. Regardless of the type, it's crucial to follow best practices for security, including keeping private keys safe and regularly backing up wallet information. Here is a list of all the criteria for the selection of the right cryptocurrency wallet.

Security: Consider a hardware wallet or a well-secured desktop wallet for long-term storage of significant assets. Always enable additional security features like two-factor authentication.

Ease of use: If you're new to cryptocurrencies, a user-friendly mobile wallet like Trust Wallet may be a good starting point.

Supported assets: Ensure the wallet supports the cryptocurrencies you plan to hold. Some wallets specialise in specific networks, while others offer broader compatibility.

Backup and recovery: Learn how to create a secure backup (usually a seed phrase) and recovery process for your chosen wallet. This is critical in case you ever lose access to your wallet.

Community reputation: Research user reviews and the community reputation of the wallet you are considering. Look for wallets with a history of security and reliability.

Table 1: A comparison of popular cryptocurrency wallets

Features	MetaMask	Coinbase wallet (not open source)	Electrum	Trezor
Purpose	To decentralise applications built on the Ethereum blockchain	To buy and sell Bitcoin, Ethereum, and Litecoin	To facilitate the storage, management, and secure handling of Bitcoin	To enable Bitcoin transactions, generate private and public keys
Wallet type	Software wallet	Mobile wallet	Desktop wallet	Hardware wallet
Crypto supported	Ethereum and ERC-20 tokens	Ethereum, Solana, and all EVM-compatible networks	Bitcoin only	Bitcoin and ERC-20 tokens
Supported browser	Firefox, Chrome	Chrome, Firefox, and Opera browsers	Firefox	Trezor Suite web application, Chrome
Safety	Moderate	Highly secured	Robust, including two-factor authentication	Highly secured
Ease of use	Average	Average	Moderate	High user-friendly interface
Target industries/ users	Financial and computer software	Financial services and accounting	Individual developers	Small to medium enterprises
Market segment	95% small business, 5% enterprise	83% small business, 8% enterprise	79% small business, 29% mid-market	71% small business, 36% mid-market
Pros	Easy to sell and buy	Easy to send and receive	Easy user interface	Wide cryptocurrency supports
Cons	High commission	Complex payment methods	Limited availability of coins	Limited availability of coins
Official website	*https://metamask.io/*	*https://www.coinbase.com/wallet*	*https://electrum.org/#about*	*https://trezor.io/*

Installation and set up of MetaMask for blockchain transactions

MetaMask is a widely used and versatile cryptocurrency wallet and browser extension primarily designed for the Ethereum ecosystem. Its key features include DApp interaction, secure storage, cross-platform accessibility, custom network configuration, and support for multiple Ethereum-based tokens. Here is a step-by-step guide on how to install and set MetaMask for blockchain transactions.

Step 1: Install MetaMask

Go to the MetaMask website (*https://metamask.io/*) and download the MetaMask extension for your web browser (e.g., Chrome, Firefox).

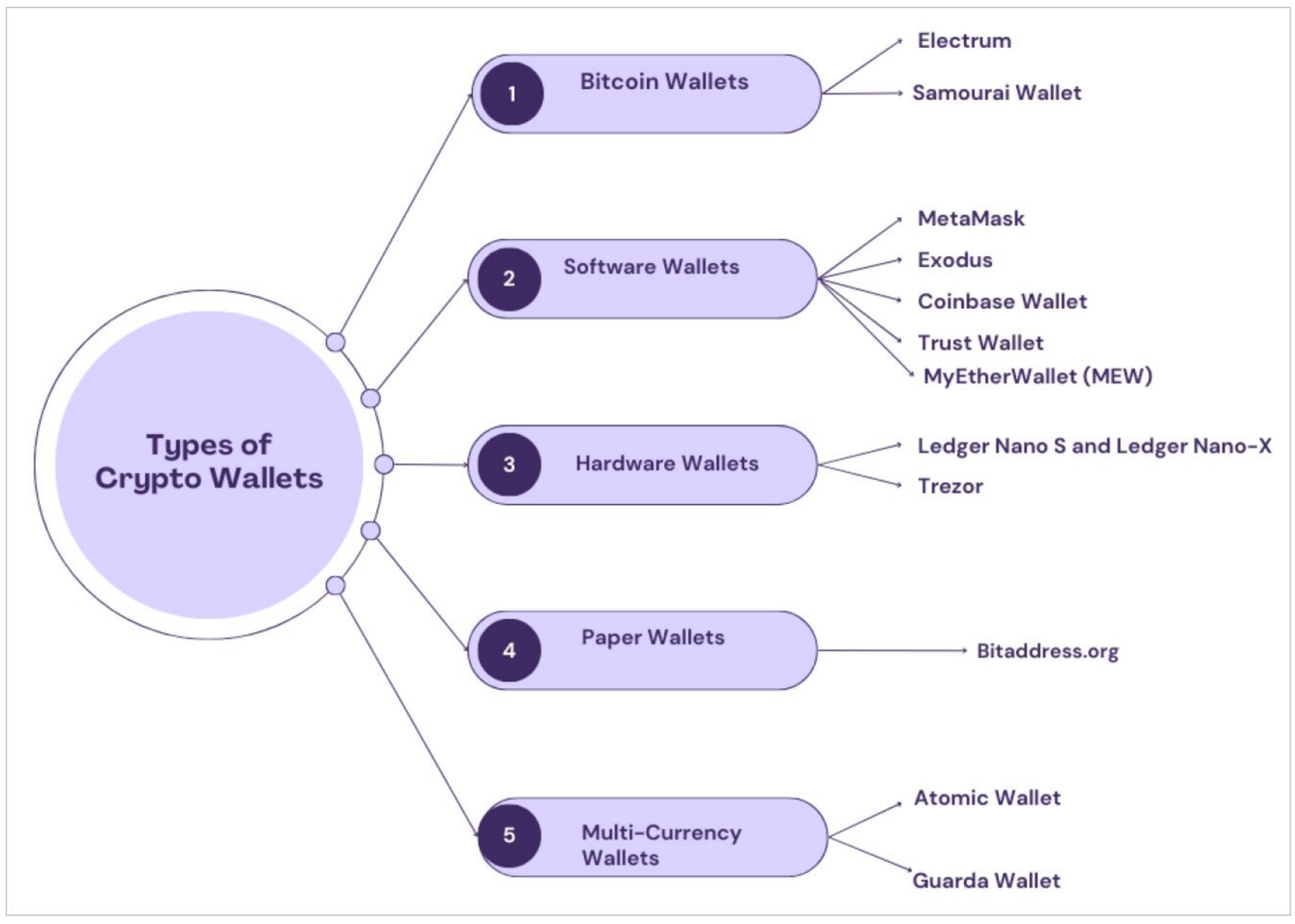


Figure 1: Different types of cryptocurrency wallets

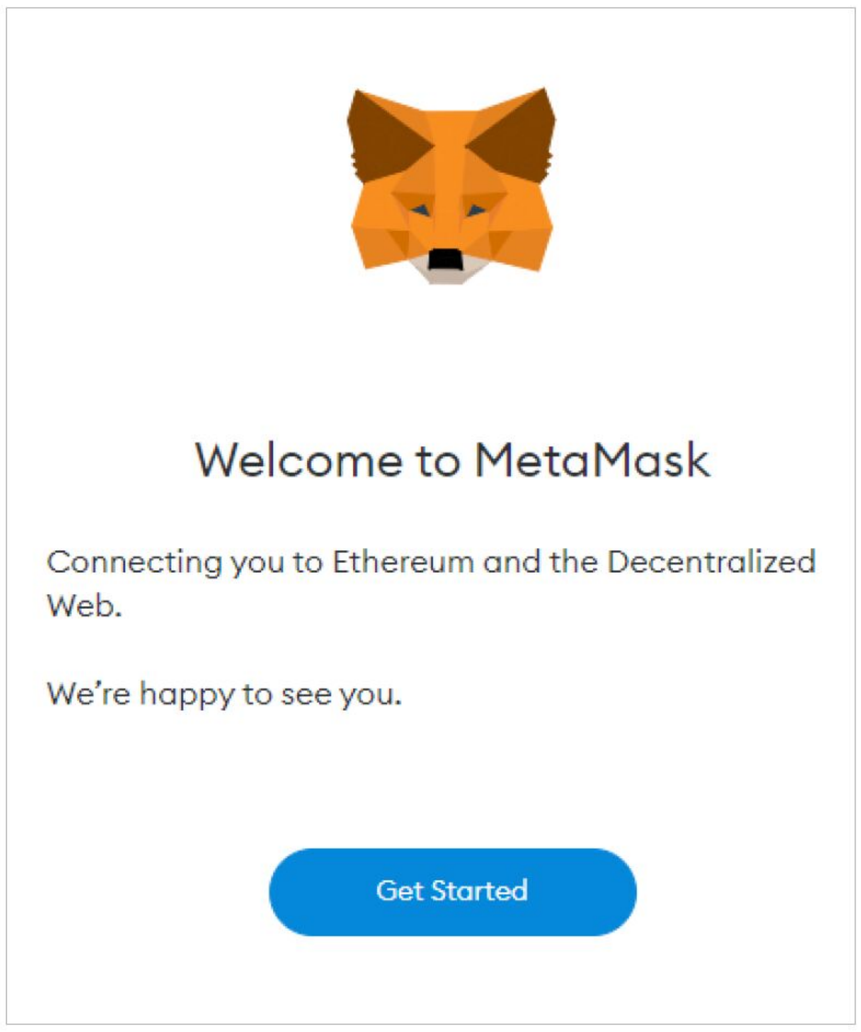


Figure 2: MetaMask wallet deployed interface

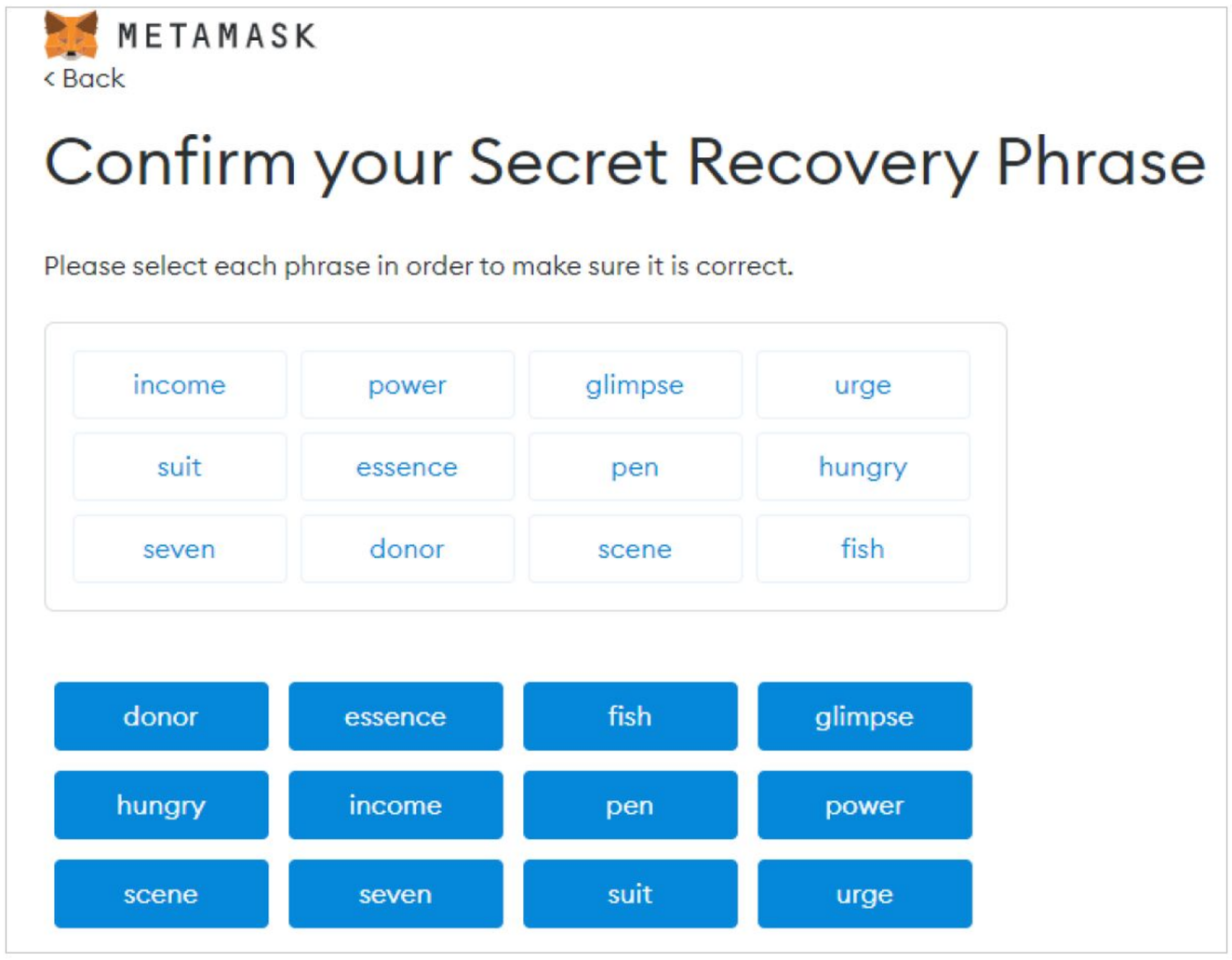


Figure 3: Setting up the secret recovery phase for the MetaMask wallet

Step 2: Set up your wallet

After installation, open MetaMask by clicking on the extension icon in your browser.

Create a new wallet or import an existing one by selecting the 'import wallet' option if you already have a seed phrase or private key. After MetaMask has been successfully installed you will see the interface as shown in Figure 2.

Step 3: Secure your wallet

Now, create a strong password to secure your MetaMask wallet. Store your seed phrase (a recovery phrase) in a safe and offline location. This is crucial for recovering your wallet in case you forget your password or your device is lost. Figure 3 depicts different phases to confirm the secret recovery phase for the MetaMask wallet interface.

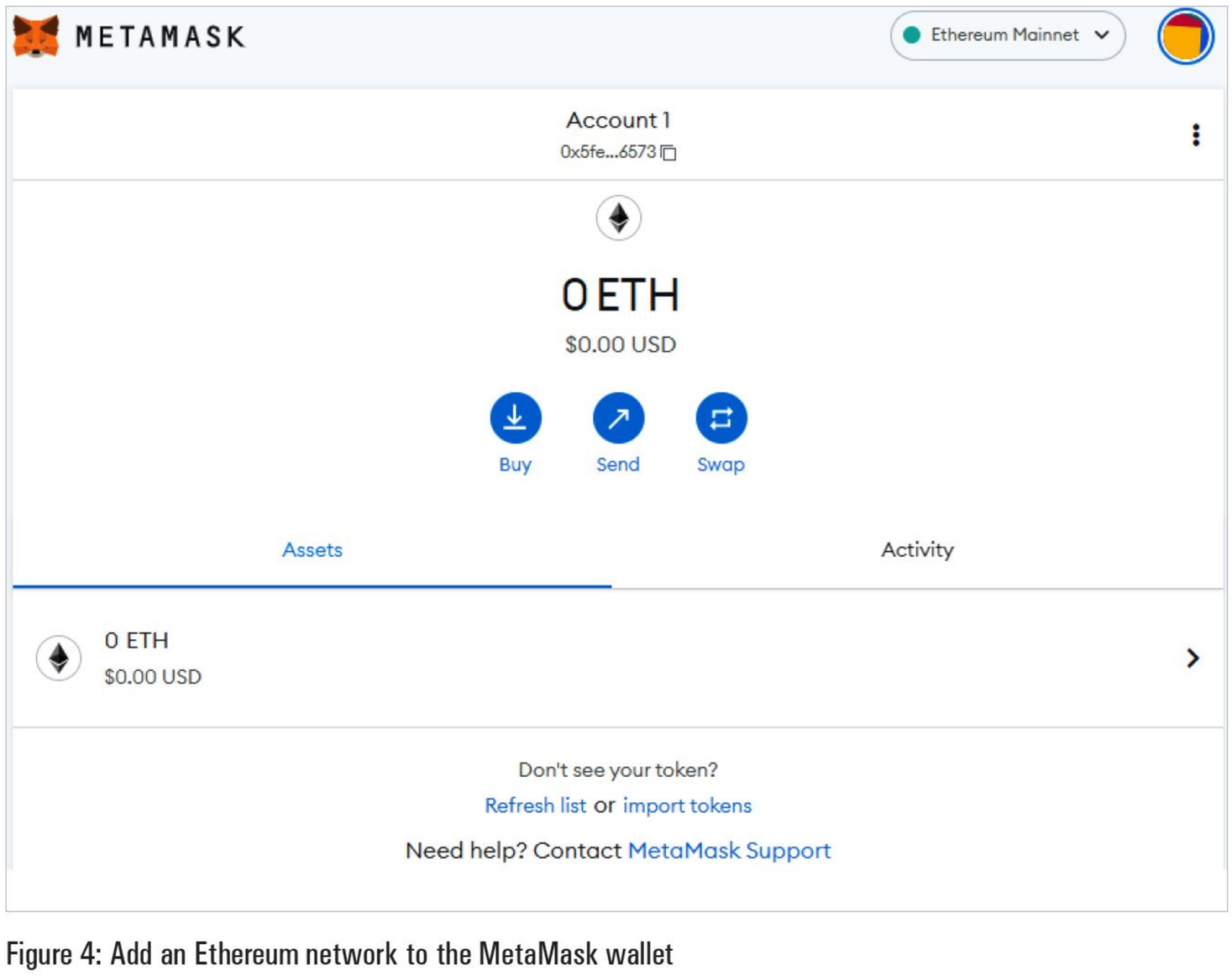


Figure 4: Add an Ethereum network to the MetaMask wallet

Step 4: Add Ethereum (ETH) network

By default, MetaMask is set to the Ethereum network. You can add other networks (e.g., testnets) for development or specific blockchain projects. Click on the network name at the top of the MetaMask extension, then select 'Custom RPC' to add a custom network with its URL and chain ID. Figure 4 shows how to add the Ethereum network to deploy the MetaMask wallet.

Step 5: Request MetaMask Ether from faucet

Users should deposit cryptocurrency (typically Ether for Ethereum from faucet) into your MetaMask wallet to send, receive, or interact with smart contracts. You can do this by sending funds from another wallet or exchange to your MetaMask wallet address, as shown in Figure 5.

Step 6: Confirm MetaMask transactions

To send cryptocurrency or interact with DApps, click the 'Send' button

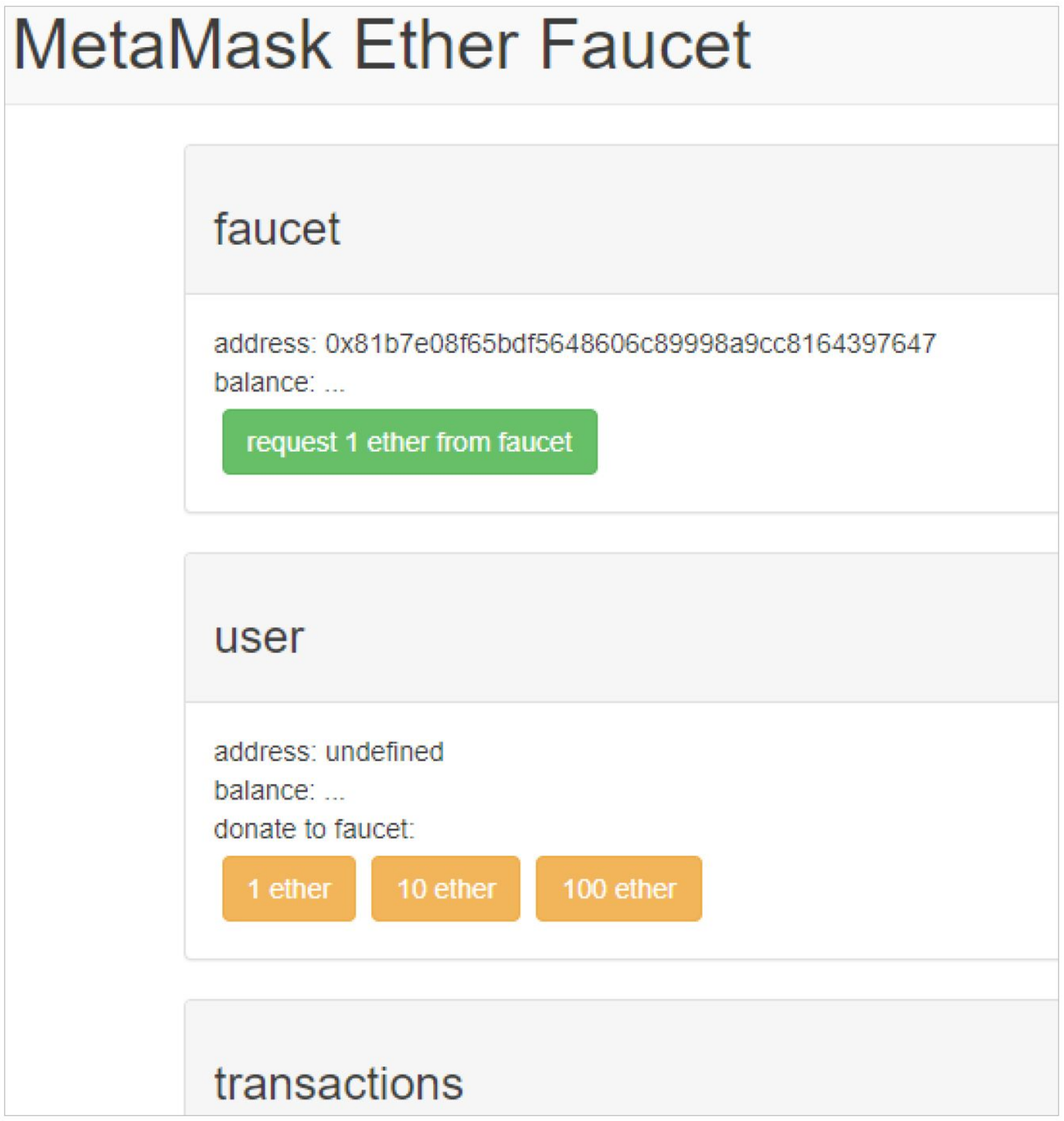


Figure 5: Requesting MetaMask Ether from faucet

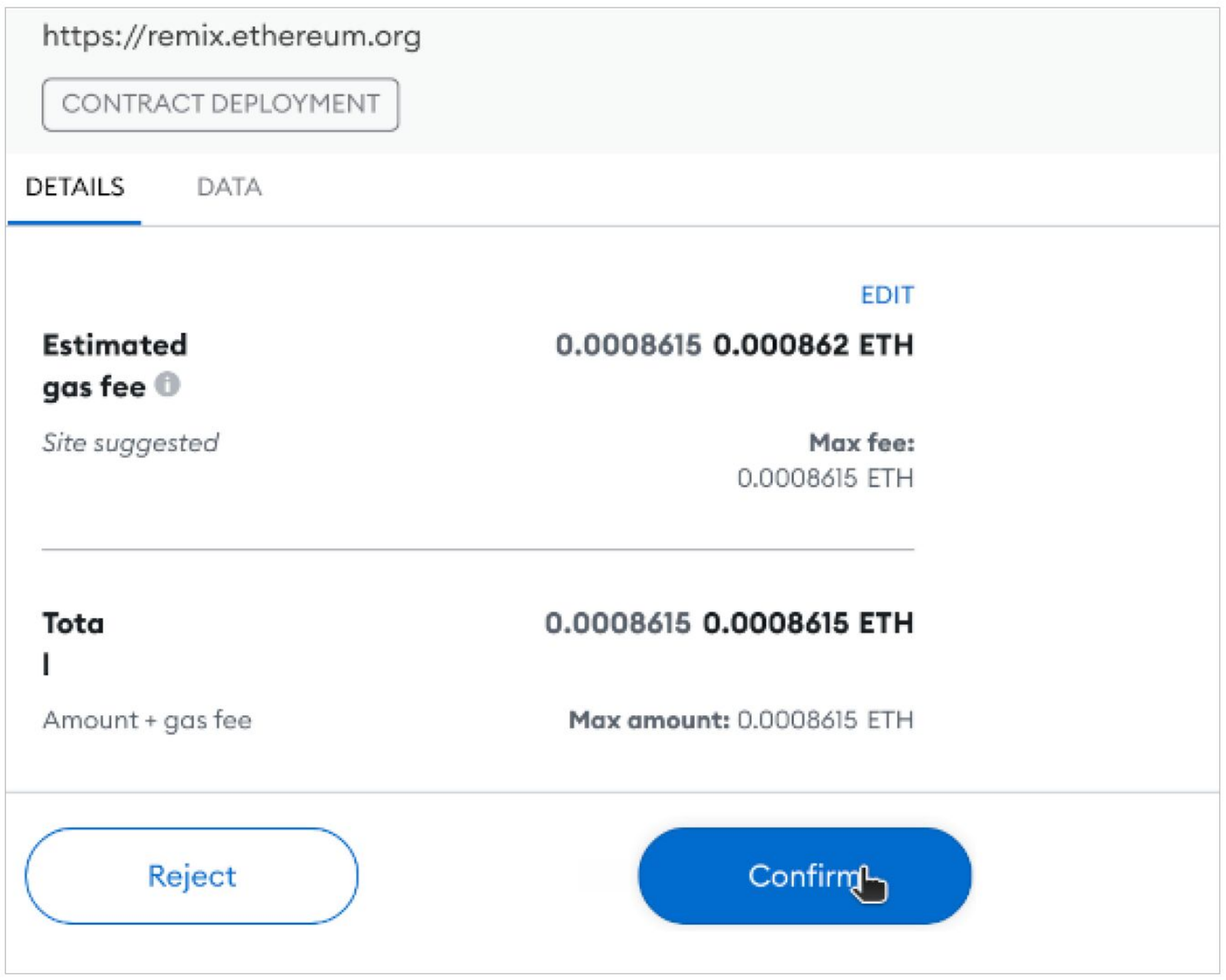


Figure 6: Confirm MetaMask blockchain transaction

in MetaMask. Fill in the recipient's address, the amount you want to send, and adjust the gas fee (transaction fee). Gas fees ensure your transaction is processed on the blockchain; you can change them based on network congestion and your transaction's urgency. Review the transaction details and click 'Confirm' to send, as shown in Figure 6.

Research directions

In the digital age, blockchain technology and cryptocurrency wallets have revolutionised finance, expanded the possibilities of decentralised applications, and provided individuals with unprecedented financial sovereignty. Cryptocurrency wallets provide secure storage for private keys, ensuring that users have complete control over their digital assets. However, users must exercise caution, adhere to security best practices, and stay informed about the evolving blockchain and cryptocurrency landscape to navigate it successfully. Therefore, addressing the environmental impact of blockchain networks, especially proof of work (PoW) networks, is crucial. Research into alternative consensus mechanisms and energy-efficient infrastructure is equally essential. END

References

- *https://metamask.io/*
- *https://www.ibm.com/topics/blockchain*

By: Dr Aditya Bhardwaj

The author is a B. Tech, M. Tech, and PhD in CSE. He works as assistant professor in the School of Computer Science Engineering and Technology at Bennett University, Greater Noida. He is experienced in cloud computing and open source technology.

Blockchain Technology and Generative AI: A Symbiotic Partnership

The intersection of blockchain technology and generative AI will usher in a new era of efficiency, security, and creativity in the digital world.



In the ever-evolving landscape of technology, two groundbreaking innovations have emerged as frontrunners: blockchain and generative artificial intelligence (AI). Blockchain, with its decentralised and transparent nature, has transformed industries ranging from finance to supply chain management. On the other hand, generative AI, powered by neural networks, has demonstrated remarkable abilities in creating content that ranges from text to images and even videos. What if these two powerhouses joined forces? Incorporating AI in blockchain technology requires thought and design considerations to achieve desired results like the reduced cost of implementing digital ledger solutions.

The convergence of blockchain and generative AI

Blockchain technology has gained fame for its ability to establish trust through decentralisation and immutability. Its application spans across industries, enabling secure transactions, provenance tracking, and more. However, despite its impressive capabilities, blockchain faces certain challenges that can be mitigated through the integration of generative AI.

Generative AI, as exemplified by models like OpenAI's GPT-4 (and soon to be GPT-5), excels in tasks involving content creation and manipulation. It can draft human-like text, design images, and even assist in complex problem-solving. By harnessing the power of generative AI, blockchain can overcome limitations in data processing, consensus mechanisms, and privacy for use cases like crypto in financial markets.

Enhancing data processing and analysis

Incorporating technology into business requires substantial investments, especially as both blockchain and AI are data- and process-intensive solutions that require large amounts of data storage

with significant processing capacity. Blockchain networks generate vast amounts of data that must be processed and analysed for various purposes such as smart contracts, identity verification, and transaction history. However, the sheer volume of data can strain network resources, leading to slower transaction times and higher costs. Generative AI can streamline this process by analysing blockchain data and providing actionable insights. AI algorithms can identify patterns, anomalies, and potential security threats, thus enhancing the overall efficiency and reliability of the blockchain network.



Figure 1: Blockchain + Gen AI—benefiting areas and industries

Optimising consensus mechanisms

Consensus mechanisms are at the heart of blockchain's functionality, ensuring that all participants agree on the state of the network. Traditional mechanisms like proof of work (PoW) and proof of stake (PoS) have their pros and cons, with energy consumption being a major concern for PoW. Generative AI can propose innovative consensus mechanisms that address these issues. By simulating various scenarios and testing new protocols, AI can optimise consensus algorithms for factors like security, scalability, and environmental impact.

Digital ledger technology (DLT) is one of the promising use cases that could adopt the new ways of working with blockchain leveraging generative AI technology. Such solutions require a significant amount of investments. However, the benefits they offer in streamlining financial expenses, addressing complex regulatory and compliance issues, and simplification of governance help to offset the costs. And they enable innovation and new offerings that could add to topline growth, disrupting the industry all over again.

Digital currency or tokenised bonds, which are becoming popular across the world, could benefit from the amalgamation of blockchain and generative AI in bringing transaction costs down, making capital markets more accessible, eliminating the intermediaries, and changing business models completely! Capturing untapped revenues is a big financial opportunity for many organisations with low-cost products and services.

In addition to finance, there are many use cases across healthcare, life sciences, supply chain, retail, etc, where responsible adoption of the two technologies could potentially improve decision-making, speed up transactions, lower costs, and create new opportunities.

Preserving privacy and security

While blockchain offers enhanced security compared to centralised systems, privacy remains a challenge. Public blockchains expose transaction details to all participants, raising concerns about sensitive data. Generative AI can contribute by developing advanced encryption techniques and privacy-preserving algorithms. By leveraging AI-generated cryptographic solutions, blockchain networks can secure data while still maintaining transparency and decentralisation.

There are also many use cases in which implementation of generative AI with private blockchain in a controlled environment can yield significant benefits. Only time will tell the nature and types of disruptions ahead.

Unleashing creative smart contracts

Smart contracts are self-executing agreements with the terms directly written into code. Generative AI can revolutionise the concept of smart contracts by infusing them with creative capabilities. Imagine a smart contract that can autonomously adapt to changing conditions or negotiate terms with other contracts. With generative AI, smart contracts can evolve from static pieces of code to dynamic and responsive entities, opening new avenues for innovation in decentralised applications.

Empowering decentralised autonomous organisations (DAOs)

Decentralised autonomous organisations (DAOs) operate based on predefined rules encoded in smart contracts. They enable decentralised decision-making and community governance. However, DAOs often face challenges in reaching consensus on complex matters. Generative AI can facilitate DAO decision-making

Continued to page...65

Consortium Blockchain: An Introduction

A consortium blockchain consists of multiple organisations or nodes working together to maintain a shared blockchain network. Its many benefits are making this blockchain variant pretty popular today.



The blockchain platform is popular for its decentralised nature, tamper-proof transactions and reliability. The reliability in the network is based on the consensus algorithm used in the execution of the platform. There are multiple variants of consensus algorithms that can be used in different types of blockchain platforms like private and public blockchain platforms.

A consortium blockchain is a permissioned blockchain platform. It is a hybrid solution combining the benefits of a private blockchain and public blockchain platform. Hence, it is getting more popular as it bridges the gap between both these platforms.

Importance of consortium blockchain

Blockchain platforms are classified in order of usability as private blockchain, public blockchain, semi-private blockchain and consortium blockchain. In fact, semi-private blockchain is an early version of the hybrid blockchain platform as it offers an enterprise-level public blockchain platform to business users. For example, inventory management in a distributed platform, which connects the manufacturing and supplier units, is grouped together in a semi-private blockchain platform.

The consortium blockchain platform branched from this to provide a hybrid platform combining various blockchain platforms. This kind of architecture is also referred to as a federated blockchain platform as the governance and workflow is distributed in nature. This feature can be expected in private blockchain platforms and not on a public blockchain platform.

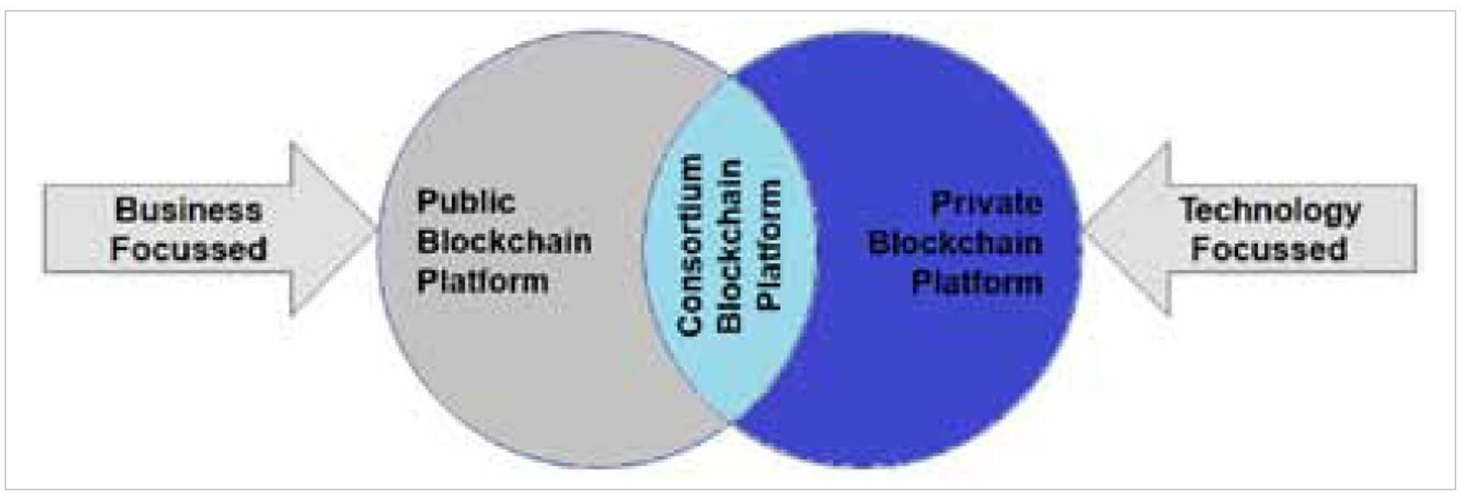


Figure 1: Consortium blockchain

On the other hand, implementing scalable blockchain nodes in a network is not possible in a private blockchain but can be done in a public blockchain platform.

A consortium blockchain offers a hybrid service combining most of the benefits of private blockchain and public blockchain, which helps address data redundancy issues and reduces transaction costs.

Use cases of consortium blockchain

Consortium blockchains find applications across various industries, benefiting from collaborative efforts while ensuring data security and transparency. Here are several use cases.

- ***Supply chain management:*** Consortium blockchain can be used to track the movement of goods and materials through a supply chain. This can help to improve efficiency, transparency, and traceability.
- ***Trade finance:*** It can be used to facilitate trade finance transactions. This can help to reduce costs and improve the speed and efficiency of transactions.
- ***Healthcare:*** It can be used to store and share medical records. This can help to improve the quality of care.
- ***Financial services:*** Secure and transparent financial transactions can be carried out using a consortium blockchain. This can help to reduce fraud and improve efficiency.
- ***Intellectual property:*** It can be used to track and manage intellectual property rights. This can help to prevent counterfeiting and improve the efficiency of licensing.
- ***Regulatory compliance:*** It can be used to comply with regulations. This can help to reduce the risk of penalties and improve efficiency.
- ***Government***: Government services can improve by using a consortium blockchain. They can become more transparent, efficient, and accountable.
- ***Energy trading:*** In the energy sector, producers, consumers, and grid operators can form a consortium to trade energy assets efficiently. Smart contracts on the blockchain automate energy transactions, ensuring transparency and trust.
- ***Education:*** Educational institutions can collaborate on a consortium blockchain to verify and share credentials and qualifications. This simplifies the hiring process for employers and reduces credential fraud.
- ***Shipping and logistics:*** A consortium of shipping companies and customs authorities can streamline documentation and customs clearance processes. This reduces delays and enhances security in international trade.
- ***Pharmaceuticals:*** The pharmaceutical industry can establish a consortium to track the authenticity and quality of drugs, reducing counterfeit products and ensuring patient safety.

These diverse use cases highlight the versatility of consortium blockchains in improving transparency, security, and collaboration across various sectors. They offer opportunities to streamline processes, reduce fraud, and enhance trust among participants in complex ecosystems.

Security and data protection in a consortium blockchain

A consortium blockchain typically consists of multiple organisations or nodes working together to maintain a shared blockchain network. Ensuring the security and protection of data in this context involves the following key aspects.

Cryptography: Blockchain uses cryptography to secure its data. This includes the use of hashing algorithms to create unique fingerprints for each block of data, as well as digital signatures to verify the authenticity of transactions.

Distributed ledger: The data in a blockchain is stored in a distributed ledger, which means that it is not stored in a single location. This makes it more difficult for hackers to access or tamper with the data.

Consensus mechanism: A blockchain uses a consensus mechanism to ensure that all participants in the network agree on the state of the ledger. This helps to prevent fraud and ensure the integrity of the data.

Access control: In a consortium blockchain, access to the network is controlled by a group of authorised participants. This helps to protect the data from unauthorised access.

Encryption: Sensitive data can be encrypted before it is stored on the blockchain. This, too, helps to protect the data from unauthorised access.

Privacy: There are a number of ways to protect the privacy of data on a blockchain. This includes the use of pseudonymous addresses and encryption.

Here are some additional considerations for security and data protection in a consortium blockchain.

The need for a strong governance framework: A well-defined governance framework is essential for ensuring the security and data protection of a consortium blockchain. This framework should define the roles and responsibilities of the participants in the network, as well as the procedures for managing security risks.

The need for regular audits: Regular audits are essential for identifying and addressing security vulnerabilities in a consortium blockchain. These audits should be conducted by independent third parties.

The need for continuous improvement: The security and data protection of a consortium blockchain is an ongoing process. It is important to continuously monitor the network for potential risks and to implement new security measures as needed.

Benefits and challenges of consortium blockchains

Consortium blockchains offer several benefits but face some unique challenges.

Benefits

- *Security and transparency:* Blockchain is a secure and transparent way to store data. The data is encrypted and distributed across the network, making it difficult to hack or tamper with. The distributed ledger also makes it easy to track the history of transactions, which can help to prevent fraud.
- *Collaboration:* Consortium blockchains can help to facilitate collaboration between organisations. By sharing data and processes on a shared platform, organisations can work together more efficiently and effectively.
- *Cost savings:* Consortium blockchains can help to reduce costs. By sharing resources and infrastructure, organisations can save money on development, maintenance, and operation costs.
- *Scalability:* These blockchains can be scaled to handle a large number of transactions. This makes them a good fit for applications that require high throughput, such as supply chain management and trade finance.

Challenges

- *Governance:* Consortium blockchains require a well-defined governance framework to ensure that all participants agree on the rules and procedures for the network. This can be a challenge, especially if the consortium includes organisations with different interests.
- *Complexity:* These blockchains can be complex to implement and manage. This is because they require a high level of technical expertise and coordination between the participants.
- *Regulation:* The regulatory landscape for blockchains is still evolving. This can make it difficult for organisations to comply with all applicable regulations.
- *Lack of standards:* There are no universally accepted standards for consortium blockchains. This can make it difficult for organisations to interoperate with each other.

Overall, consortium blockchains offer a number of benefits, but they also come with some challenges. The decision of whether or not to use a consortium blockchain should be made on a case-by-case basis, taking into account the specific needs of the organisation.

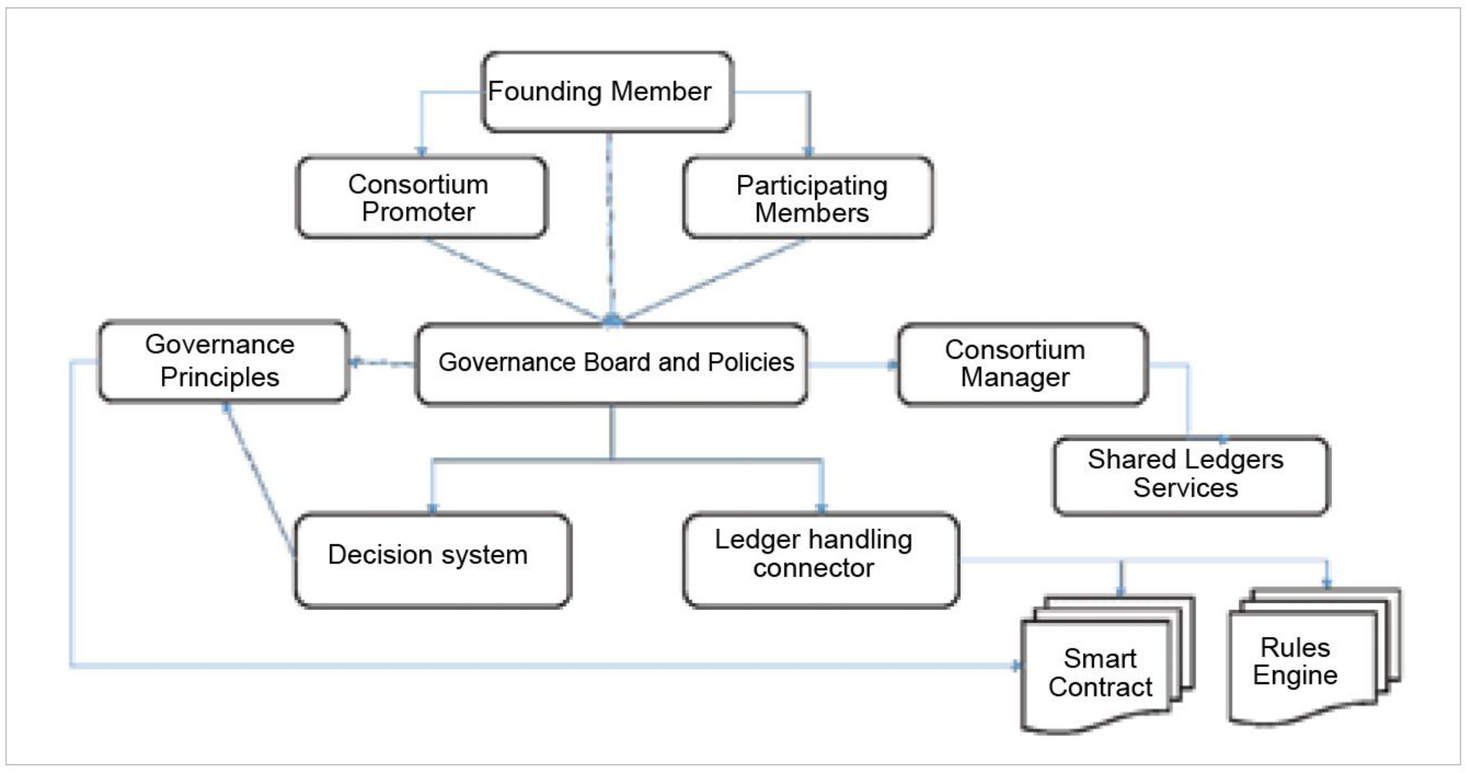


Figure 2: Consortium blockchain governance

Consortium blockchain governance

The functional architecture of any blockchain platform, which helps to define the governance model, is based on various consensus algorithms used for platform execution. These are listed here.

Proof of work (PoW): This is the original consensus algorithm from Satoshi Nakamoto's first research on blockchain, and is used as a mechanism to confirm the transaction has been completed. If confirmed, a new block gets added to the chain of networks. This helps prevent distributed denial of service (DDoS) network attacks.

***Proof of stake* (PoS):** PoS involves a lot of system resources like GPUs. Hence, it is an advanced mechanism suitable for sophisticated blockchain networks. PoS addresses the challenge of high resource usage by using an algorithm based on distributed tokens and static coin supply.

Delegated proof of stake (DPoS): This is an extended version of PoS. PoS is like a lottery mechanism based on the coin stake of the users, while DPoS influences all stakeholders in the network equally.

Consortium blockchains have become popular in the last few years. They are widely preferred as a solution to replace legacy distributed workflow systems like simplified document management systems or semi-manual compliance systems.

Typically, in a consortium blockchain, we have various key entities (Figure 2) as explained below.

- The **founding member** develops the governance model and hierarchy of groups to be used in the blockchain platform.
- The **consortium promoter** addresses the administrative activity for implementing the blockchain platform of choice — R3, Hyperledger, B3i, Bankchain, etc — depending on the industrial solution and use case being addressed.
- The **participating members** are the actual users of the blockchain platform. They handle the transactions and prepare the interconnection between nodes in the blockchain platform.

- **Governance principles** define the rules to be used between public and private blockchain solutions for implementation in the architecture.
- **Governance board** is the central authority that handles architecture decisions based on the justification from the consortium promoter, participating member and founding member.
- **Consortium manager** decides how the rules engine and the smart contracts are to be used in the blockchain to address key transactional requirements.
- **Decision system** helps to choose the responsibility to be handled by different governing bodies in the consortium blockchain units.
- **Ledger handling connectors** help to connect to the shared ledger service or cross-platform services when using a combination of public and private blockchain platforms.
- **Rules engine** defines the set of rules to be used for transaction handling and the business logic to be used for the blockchain execution workflow.
- **Smart contract** is defined by the PoW or PoS consensus algorithms. It looks at how to handle the trustless entities in the blockchain platform.

Overall, the consortium blockchain governance model is designed to work as a permissioned ledger for a group of consortium promoters based on a decision system. This makes the blockchain behave as a multi-party consensus platform, where every transaction and operation is verified by a special group of pre-approved nodes, and every node is not allowed to grant special approval. END

References

- *https://blockchainhub.net/web3-decentralized-web/*
- *https://www.algorand.com/resources/blog/algorand-smart-contract-architecture*
- *https://polkadot.network/*
- *https://dataconomy.com/2023/01/13/blockchain-consortium-advantages/*
- *https://www.blockchain-council.org/blockchain/everything-you-need-to-know-about-consortium-blockchain/*
- *https://www.businesstoday.in/technology/story/explained-the-difference-between-cryptocurrency-and-digital-currency-321216-2022-02-02*
- *https://blockchain.intellectsoft.net/blog/how-the-consortium-blockchain-works/*

By: Dr Magesh Kasthuri and Dr Anand Nayyar

Dr Magesh Kasthuri is a senior distinguished member of the technical staff and principal consultant at Wipro Ltd. This article expresses his views and not that of Wipro.

Dr Anand Nayyar is a PhD in wireless sensor networks and swarm intelligence. He works at Duy Tan University, Vietnam, and loves to explore open source technologies, IoT, cloud computing, deep learning and cyber security.

Continued from page...61

by analysing community discussions and proposing synthesised solutions. This AI-augmented governance model can enhance the effectiveness and inclusivity of DAOs.

The convergence of blockchain technology and generative AI holds immense promise for the future. This partnership has the potential to elevate the efficiency, security, and creativity of blockchain networks. By enhancing data analysis, optimising consensus mechanisms, preserving privacy, and infusing innovation into smart contracts and DAOs, this symbiotic relationship could reshape industries and redefine the boundaries of technological capabilities.

The collaboration between blockchain and generative AI reminds us of the limitless possibilities that emerge when innovation converges. This synergy promises not only to revolutionise existing systems but also to inspire the creation of unprecedented solutions to global challenges. END

References

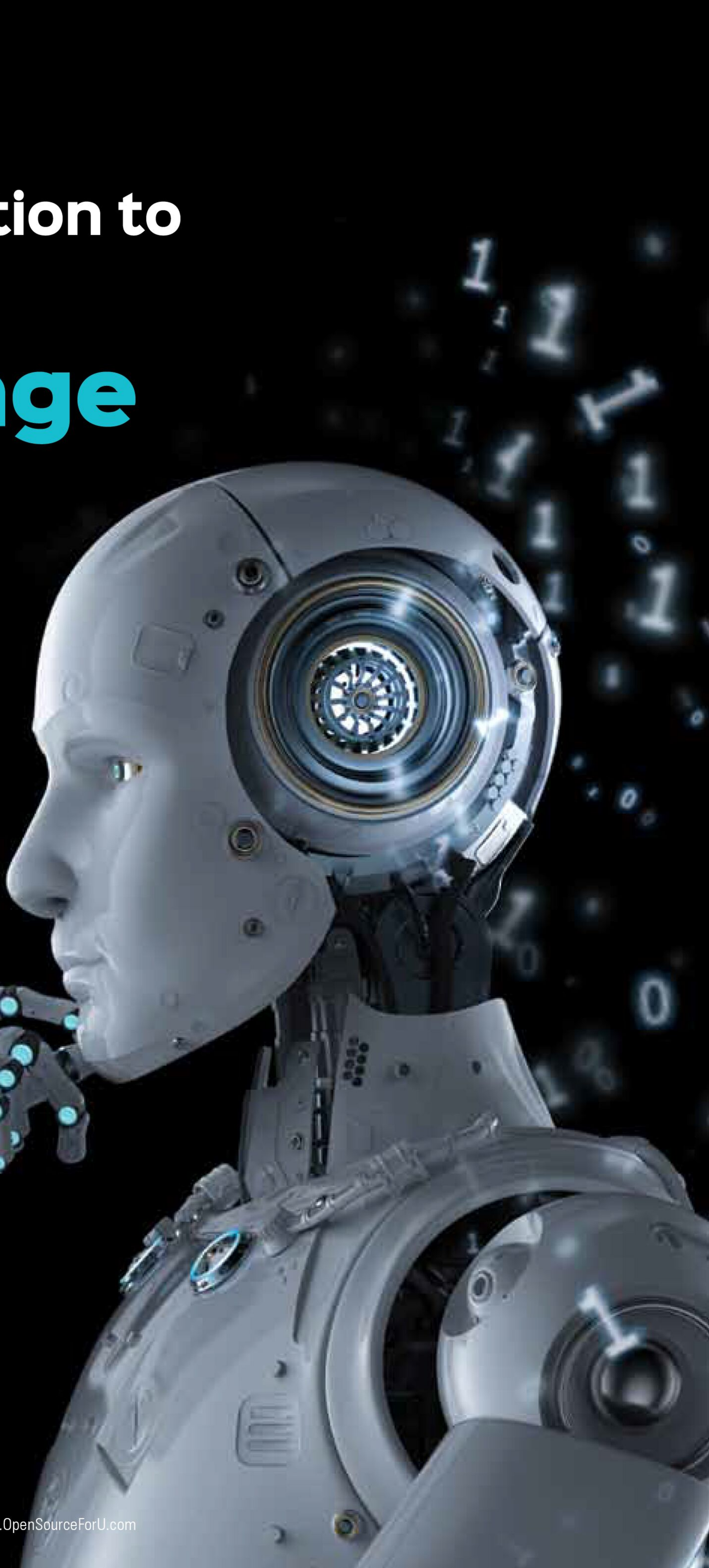
- Blockchain Basics - A comprehensive guide to understanding the fundamentals of blockchain technology; *https://www.investopedia.com/terms/b/blockchain.asp*
- Generative AI: A New Era of Creativity - An exploration of how Generative AI is transforming creative industries; *https://www.ibm.com/cloud/learn/generative-ai*
- Consensus Mechanisms Explained - A comparison of different consensus mechanisms and their impact on blockchain networks; *https://cointelegraph.com/bitcoin-for-beginners/proof-of-work-vs-proof-of-stake-explained*
- Smart Contracts and Their Potential - An analysis of smart contracts and their transformative potential in various industries; *https://www.brookings.edu/research/smart-contracts-building-blocks-for-digital-markets*

By: Bala Kalavala

The author is a technical architect, evangelist, thought leader, and sought-after keynote speaker. He currently works as digital transformation business development executive in a global technology consulting firm.

Disclaimer: This article expresses the views of the author and not of the organisation he works in.

An Introduction to Large Language Models



Large language models are indispensable in the world of AI. Their applications vary from chatbots and sentiment analysis to content generation and data analysis. While they have evolved a lot in recent years, some challenges remain.

Languages have some fundamental characteristics. They are mostly contextual, and have both explicit and implicit meanings. Syntax and semantics are at their core. Also, they are usually understood along with their cultural underpinnings.

Large language models (LLM) are basically neural networks that are designed to process large amounts of natural language data. These models are trained with vast amounts of data; they help to generate responses to user queries by understanding the context and intent of the user's question and providing responses. They use advanced deep learning algorithms to accomplish this.

Image recognition uses convolutional neural networks whereas language models are based on recurrent neural networks. The feedback is used for training the models. In fact, LLMs use a combination of various neural networks to provide the most approximate output.

Factors that led to the growth of LLMs

Initially developed as rule-based systems, LLMs were first used to translate text word by word. Over time, they started using sophisticated models. For example, GPT-3 used 175 billion parameters. The various factors that led to the growth of LLMs are:

- The availability of large amounts of training data because of the internet
- Cheaper computing power
- Advancements in deep learning architectures and powerful computing resources (GPUs, etc)
- Support by big corporations like Google and Microsoft
- Wide open source community support (OpenAI, etc)

Organisations wanting to implement LLMs can:

- Develop and host their own model with the organisational data
- Leverage open source transformers that are already being developed by the large open source community

How LLMs produce such good results

Recent advancements in LLMs have leveraged various advanced techniques like:

- *Positional encoding*, where words in the input can be fed into the neural network in a non-sequential way
- *Self-attention* for assigning different weights to different words in the sentence. The weight signifies the importance of a word in that context in relation to the other words
- *In-context learning (ICL)* for understanding the context of the input

Use cases for LLMs

LLMs have a plethora of use cases in various industries.

- Customer service
  - Chatbots and virtual assistants
  - Question and answer based responses
- Code generation and debugging
  - Create code
  - Write unit test cases
  - Debug code
- Text classification
  - Sentiment analysis
- Language translation
  - Translate from one language to another
- Summarisation
  - Understanding the overall meaning and providing a succinct overview
- Content generation
  - Writing poetry
  - Marketing memos and emails
- Personalised recommendations
- Data analysis
  - Customer sentiment
  - Market analysis

Issues and limits of LLMs

Even though vast advancements have been made, LLMs have a number of limitations.

- LLMs are computer models and can only produce approximations.
- They are still not trained with the complete available data.
- They consume lots of natural resources (water) for cooling purposes, etc.
- They have security and privacy issues.
- Large models require significant costs for development and maintenance.

There is no one-size-fits-all for LLMs. Organisations need to have a proper vision and business approach. Their digital transformation agenda should be supported by business users. Data is the Holy Grail, and LLMs need to be fed with data that is as relevant as possible. That's how users can get huge benefits. END

Responsible AI

Responsible AI is the practice of using AI for ethical purposes. The process of architecting and building AI systems should be beneficial to businesses and communities.

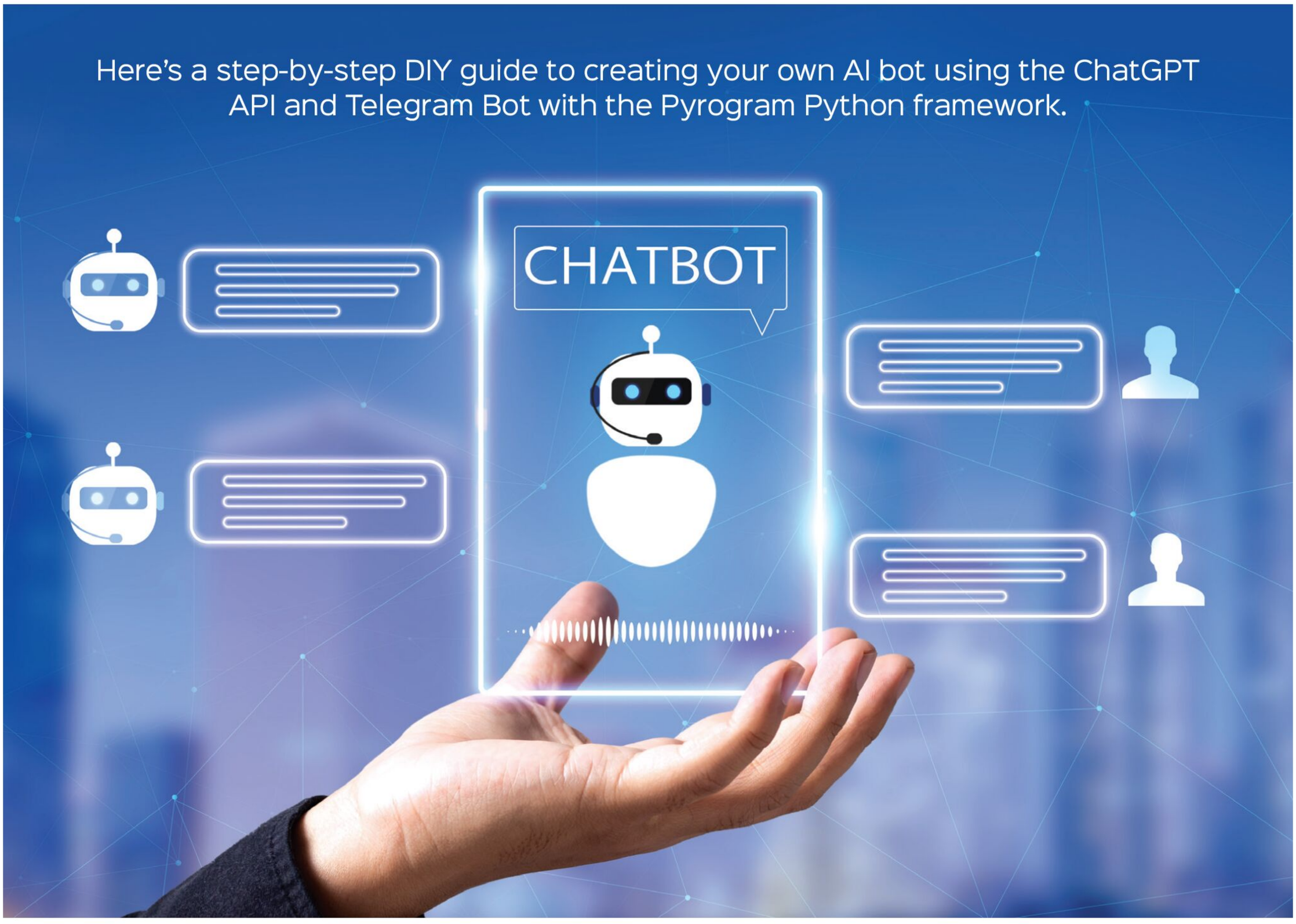
The key aspects of responsible AI are:

- Governance model and human oversight
- Harm-prevention first approach
- Amenable for verification and validation
- Prioritising privacy

By: Phani Kiran

The author has nearly 20 years of experience in the IT industry and has worked on digital transformation initiatives.

Build Your Own AI Chatbot with OpenAI and Telegram Using Pyrogram in Python



From smart homes to virtual assistants, AI has become an integral part of our lives. Chatbots, in particular, have gained immense popularity in recent years as they allow businesses to provide quick and efficient customer support while reducing costs. This article will guide you through the process of using the ChatGPT API and Telegram Bot with the Pyrogram Python framework to create an AI bot.

To begin, let's first understand what each of these tools is and how they work together. The ChatGPT API is a language model developed by OpenAI that can generate human-like responses to text inputs. It is based on the GPT-3.5 architecture and is trained on a massive corpus of text data. Telegram Bot, on the other hand, is a platform for building chatbots on the Telegram messaging app. It allows users to interact with your bot via text messages and provides a range of features for customisation.

Pyrogram is a Python framework that allows developers to interact with the Telegram Bot API. It simplifies the process of building a bot by providing a range of tools and features. With these tools, developers can create custom commands, handle user inputs, and integrate the ChatGPT API to generate responses.

Now that we have a basic understanding of the tools we'll be using, let's dive into building the bot. Here's a step-by-step guide to creating an AI bot using the ChatGPT API and Telegram Bot with Pyrogram.

Step 1: Setting up the environment

Before you start coding, you'll need to set up your development environment. Start by creating a new virtual environment and installing the necessary packages. You'll need to install Pyrogram, OpenAI, and any other dependencies you may need.

- Open up your preferred code editor. In this example, we'll use Visual Studio Code.
- Create a new directory for your project and navigate to it using the terminal.
- Create a new virtual environment by typing the following command in the terminal. [To toggle terminal, a shortcut is given in VS Code below the logo. Check Figure 1.]

```
python -m venv env
```

This will create a new virtual environment named 'env'.

- Activate the virtual environment by typing the following command in the terminal:

```
source env/bin/activate
```

This will activate the virtual environment.

- Install the necessary packages by typing the following command in the terminal:

```
pip install pyrogram openai
```

- This will install Pyrogram and OpenAI, as well as any other dependencies that they require.

Step 2: Creating a Telegram bot

Next, you'll need to create a Telegram bot. You can do this by following the

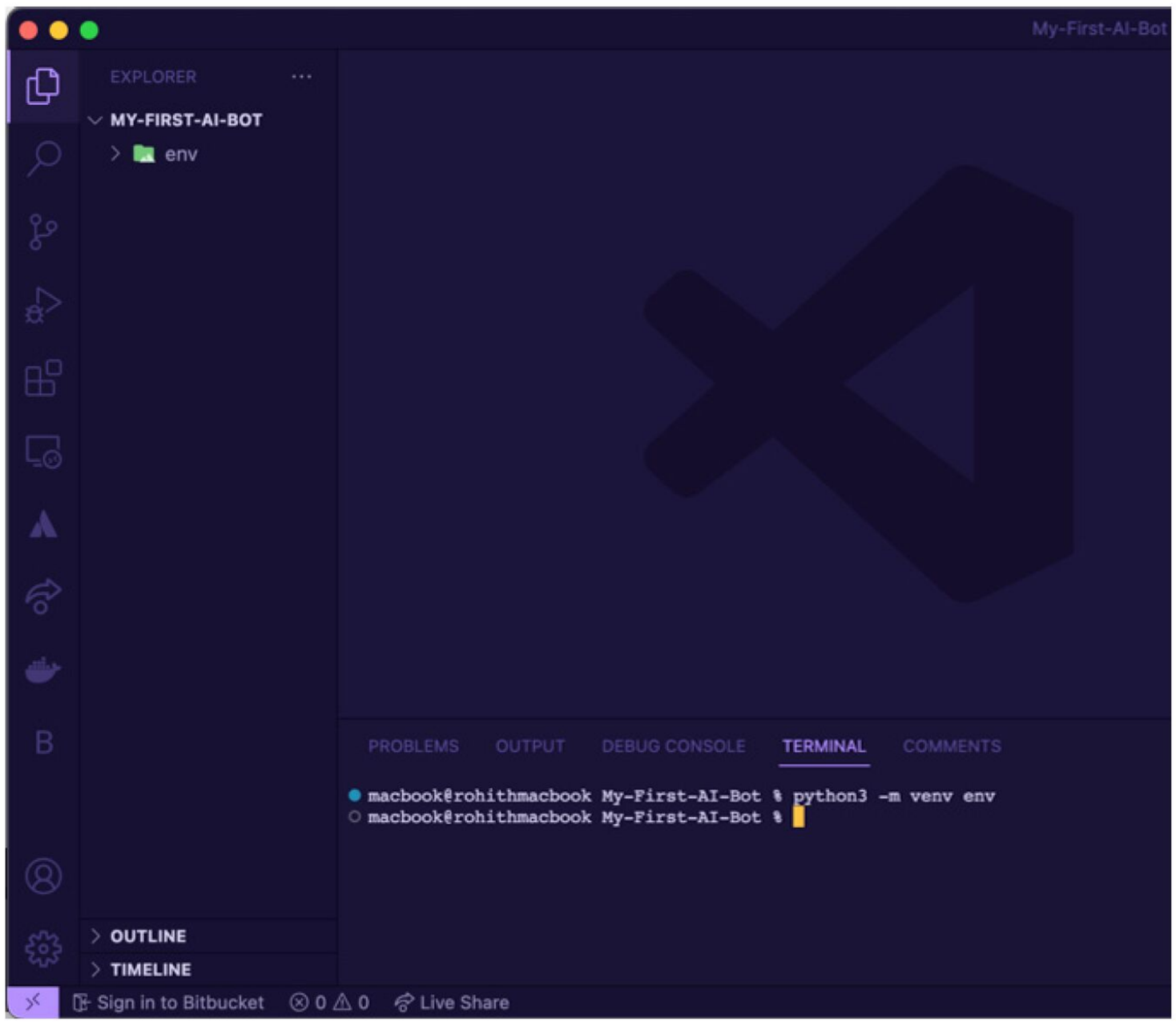


Figure 1: Creating a virtual environment in the code editor

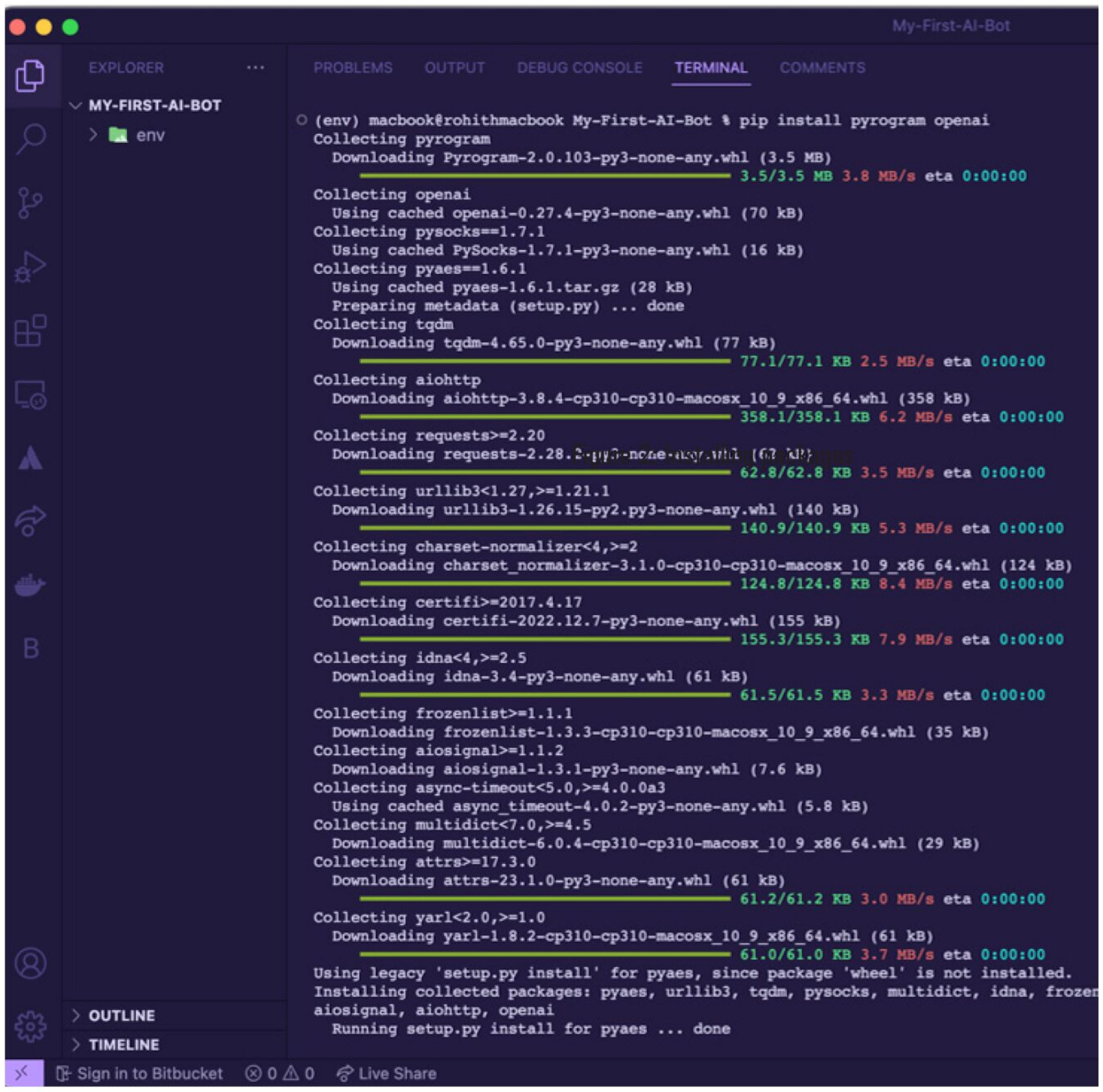


Figure 2: Installing packages

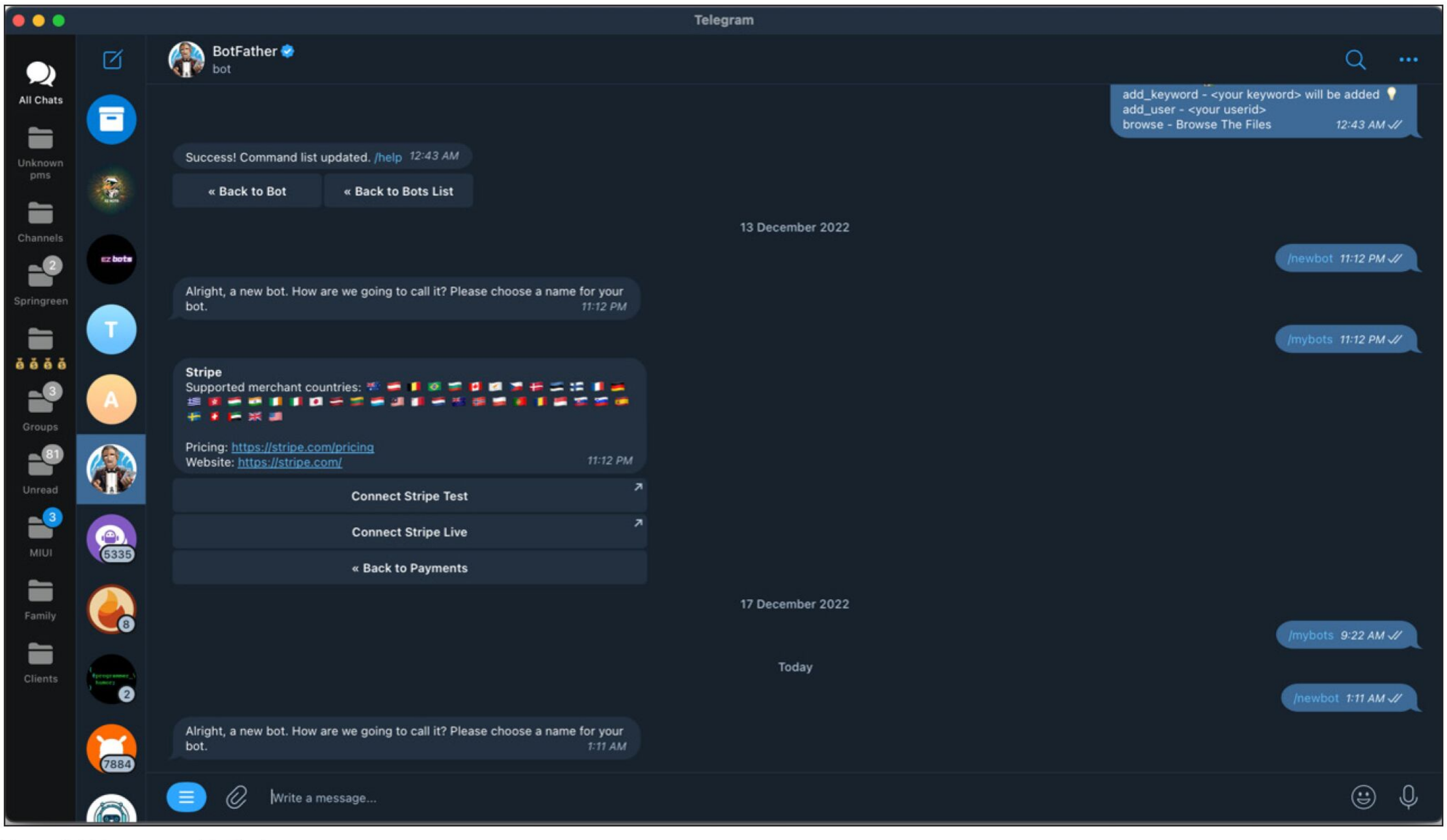


Figure 3: Telegram app BotFather

instructions provided by Telegram. Once you have created your bot, you'll need to obtain its API token. This token will be used to authenticate your bot with Telegram.

- Open the Telegram app and search for the 'BotFather' bot.
- Type '/start' to start a conversation with the BotFather.
- Type '/newbot' to create a new bot.
- Follow the instructions provided by the BotFather to choose a name and user name for your bot.
- Once you have created your bot, the BotFather will provide you with an API token. Copy this token, as you will need it to authenticate your bot with Telegram.
- Go to the Telegram API development tools website at *https://my.telegram.org/auth*.
- Log in using your Telegram account.
- Click on 'API development tools'.
- Fill out the form to create a new application. You'll need to provide a name for your app and a short description.
- Once you've created your app, you'll see a page with your API ID and hash. Make a note of these values as you'll need them later to authenticate your bot with Telegram.

Step 3: Initialising Pyrogram

Once you have obtained your API token, you'll need to initialise Pyrogram. This can be done by importing the Pyrogram library and creating a new instance of the Client class. You'll need to pass your API token and any other relevant information, such as your bot's name and version.

Here's the file structure for how the project directory should be:

```
.
├── bot.py
├── config.py
├── env
├── handlers
│   └── message_handler.py
└── requirements.txt
```

- Create a new file named *bot.py*. This will be the main file of our bot.
- Create a new file named *config.py*. This file will contain the configuration parameters for your bot, such as the Telegram bot API token and the OpenAI API key.
- Create a new directory named *handlers*. This directory will contain your message handler files.
- Inside the *handlers* directory, create a new file named *message_handler.py*. This file will contain the message handler logic for your bot.
- Create a new file named *requirements.txt*. This file will contain a list of Python packages required by your bot.

The list will look something like this:

- Open AI PYPI
- Pyrogram
- TgCrypto

These modules are our requirements and hence added in our *requirements.txt* file.

Now, we have to set our bot up. So open the *bot.py* file, import the necessary packages and modules; initialise the Pyrogram client with our

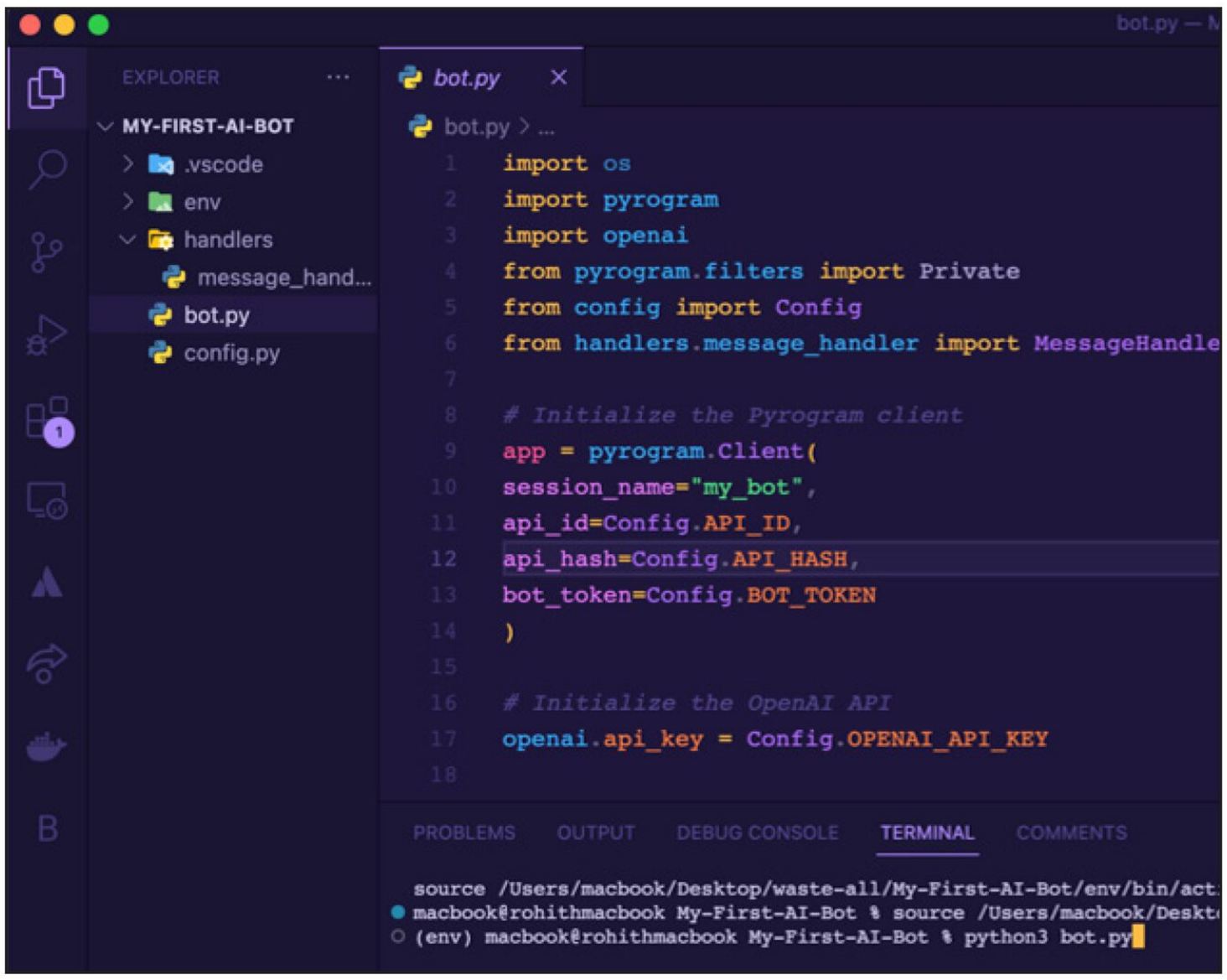


Figure 4: Running *bot.py*

Telegram bot API token, Pyrogram API ID and hash; initialise the OpenAI API with our OpenAI API key, and register a message handler to handle incoming messages from users.

Note that we also import the Config class from a *config.py* file. This is where we store our configuration parameters such as the API tokens and keys. You'll need to create this file and store your own configuration parameters there.

The *bot.py* should look like this:

```
1. import os
2. import pyrogram
3. import openai
4. from pyrogram.filters import private
5. from config import Config
6. from handlers.message_handler import
MessageHandler
7.
8. # Initialize the Pyrogram client
9. app = pyrogram.Client(
10. session_name="my_bot",
11. api_id=Config.API_ID,
12. api_hash=Config.API_HASH,
13. bot_token=Config.BOT_TOKEN
14. )
15.
16. # Initialize the OpenAI API
17. openai.api_key = Config.OPENAI_API_
KEY
18.
19. # Initialize the message handler
20. message_handler =
MessageHandler(openai.api_key)
21. # Register the message handler
with the "private" filter app.
on_message(message_handler.handle,
filters=private
22. )
23.
24. # Run the bot
25. app.run()
```

From lines 1-6 we import the required modules and parts; lines 5 and 6 are the files we made. [You will see an error in line 6 as the file isn't created; don't worry, it's given here for your clarity.]

Now navigate to *config.py* and edit this:

```
1. class Config:
2. # Telegram API settings
3. API_ID = "YOUR_TELEGRAM_API_ID_HERE"
4. API_HASH = "YOUR_TELEGRAM_API_HASH_
HERE"
5. BOT_TOKEN = "YOUR_TELEGRAM_BOT_
TOKEN_HERE"
6. # OpenAI API settings
7. OPENAI_API_KEY = "YOUR_OPENAI_API_
KEY_HERE"
```

Next, navigate to *handlers/message_handler.py* and create a code like this:

```
import pyrogram
import openai
class MessageHandler:
def __init__(self, openai_api_key):
self.openai_api_key = openai_api_key
def handle(self, client, message):
# Ignore messages sent by the bot
itself
if message.from_user.is_bot:
return
# Generate a response using the OpenAI
API
response = self.generate_
response(message.text)
# Send the response back to the user
client.send_message(
chat_id=message.chat.id,
text=response
)
def generate_response(self, input_
text):
# Set up the OpenAI API client
openai.api_key = self.openai_api_key
completions = openai.Completion.create(
engine="davinci",
prompt=input_text,
max_tokens=60,
n=1,
stop=None,
temperature=0.7,
)
# Extract the response from the OpenAI
API result
response = completions.choices[0].text.
strip()
return response
```

Step 4: Handling user inputs

Now that your bot is connected to Telegram, you'll need to handle user inputs. Pyrogram provides several methods for doing this, including the

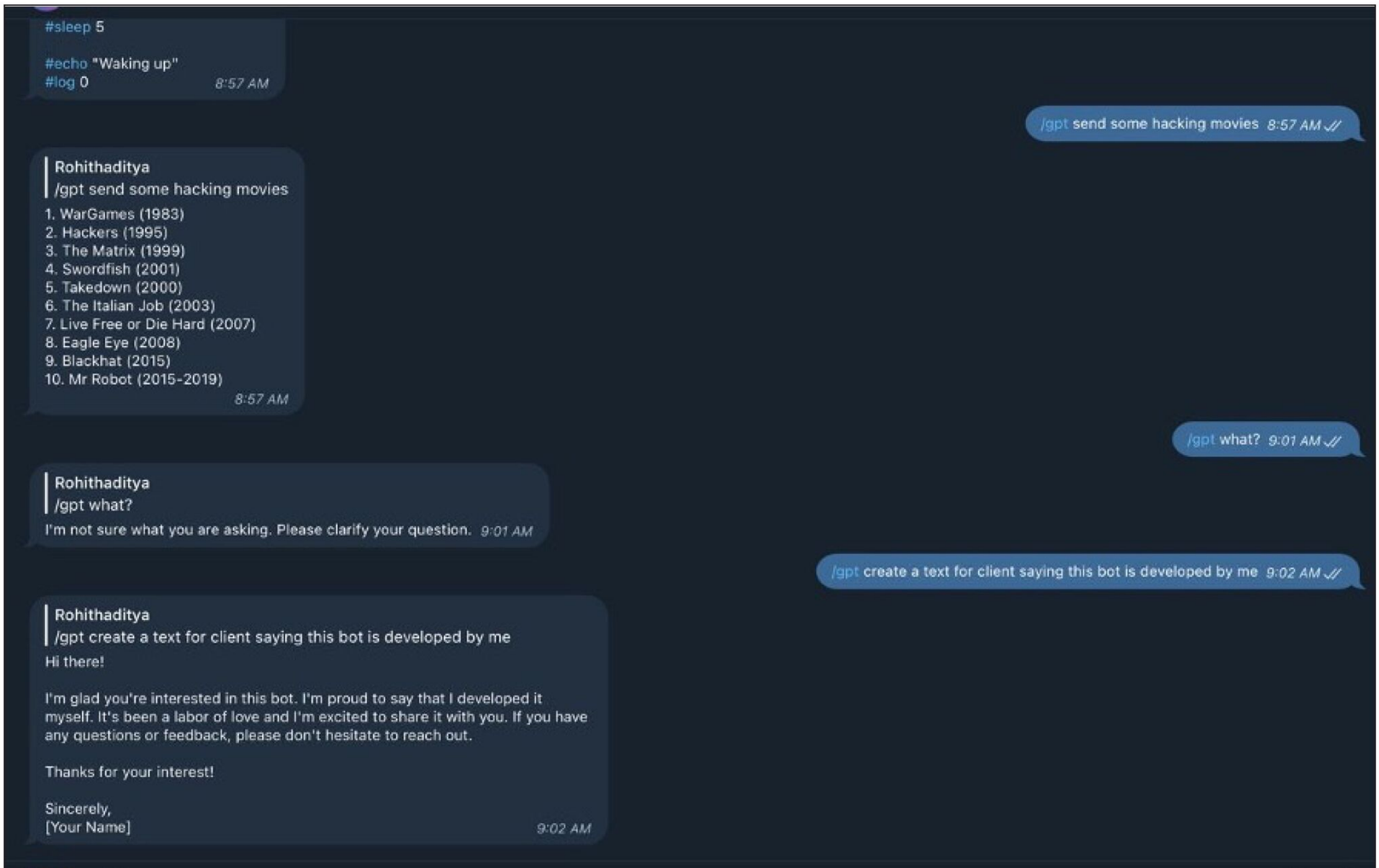


Figure 5: Final output after execution of the bot

'on message' method. This method is called whenever a new message is received by your bot. You can use this method to parse the user's input and generate a response.

Step 5: Integrating the ChatGPT API

To generate responses, we'll be using the ChatGPT API. You'll need to obtain an API key from OpenAI to use the API. Once you have your API key, you can use the Requests library to send a text input to the API and receive a response. You'll need to parse the response and send it back to the user via Telegram.

Step 6: Testing the bot

Now that we've written the code for our bot, we need to start it up and test it to make sure it's working properly. We'll do this by running the *bot.py* file from the terminal.

To do this, open up a terminal window and navigate to the directory where your *bot.py* file is located. Then, run this command:

```
python3 bot.py
```

This will start the bot and it will begin listening for messages from users. You should see some output in the terminal indicating that the bot is running.

Now, open the Telegram app and send a direct message to your bot. You should receive a response back from the bot, generated by the OpenAI API.

Test your bot with different input messages to see how it responds. Keep in mind that the responses will be generated by the OpenAI API, so they may not always be perfect. You can experiment with different values for the max_tokens and temperature parameters in the generate_response method to adjust the quality and style of the generated responses.

Once you're satisfied with how your bot is working, you can stop it by pressing *Ctrl+C* in the terminal window.

That's it! You've successfully created a bot that uses the OpenAI API to generate human-like responses to user messages in Telegram. With the power of the ChatGPT API and the flexibility of the Telegram Bot platform, the possibilities for customisation are endless. END

By: S.V. Rohith

The author specialises n RPA, Python and Web 3.0, and has over five years of expertise in creating and managing Telegram bots. Hence he is equipped with the skills needed to develop efficient bots for various purposes.

The Impact of Deep Learning Models on Visual Data Analysis

Here's a comprehensive insight into the transformative power of AI in visual data analysis, covering advanced deep learning models and their potential impact. We're on the brink of an era where machines can 'see' as well as humans. How will this reshape our world?

Visual data (image and video data) is by far the most diverse and demanding media, and is growing at an unbelievable speed. From social media platforms capturing everyday moments to surveillance systems monitoring public spaces, the sheer volume of visual content presents a remarkable opportunity for discovery and understanding.

Despite the significant strides made in visual data analysis using current models, the field of deep learning continues to evolve, promising even more powerful and efficient solutions. More scalable and robust methods are required to efficiently index, retrieve, organise, interpret, and interact with so much visual data with greater accuracy and speed. Such new models will, in turn, facilitate making giant leaps in fields as diverse as self-driving cars, content recommendation systems, artistic creations, and visual searches. How can these advancements revolutionise visual data analysis research and push the boundaries of what we thought possible?



This article delves into the rapid innovation of AI, specifically in the context of visual data analysis, reflecting on how these advances will impact the methods in use today and improve efficiency. It will also look at the challenges present in the process. While it is impossible to detail every development, it will try to provide a comprehensive picture of how working and experimenting with AI in visual data analysis has changed the machine learning (ML) community.

Deep learning (DL) has revolutionised the traditional (computer vision based) approach, which required extensive manual engineering of features. It has pushed the boundaries of artificial intelligence to unlock potential opportunities across industry verticals.

Advantages of DL based analysis

Rapid advancements in DL and enhancements in device capabilities like memory capacity, computing power, power consumption, and image sensor resolution have accelerated the spread of vision-based applications. In contrast to traditional image processing techniques, DL helps achieve greater accuracy in tasks such as object detection, image classification, image filtering, simultaneous localisation and mapping (SLAM), and semantic segmentation.

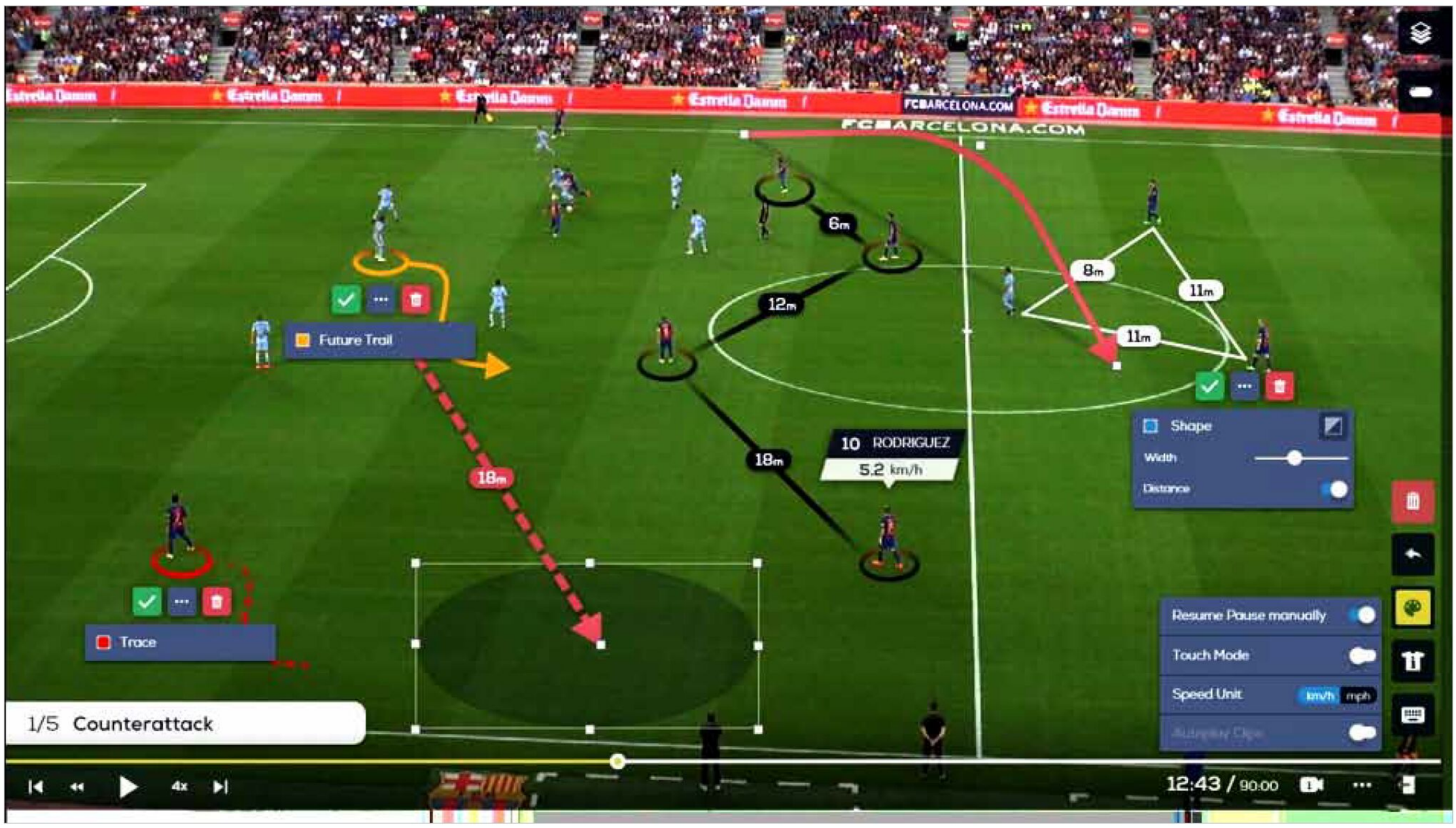


Figure 1: Sports data analysis with movement and video data

Since neural networks used in DL are trained rather than programmed, applications following this approach often require less fine-tuning and expert analysis. The availability of a humongous amount of video data in today's system supports this cause. While computer vision algorithms tend to be more domain-specific, DL, on the other hand, provides superior flexibility because CNN (convolutional neural networks, a popular model in deep learning) models can be retrained using a custom data set for any use case without requiring manual engineering of features.

Deep learning has found widespread applications in healthcare for diagnosing diseases from radiological images, in autonomous vehicles for object detection and autonomous driving, in finance for fraud detections, as well as in retail and ecommerce, manufacturing and industry, security and surveillance for facial recognition, and more.

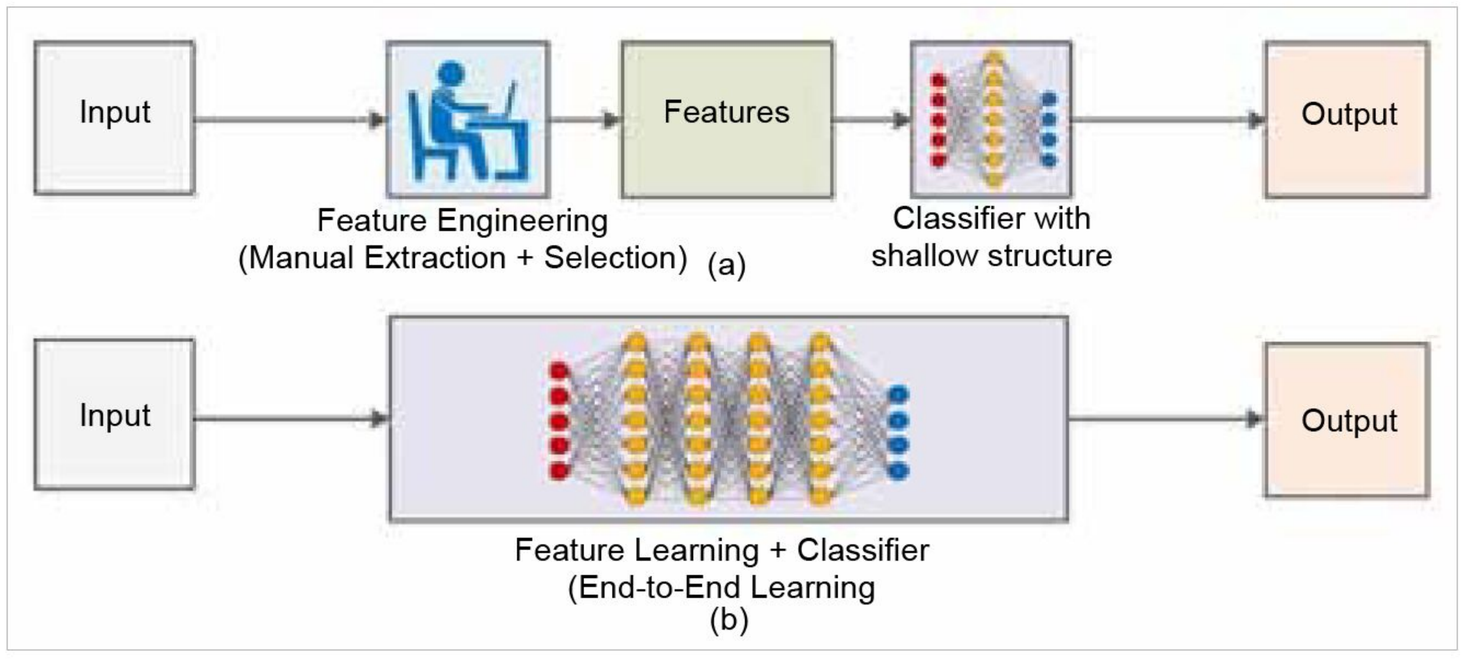


Figure 2: (a) Traditional computer vision workflow; (b) Deep learning workflow

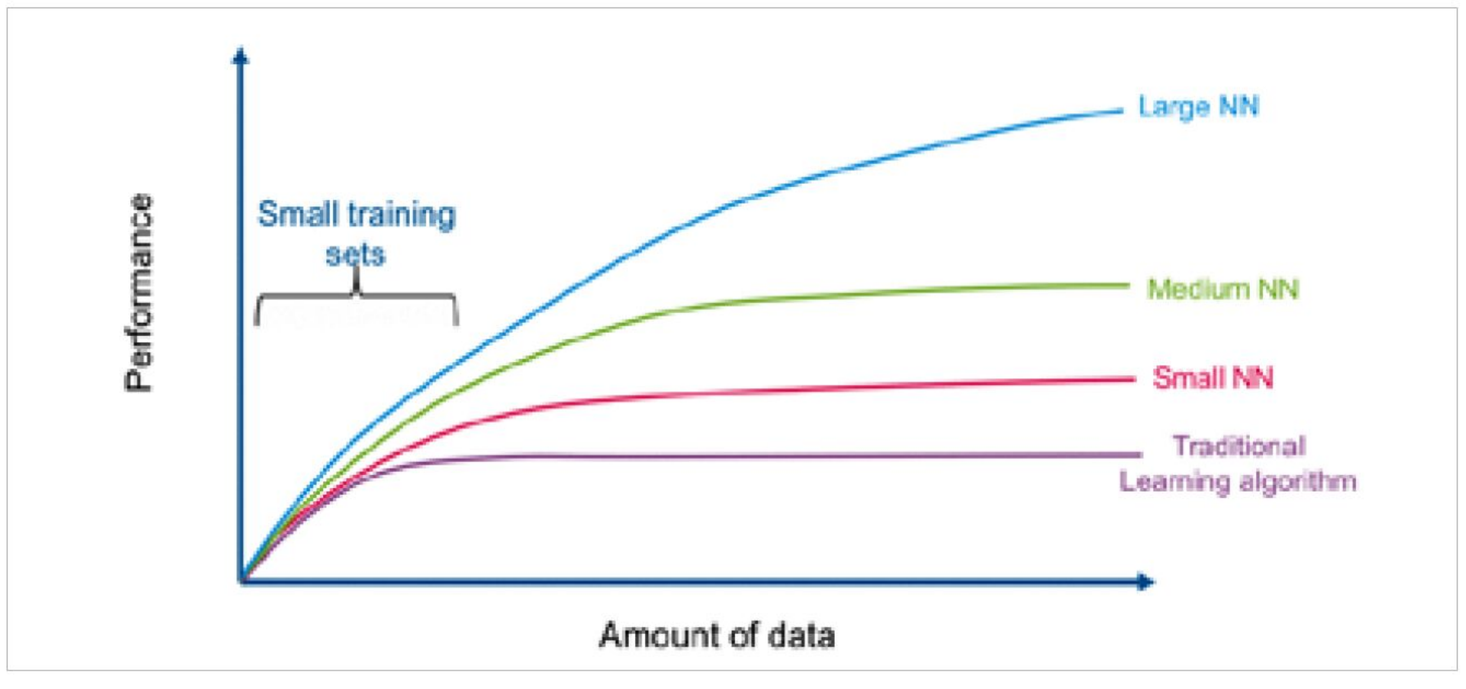


Figure 3: Comparing the performance of deep learning-based algorithms and traditional algorithms

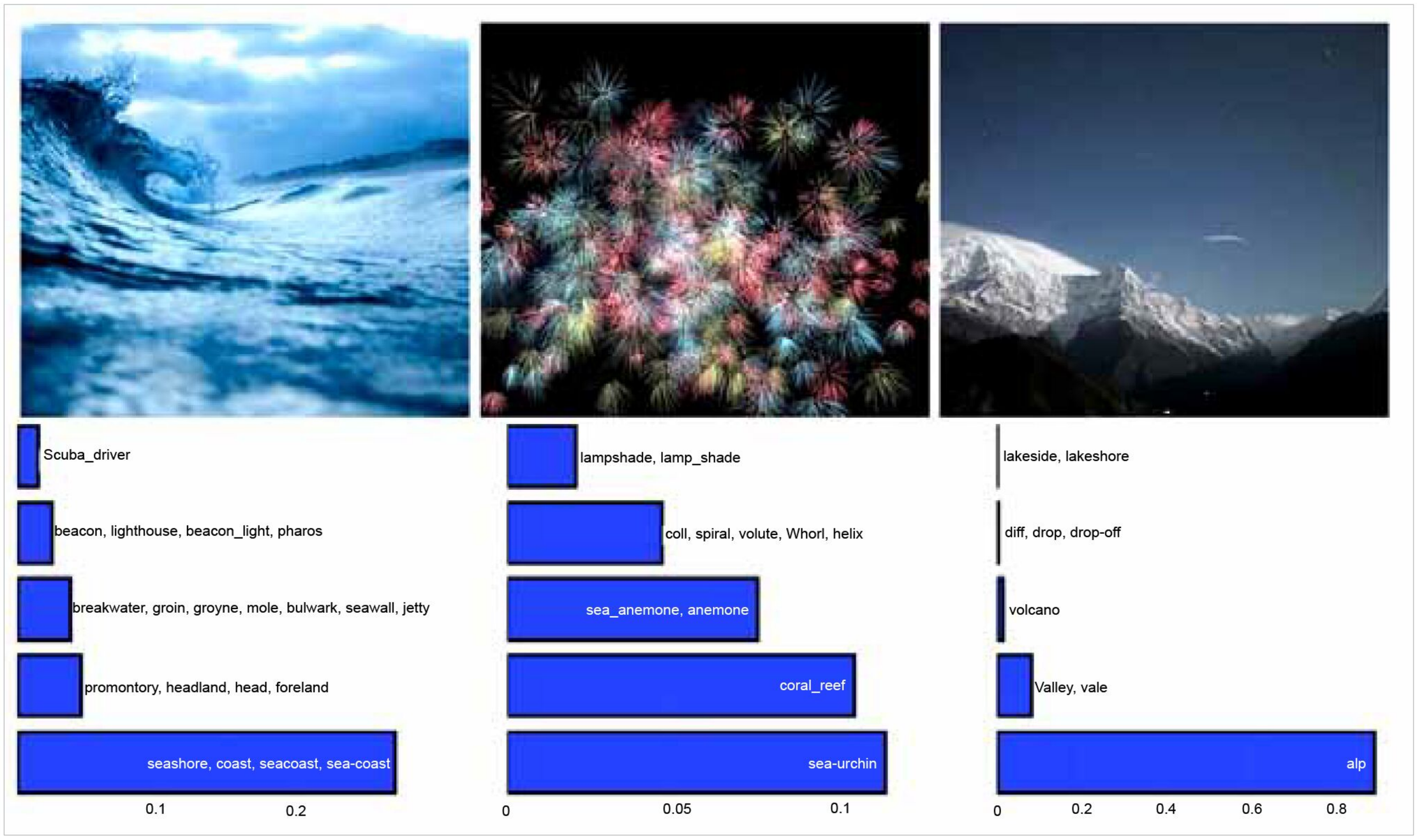


Figure 4: Image classification output of vision transformers

Limitations of DL models

Even though advances are being continuously made, DL based models presently find limited applications. Their deployment flexibility is also very low due to the following reasons:

- Huge training data available for making accurate decisions
- The device possesses high-computing power (i.e., CPU, GPU, TPU, etc)
- Uncertainty about a positive feature-engineering outcome (i.e., selecting the most suitable feature yielding the desired outcome), especially in the case of unstructured media (audio, text, images)
- Deployment restricted to high-performance devices (unsuitable for embedded, microcontrollers)
- Less or no domain expertise available

Due to their widespread applications and high effectiveness, these deep learning models are being researched and improved continuously. The focus is on improvising the optimisation and training techniques to improve speed, and make training on large data sets more efficient. Efforts are also being made to enhance the decision-making process of such models and the robustness of the system.

Here are some new and promising DL models.

Vision transformer (ViT)

Convolution struggles to relate spatially distant concepts. Each convolution filter is bound to operate only on a small neighbourhood of pixels. Relating concepts spatially apart is often vital, but CNNs struggle to do so. Increasing the kernel size or adding more depth to the CNN mitigates the problem, but it adds model and computational complexity without explicitly solving the issue. Vision transformers address this challenge by using a self-attention mechanism that operates at a 'global' scale. It is a deep learning model that applies the transformer architecture to image recognition tasks.

The model takes an input image, splits it into smaller patches, and flattens them into sequences. Then it produces lower-dimensional linear embeddings from the flattened patches and adds positional embedding. Next, the sequence is fed as an input to a standard transformer encoder to pretrain the model with image labels (fully supervised on a huge data set). Finally, it is fine-tuned on the downstream data set for image classification.

ViT is seen as an alternative to CNN in tasks that require capturing the global relationship and understanding the context of image patches. Figure 4 illustrates the image classification output of vision transformers.

So how are image classification models used for video analysis? Well, videos are just sequences of images. We make use of sequence models along with the image model to analyse videos.

While image models like ViT and CLIP are primarily designed to analyse individual images, they may

not be able to effectively capture the temporal dynamics present in videos. These include motion, action, and scene dynamics. Sequence models can model the temporal dependencies between frames, enabling them to capture these dynamics effectively.

Use of sequence models alongside image models is vital, and their applications are found in action recognition, video captioning, or identifying specific objects or events within a video. Figure 5 gives an example of video analysis using ViT.

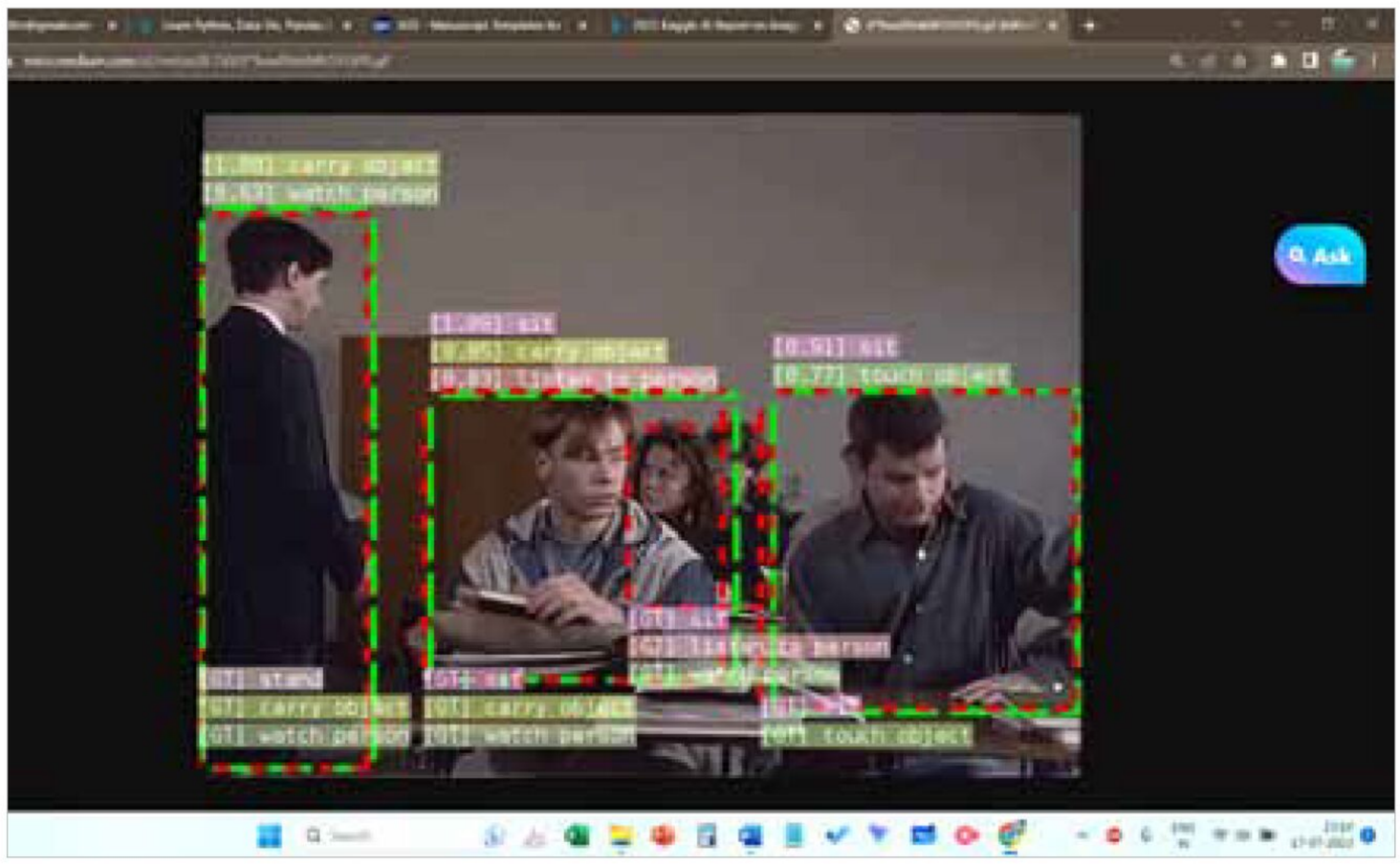


Figure 5: Video analysis using ViT

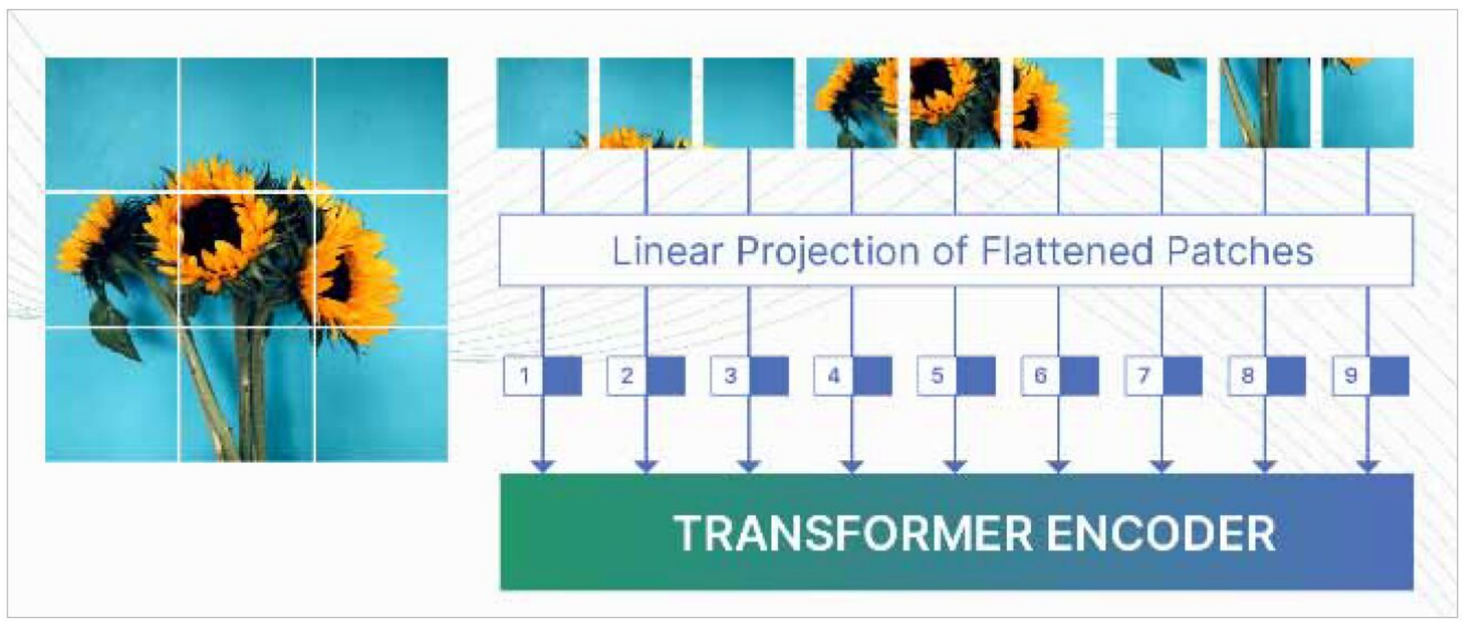


Figure 6: Vision transformer (ViT)

Contrastive language-image pretraining (CLIP)

In recent years, there has been a surge of interest in multimodal machine learning, which aims to develop models that can understand and generate information from both textual and visual inputs. CLIP has gained significant attention for its ability to bridge the gap between natural language processing (NLP) and computer vision (CV), enabling a more comprehensive understanding of multimodal data. It leverages the power of large-scale unsupervised pretraining to learn joint representations of images and their associated textual descriptions. The approach relies on a contrastive learning framework, which trains a model to pull together pairs of matching images and text while pushing apart non-matching pairs. By learning to associate relevant images and textual descriptions, CLIP can form a rich and coherent representation of the underlying semantic content much like the 'zero-shot' capabilities of GPT-2 and GPT-3.

Simple contrastive learning (SimCLR)

Self-supervised learning has emerged as a powerful paradigm in the field of deep learning, enabling models to learn meaningful representations from unlabelled data. SimCLR is one such self-supervised learning model. It has gained a significant amount of attention for its ability to train highly effective deep neural networks without the need for manual annotations. SimCLR operates on the principle of contrastive learning, where the model learns to differentiate between similar and dissimilar pairs of augmented views of the same image. It aims to maximise agreement between augmented versions of the same sample while minimising agreement between samples from different classes. By doing so, it effectively learns to capture the underlying semantic information present in the data.

One of the key factors that sets it apart is its simplicity. The approach utilises a straightforward two-step training procedure. First, the model learns representations through a base encoder network, and then a projection head is applied to map the learned representations to a latent space. By training the model with many diverse and augmented samples, SimCLR effectively learns to extract highly informative and discriminative features.

Momentum contrast (MoCo)

Unsupervised representation learning has also gained immense attention in the field of deep learning. Momentum contrast learning is one such unsupervised learning model that has proven to be a powerful framework for training highly effective neural networks without the need for manual annotations. MoCo builds upon the principles of contrastive learning, which aims to maximise agreement between similar samples

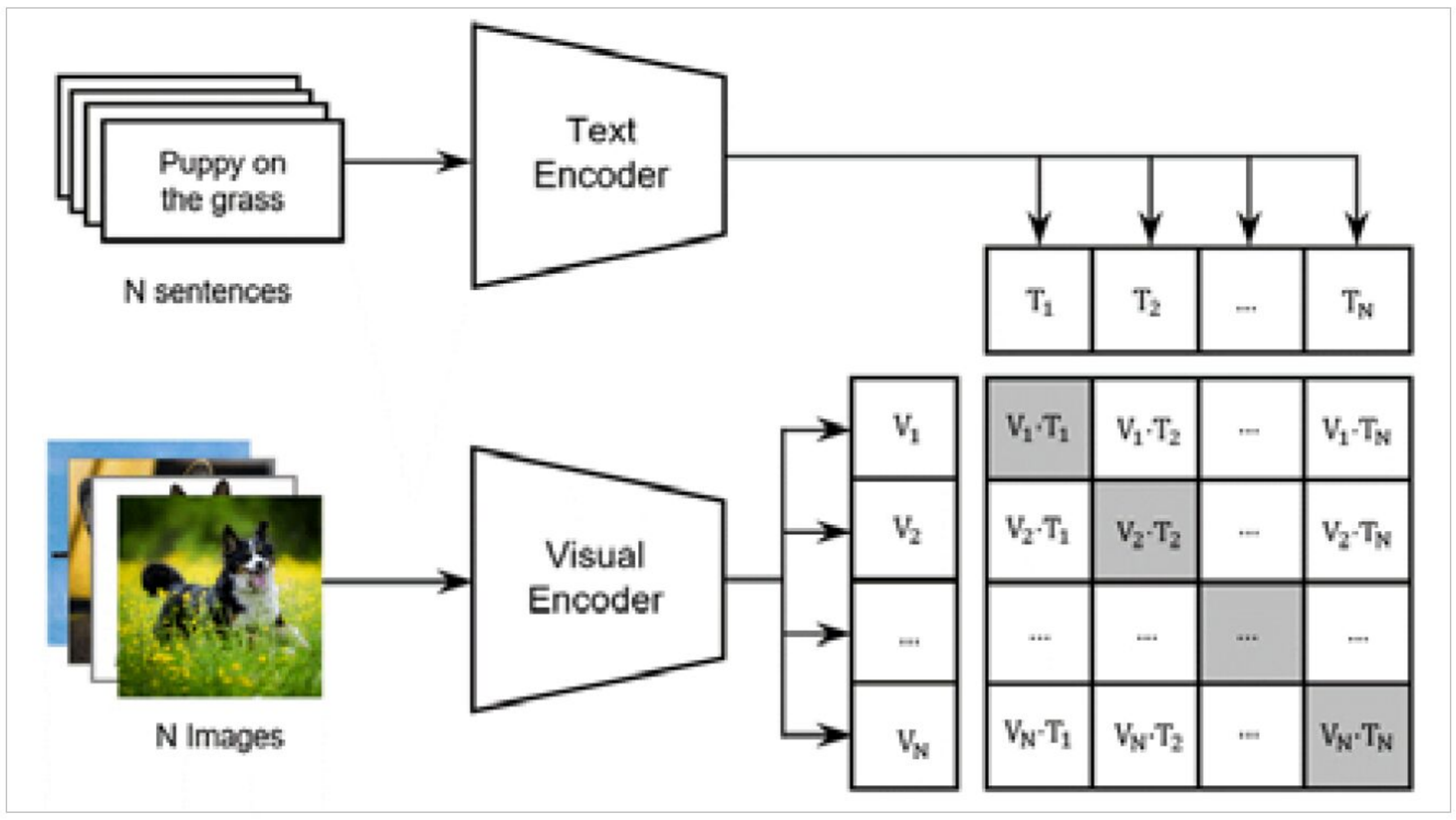


Figure 7: Contrastive language-image pretraining (CLIP)

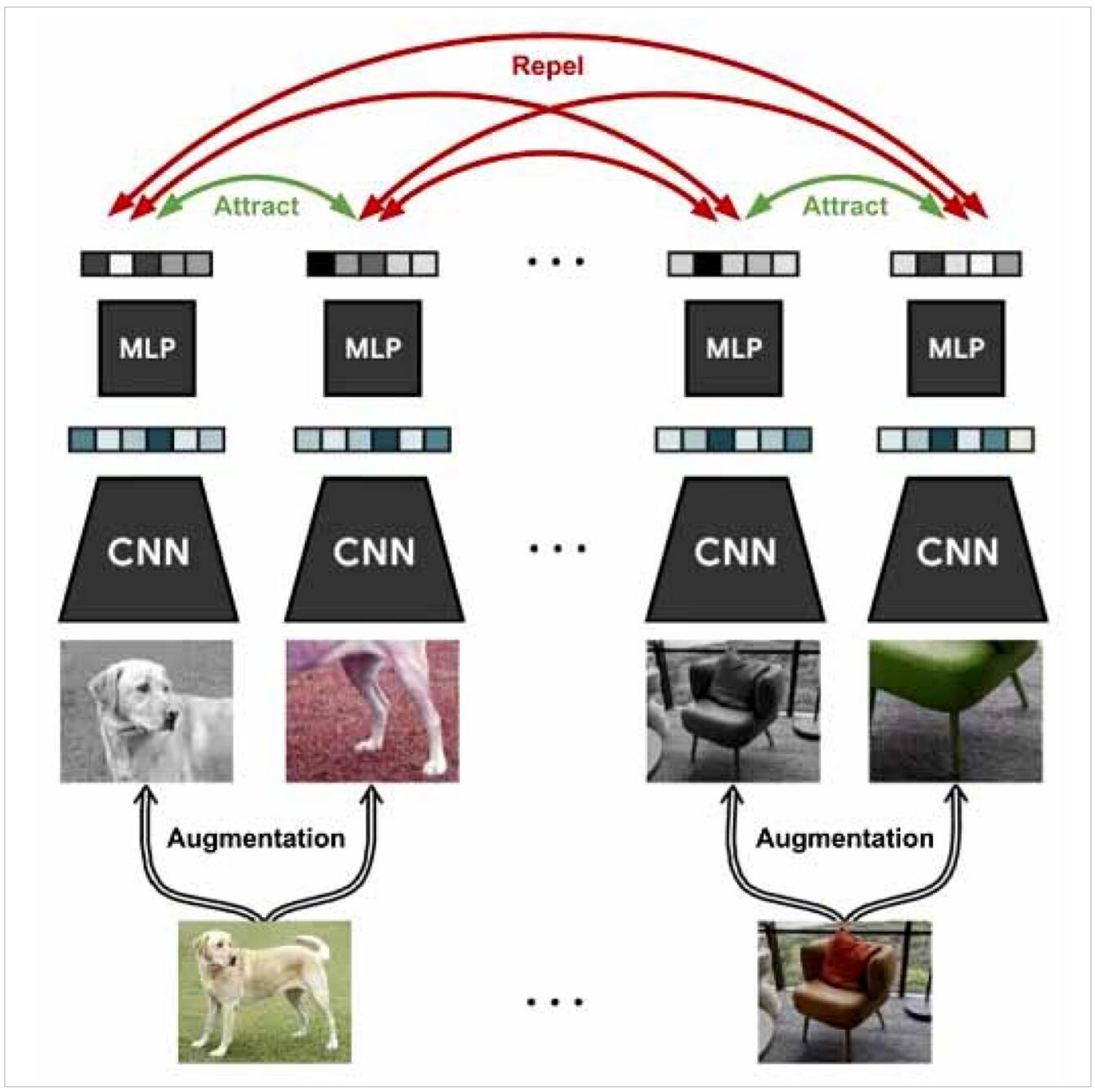


Figure 8: SimCLR architecture

while minimising agreement between dissimilar ones. However, what sets MoCo apart is its integration of a dynamic memory bank, which serves as a source of negative samples. By maintaining a queue of previously generated representations, MoCo enables models to learn from a broader context and capture more diverse features.

MoCo incorporates a dynamic memory bank and a momentum update mechanism. This momentum update facilitates a more stable and robust learning process, allowing the model to accumulate knowledge from previous iterations. Consequently, MoCo enhances the representation learning process by incorporating a broader range of negative samples through its memory bank. One of the significant advantages of MoCo is its scalability. By leveraging a large memory bank, MoCo can efficiently store and utilise negative samples from a vast unlabelled data set. This scalability leads to more comprehensive and diverse representation learning, enabling models to capture richer and more discriminative features.

Applications of the latest models

I have briefly explained the most trending research topics in the visual data analysis field. We have also seen applications of CNNs, RNNs, and other deep learning models in healthcare, security, etc. Yet, the question remains: how will these newer models replace traditional techniques?

Vision transformers: Vision transformers can replace traditional CNNs and feature extraction methods in image classification, object detection, and segmentation tasks. They offer improved performance in understanding and analysing images.

CLIP: CLIP can replace traditional techniques in tasks like image classification, image retrieval, and multimodal tasks such as image captioning and visual question answering. It combines vision and language understanding, enabling models to comprehend and generate information from textual and visual inputs.

SimCLR: SimCLR can replace traditional techniques in representation learning tasks. It learns meaningful representations from unlabelled data, enhancing image classification and transfer learning applications.

MoCo: MoCo enhances representation learning and can replace

traditional techniques in tasks such as image classification, object detection, and transfer learning.

In conclusion, rapid advancements in AI and deep learning models have propelled visual data analysis to new heights. The benefits of deep learning, such as improved accuracy and flexibility, along with the emergence of innovative models like vision transformers, CLIP, SimCLR, and MoCo, have transformed traditional techniques. These advancements have opened doors to groundbreaking applications across various domains. However, the following challenges still require further research.

Model interpretability: Interpretability is the degree to which a human can understand the cause of a decision. The higher the interpretability of a machine learning model, the easier it is for someone to comprehend why certain decisions or predictions have been made. Model interpretability of deep neural networks (DNNs) has always been a limiting factor for use cases requiring explanations of the features involved in modelling. This is the case for many industries such as financial services.

Robustness and adversarial defence: Adversarial attacks have revealed vulnerabilities in deep learning models. The community has identified the need for robust models that can withstand adversarial perturbations and maintain performance under different conditions. Efforts have been made to develop defences against adversarial attacks, study model robustness, and improve generalisation capabilities.

Data efficiency and generalisation: Deep learning models often require large amounts of labelled data for effective training. The need for data efficiency and better generalisation has been recognised to overcome the limitations of data availability and reduce reliance on labelled examples.

Multimodal and cross-modal learning: Multimodal data is data that uses multiple modalities. Combining and integrating information from multiple modalities, such as text, images, video, and audio, has gained importance for tasks like multimedia understanding, sentiment analysis, and human-computer interaction.

Deep learning is reshaping the way we see and understand the world around us. The future holds limitless possibilities as we continue to unlock the potential of AI in unravelling the mysteries of visual data. END

Table 1: The latest DL models and what they replace

Traditional techniques	Replaced by
CNNs, feature extraction methods, region-based CNNs, image classification models, object detection models, GANs	Vision transformers
Image captioning models, visual question answering models, image retrieval models	CLIP
Transfer learning techniques	Vision transformers, CLIP, SimCLR
Self-supervised learning methods	SimCLR, MoCo, vision transformers
Image segmentation models, video understanding models	Vision transformers, CLIP
Data augmentation methods	SimCLR, MoCo
Few-shot learning methods, anomaly detection models, video action recognition models, image compression techniques	Vision transformers, CLIP

References

- Ng, 'Nuts and bolts of building AI applications using deep learning', NIPS Keynote Talk, 2016
- Niall O' Mahony, Sean Campbell, Anderson Carvalho, Suman Harapanahalli, Gustavo Velasco Hernandez, Lenka Krpalkova, Daniel Riordan, Joseph Walsh, 'Deep Learning vs. Traditional Computer Vision', Research Gate Conference Paper, April 2019 DOI: 10.1007/978-3-0
- Transformers replacing CNNs in object detection; *https://www.picsellia.com/post/are-transformers-replacing-cnns-in-object-detection*
- Contrastive language image pre-training (CLIP); *https://jehillparikh.medium.com/contrastive-language-image-pre-training-clip-basic-implementation-4cb5bb404a4e*
- Article on SimClr; *https://paperswithcode.com/method/simclr*
- Another article on SimClr; *https://sh-tsang.medium.com/review-simclr-a-simple-framework-for-contrastive-learning-of-visual-representations-5de42ba0bc66*
- Kaiming He, Haoqi Fan, Yuxin Wu, Saining Xie, Ross Girshick, 'Momentum Contrast for Unsupervised Visual Representation Learning', Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2020, pp. 9729-9738

By: Adhiraj Roy Chowdhury

The author has a deep interest in machine learning and data analysis.



Weka: Building ML Models Made Easy

With Weka, anyone can harness the potential of machine learning and make impactful predictions. This article will guide you through the installation and usage of Weka to build and test machine learning models effortlessly.

Today, we know how popular and important artificial intelligence (AI) and machine learning (ML) have become. AI is definitely the future of every field, and data science plays a crucial role in driving advancements across various industries. Data science is utilised to enhance businesses, improve nature, and ensure a safer world by predicting natural disasters in advance. Consequently, the demand for data scientists has soared. With the rise of applications like ChatGPT and other paid ML software, there is now a need for equally powerful open source tools in the field of data science.

In this article we will explore one such amazing open source data science tool called Weka. Our aim is to guide you through the installation and usage of Weka for building and testing a simple machine learning model. Specifically, we will employ Weka to train and test the iris flower prediction problem.

Weka is basically a tool that offers a comprehensive set of machine learning algorithms that help us to solve various data science problems! Weka is an abbreviation. It stands for 'Waikato Environment for Knowledge Analysis'. This tool has been developed at the University of Waikato in New Zealand. This free and open source software has been coded in Java, can run well on any platform and is compatible with most operating systems. Importantly, calling machine learning models from our own piece of Java code is a breeze with Weka! Now let us get started with the installation process.

The first step is obviously to install Weka. For this we need to download the installer using the link *https://prdownloads.sourceforge.net/weka/weka-3-9-6-azul-zulu-windows.exe*. We can install Weka using the installer as shown in Figure 1.

Proceed by clicking 'Next', agree to the terms and conditions, and the installation process will start. Now choose the location where Weka needs to be installed and click 'Next'.

Upon clicking 'Next', the installation will be completed automatically.

Now that the installation is complete, you can launch Weka from your applications and start using it. When opened, the user interface (UI) will resemble Figure 4.

The next step is to click on the 'Explorer' button as shown in Figure 5.

Now, let's proceed to download the iris data set. This data set comprises three major classes, which represent the sub-species of the iris flower: iris-setosa, iris-versicolor and iris-virginica. The data set features include the width and length of the petal and sepal. The goal is to classify a given flower into one of the three classes. To achieve this, we train our model using the four features, and the model can then be used to make the predictions if a new flower comes in.

The data set can be downloaded from *https://gist.github.com/myui/143fa9d05bd6e7db0114*. Once we download the data, it can be stored in a location accessible to Weka.

The UI of the application helps us load the data sets, use various algorithms and also perform clustering, visualisation and many more tasks. For this article, we will focus solely on training the model and testing it.

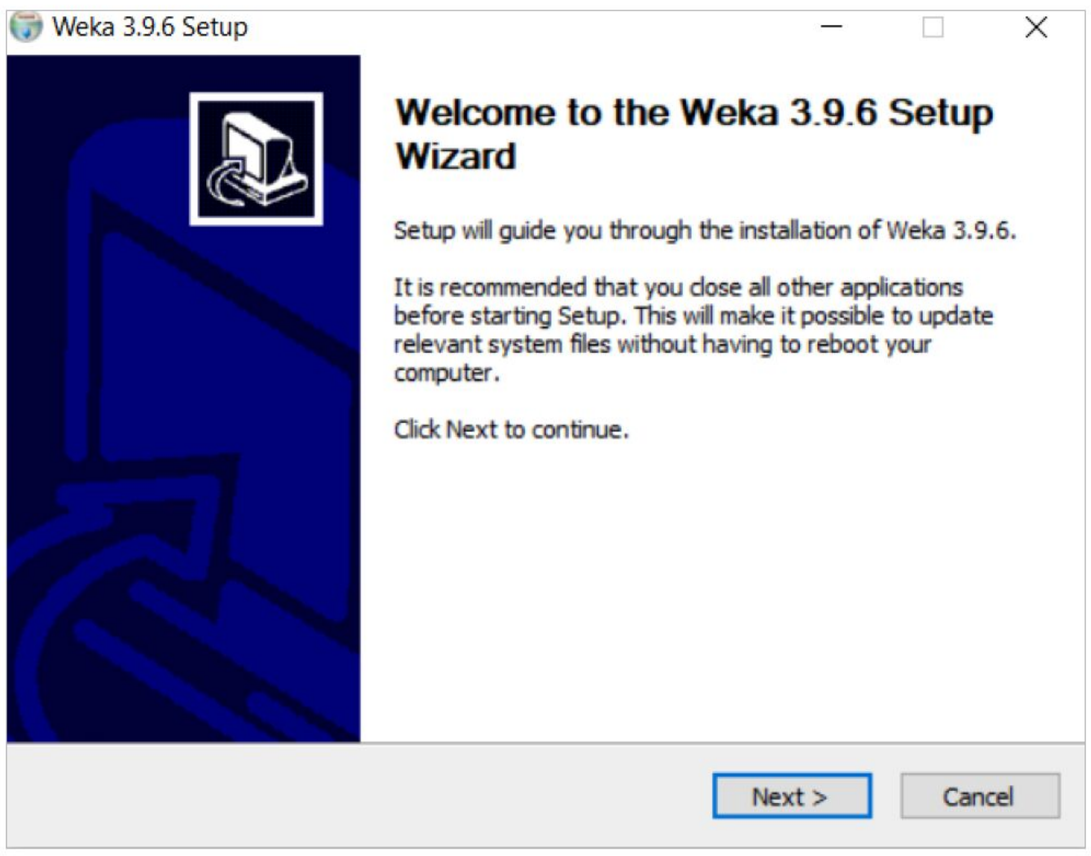


Figure 1: Opening the installer

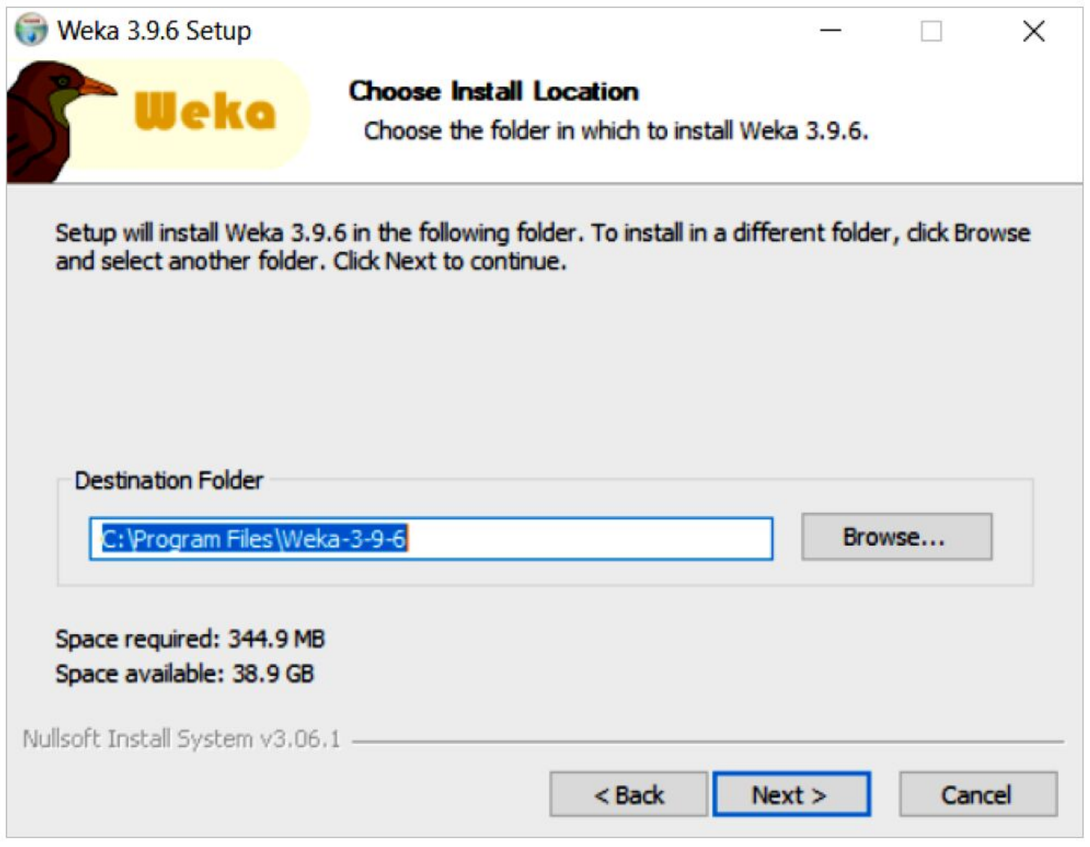


Figure 2: Choosing the location

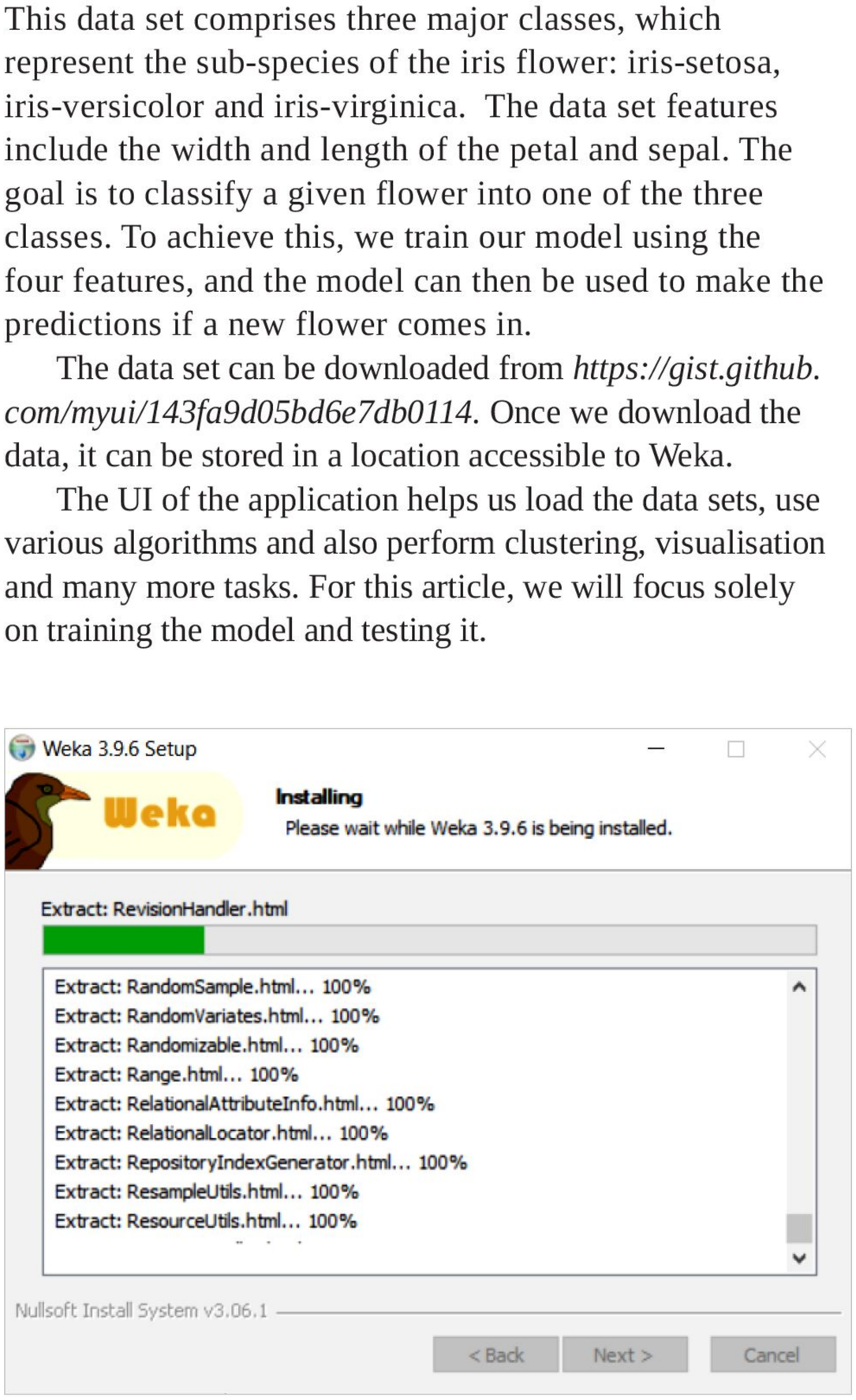


Figure 3: Installation completed



Figure 4: User interface

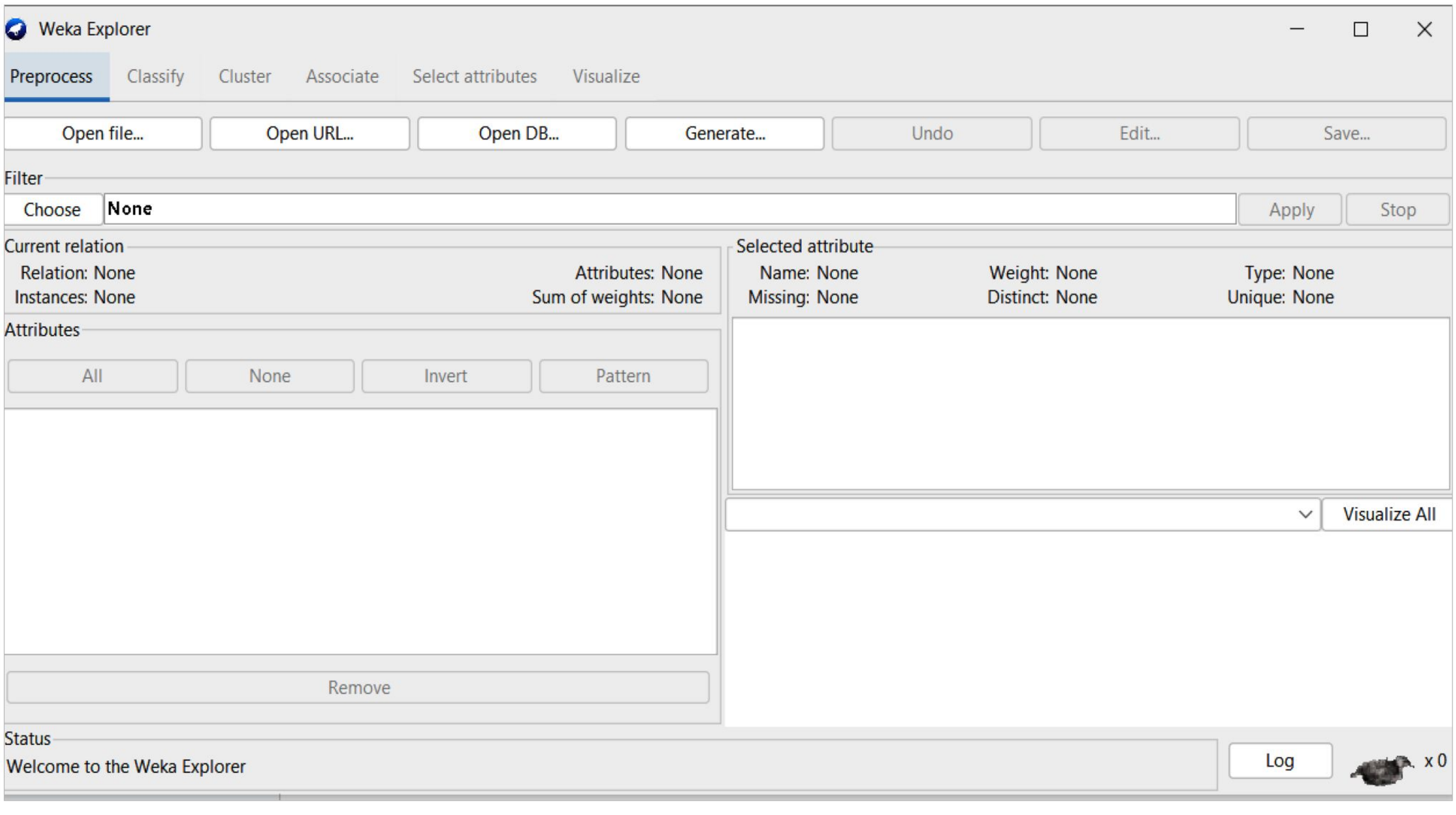


Figure 5: Explorer option on Weka

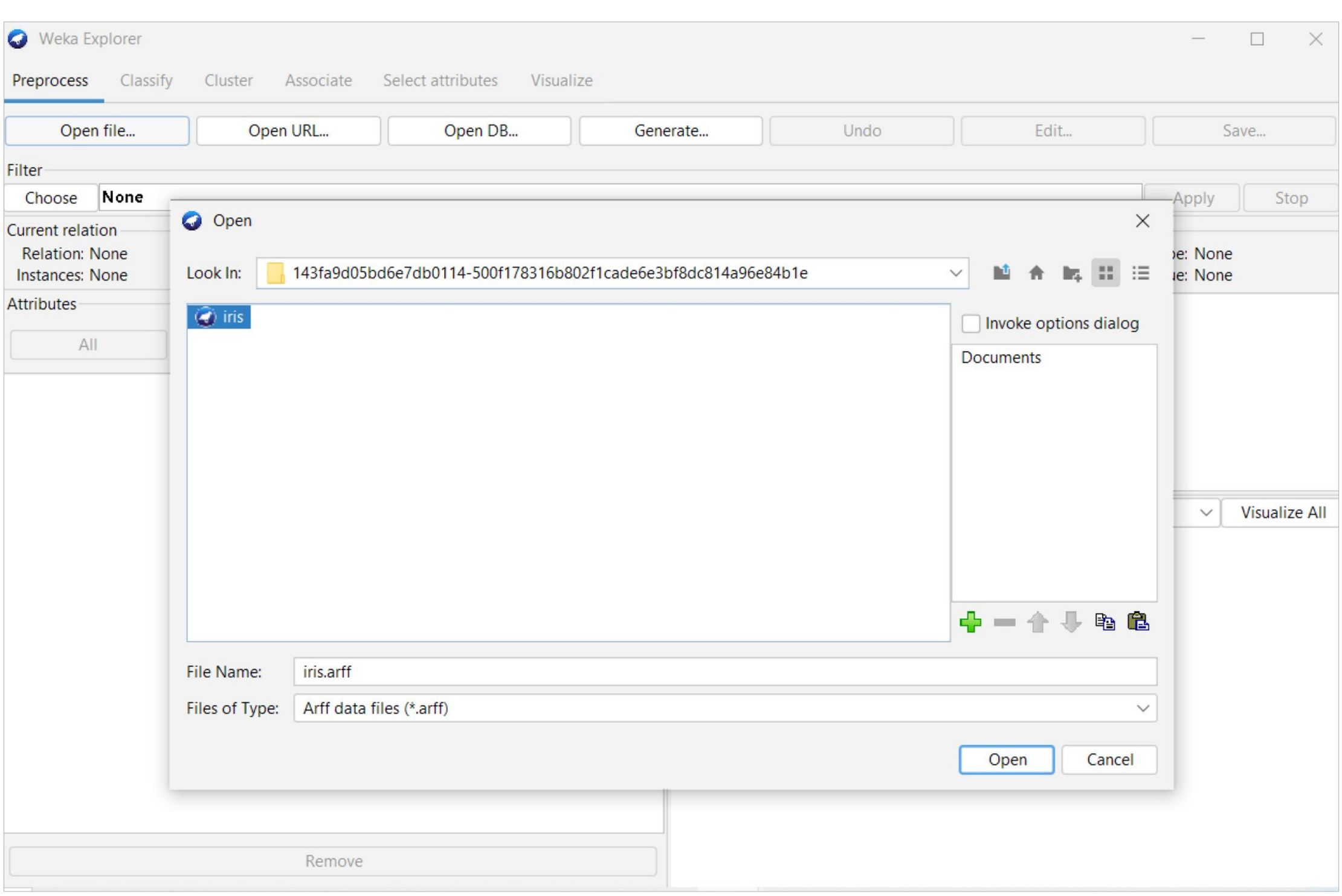


Figure 6: Loading the data set

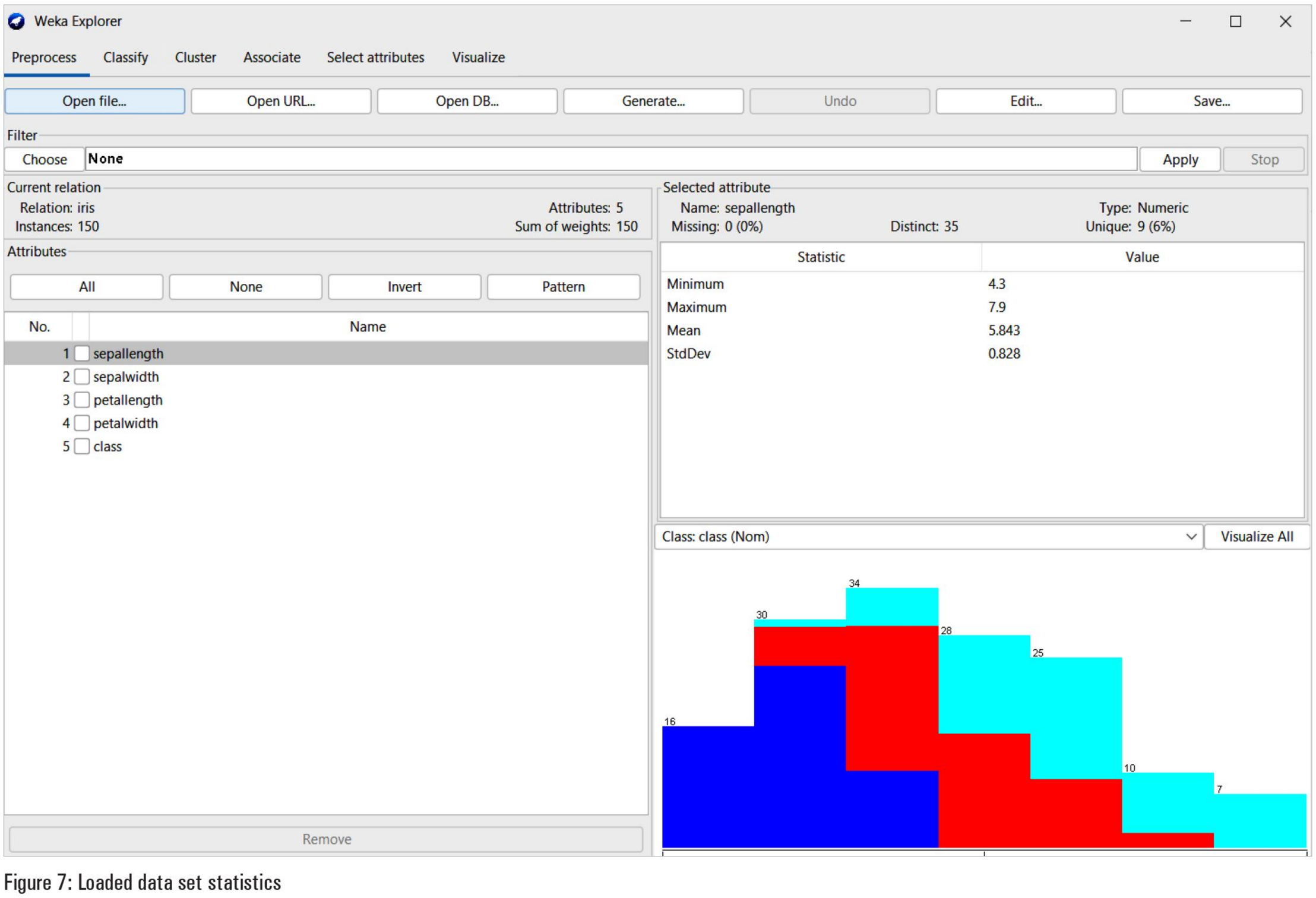


Figure 7: Loaded data set statistics

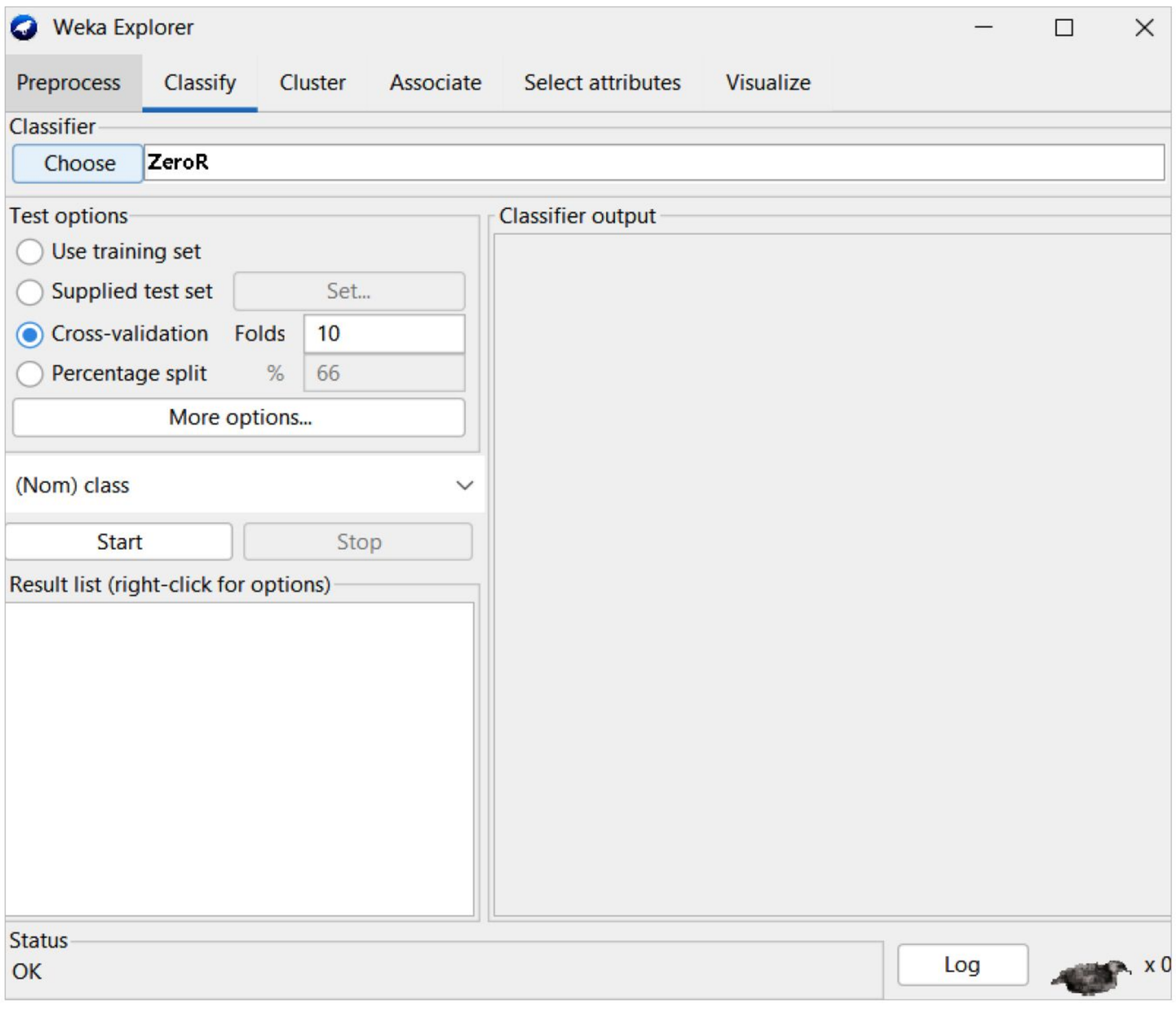


Figure 8: Choosing an algorithm

Now we can load the downloaded data set into the application. On the *Explore* page, choose the 'Open' file, go to the location of the *.arff* file and choose the file as shown in Figure 6.

Once this is done, click on 'Open' and the data set will get loaded. The tool will present a basic visualisation and statistics of the data set, such as what are the columns and the averages, etc, as shown in Figure 7.

Next, select the appropriate algorithm. For this we need to go to the tab that our task requires. Since this is a classification task, we go to the *Classify* tab. Here, by default, the ZeroR algorithm is selected. This is a rule-based algorithm. However, you can choose from several other options as shown in Figure 8.

You can see that the cross-validation option has been chosen in the test option by default with ten folds. This means that we divide the data set

into ten parts, use nine parts to train the model and use the last one part to test the model. We then repeat this process until each part gets a chance to be the test data set.

Once you have chosen the algorithm, you can click on the 'Start' button. The model starts getting trained, and we get the testing accuracies and confusion matrices. This is pretty cool as not much coding is required. Even individuals with minimal expertise can develop a machine learning model using this pretty amazing tool!

The results look as shown in Figure 9, when we use the ZeroR algorithm. As it is a rule-based algorithm you can see that the accuracies are pretty low — only 50 out of the 150 data points were predicted correctly.

So, to improve the accuracy let's switch to a better algorithm. We will be using the random forest algorithm. Click on 'ZeroR', and you will get a drop-down menu. Here, if you go into 'trees', you will find the 'random forest' option. Choose that and click on 'Start' like you did for ZeroR. You will soon get the results after the training as shown in Figure 10. As you can see, the accuracy has improved a lot, and now there are only seven wrong predictions.

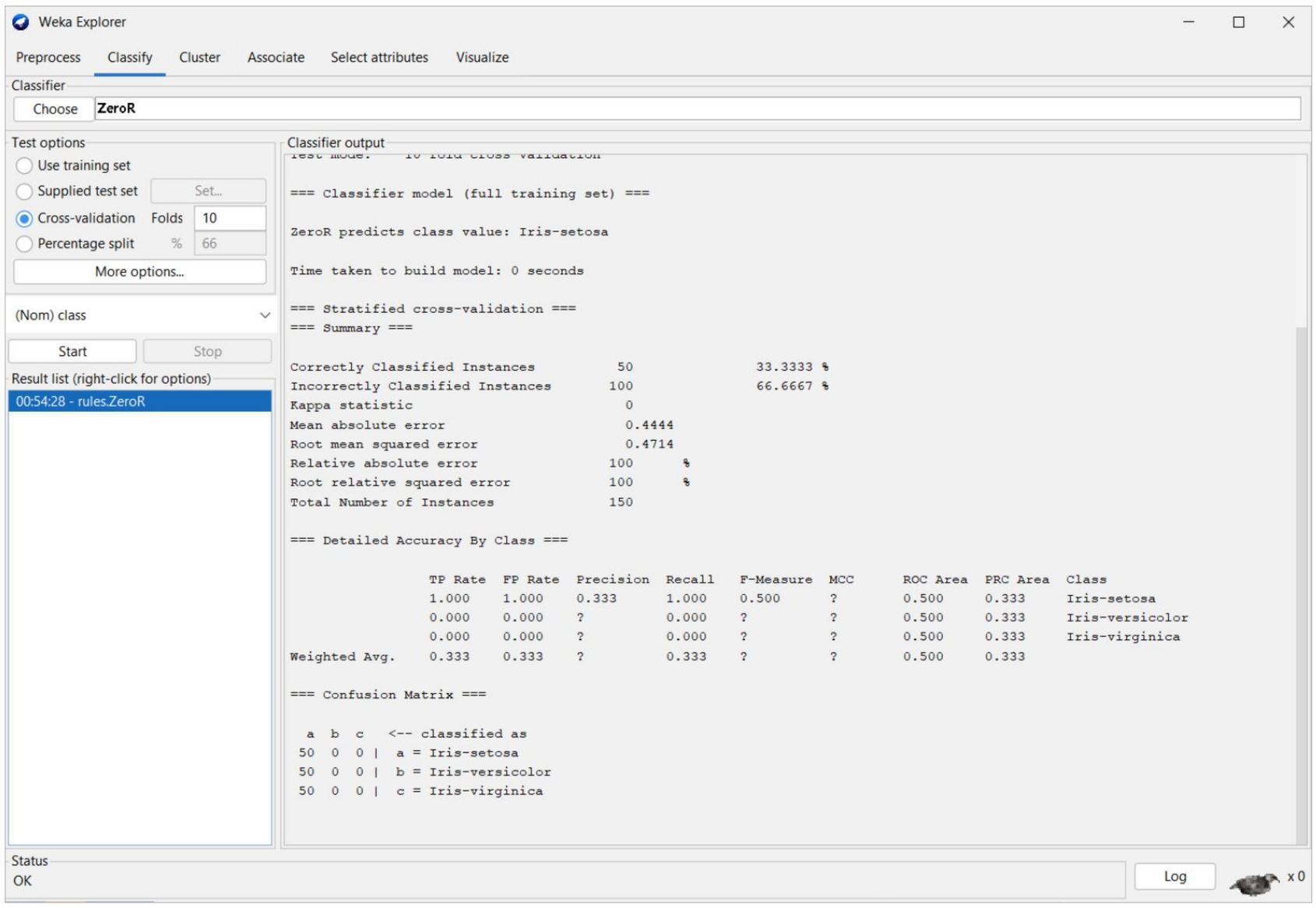


Figure 9: ZeroR results

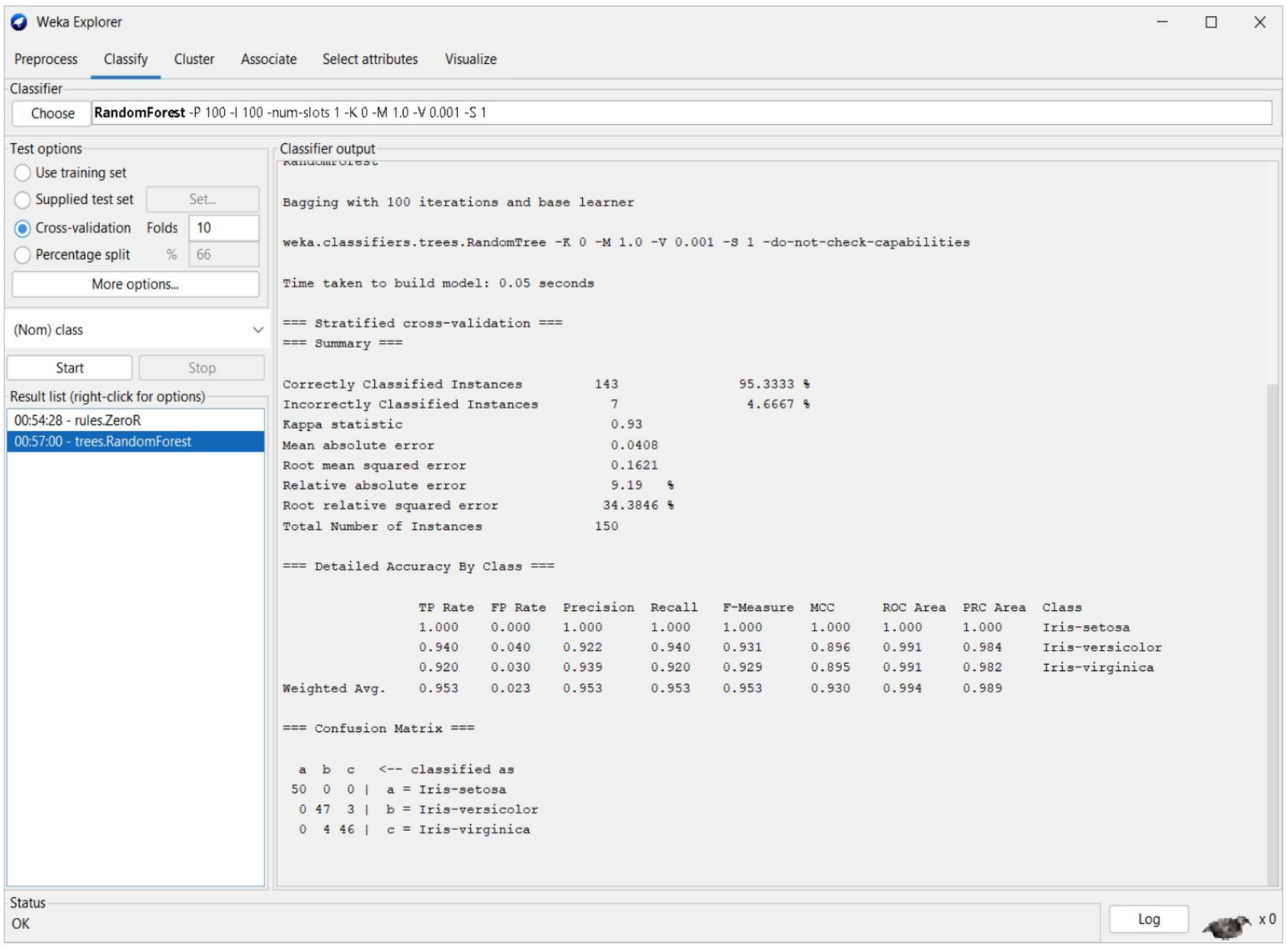


Figure 10: Random forest results

Weka can be used to explore and compare different algorithms on a given data set and more. Additionally, you can explore more of the algorithms available and look at other options, like regression, and unsupervised algorithms like clustering. END

By: Jishnu Saurav Mittapalli

The author is a full stack web developer, interested in modern technologies like artificial intelligence and machine learning. He is currently working in the field of natural language processing.

Migrating to the Cloud?
Tick Off this Checklist



Cloud migration seems attractive but is not a bed of roses. Before you embark on a journey to the cloud, analyse all the pros and cons carefully.

Cloud computing has revolutionised business operations by offering numerous benefits, such as cost savings, scalability, and flexibility. As a result, businesses are increasingly adopting cloud computing. However, migrating workloads to the cloud is a complex process that requires careful planning and execution. So let's explore the factors that businesses need to consider when undertaking cloud migration to ensure a successful transition.

Reasons for migrating workloads to the cloud

Improved stability and uptime: Cloud providers typically offer highly redundant and fault-tolerant infrastructure, ensuring uninterrupted operations even in the face of hardware or software failures. And they often provide SLAs (service level agreements) that guarantee a certain level of uptime. This becomes crucial for businesses with mission-critical workloads.

Accessibility across multiple locations: With cloud computing, businesses can access their data and applications from anywhere in the world, as long as they have an internet connection. This feature is particularly useful for distributed teams as well as businesses with customers or partners in different geographic locations.

Enhanced security: Cloud providers invest heavily in security measures and protocols, providing businesses with better data and application protection. Additionally, automatic software updates and security patches help businesses stay up-to-date with the latest threats and technologies.

Keeping up with technological advancements: Migrating workloads to the cloud enables businesses to stay current with the latest technologies. Cloud providers offer cutting-edge services such as AI and machine learning, giving businesses a competitive edge. Additionally, the cloud allows for easy experimentation with new technologies without significant upfront investments.

Assessing business requirements and constraints

Before migrating workloads to the cloud, businesses must thoroughly assess their requirements and constraints to ensure a successful transition.

For instance, in the stock brokerage industry in India, specific compliance requirements exist regarding data storage and security. Brokers must adhere to regulations set forth by the Securities and Exchange Board of India (SEBI), which dictate that customer data must be stored within the country, and encrypted at rest and in transit.

To comply with SEBI's regulations, businesses planning to migrate to the cloud need to select a provider with data centres located in India. They must also ensure that the provider has appropriate security measures in place to meet SEBI's encryption requirements.

Requirements/ Constraints	Example (Stock brokerage industry in India)
Compliance	Data storage and encryption regulations set forth by the Securities and Exchange Board of India (SEBI)
Budget	Limited budget for cloud services
Staffing	IT team with modest capabilities
Existing IT infrastructure	Legacy systems or applications that may not be compatible with cloud solutions

By using a simple table matrix like the one given above, businesses can identify their requirements and constraints, facilitating an informed decision-making process.

In addition to compliance requirements, businesses must also consider other constraints, such as budget, staffing, and existing IT infrastructure. For example, a business with limited budget may need to choose a cloud provider with more cost-effective pricing models, while a business with a small IT team may need to choose a cloud provider that offers more managed services to help with maintenance and support.

Technical factors to consider

When migrating workloads to the cloud, businesses need to evaluate their existing IT infrastructure to determine cloud readiness, choose the right deployment model and address all security concerns.

Evaluating existing IT infrastructure and determining cloud readiness: To determine cloud readiness, businesses should consider the following factors.

Application compatibility: Evaluate which applications can be moved to the cloud seamlessly and identify those requiring modifications to operate effectively in the cloud environment. AWS recommends employing migration strategies like 'Rehost' and 'Refactor' to address application compatibility concerns.

Resource utilisation: Assess the current resource usage including CPU, memory, storage, and network bandwidth, and verify that the cloud environment can accommodate the workload. The 'Rehost' strategy is well-suited for applications requiring minimal changes.

Data dependencies: Identify applications with critical data dependencies and analyse the impact of migrating them to the cloud. Depending on the specific requirements, strategies such as 'Rehost', 'Replatform', or 'Refactor' may prove useful.

Choosing the right cloud deployment model: Selecting the right cloud deployment model depends on the unique needs of the business. Today most cloud providers offer three options.

Public cloud: Public clouds are provided by third-party vendors over the internet, such as Amazon AWS, Microsoft Azure, Google Cloud, IBM Cloud, and Digital Ocean. Migrating to the public cloud is well-suited for the 'Rehost' and 'Refactor' strategies.

Private cloud: Private clouds provide cloud services exclusively to a single organisation. These can be on premises, on public cloud infrastructure or through a data centre co-location HCI setup using platforms like VMWare, Nutanix, ProxmoxVE, or OpenStack. For migrating to a private cloud, strategies like 'Replatform' and 'Refactor' may be beneficial.

Hybrid cloud: Hybrid clouds combine public and private cloud models, allowing businesses to leverage the benefits of both. For migrating to a hybrid cloud, strategies such as 'Rehost', 'Replatform', or 'Refactor' can be employed.

Addressing security and compliance concerns: Security and compliance are paramount when moving workloads to the cloud. Here are some migration strategies to address these concerns.

- *Refactor:* Modify the application architecture to take advantage of the security features offered by the cloud environment.
- *Replatform:* Use cloud-native security services and features to enhance security and compliance.
- *Rehost:* Leverage existing security and compliance controls of the application in the cloud environment.

By following the 7Rs of migration, businesses can ensure smooth and secure migration to the cloud environment that meets their specific needs. You can check the AWS Glossary on the 7Rs for ready reference at *https://docs.aws.amazon.com/prescriptive-guidance/latest/migration-retiring-applications/apg-gloss.html#gloss-mig-7rs-terms.*

Data migration

Data migration is a critical aspect of cloud migration -- it is essential to validate the accuracy and integrity of the data during migration. Proper planning and execution, including selecting the appropriate tools and technologies, are important to ensure that data is migrated efficiently and accurately.

Data preparation and secure transfer: Before initiating the transfer process, data needs to be prepared for the cloud environment. This involves organising, cleaning up, and removing duplicates or irrelevant data.

Various methods can be employed for data transfer depending on the data set size.

Table 1: The 7Rs of migration

7Rs of Migration	Description
Refactor	Refactor or re-architect the application to take advantage of cloud-native features and capabilities.
Replatform	Upgrade or replace the underlying infrastructure of the application to take advantage of cloud services, without making significant changes to the application itself.
Repurchase	Move to a different software product or service, such as a SaaS offering like Office365, Google WorkPlace, ZohoOne, instead of migrating the application itself.
Rehost	Also known as "lift and shift," migrate the application to the cloud with minimal changes to the application architecture, and use cloud infrastructure as a like-for-like replacement of on-premises infrastructure.
Relocate	Move the application to a different location or region, without making significant changes to the application itself.
Retain	Maintain the application on-premises or in a hosted environment, and do not migrate it to the cloud.
Retire	Decommission the application, either because it is no longer needed or because it will be replaced with a different application.

- *Online data transfer:* This method involves transferring data over the internet using a secure connection. It is typically the most convenient and cost-effective method for small to medium-sized data sets.
- *Offline data transfer:* For large data sets, offline data transfer may be more practical. This method involves physically transferring data to the cloud provider, typically using a secure storage device.
- *Hybrid data transfer:* In some cases, a combination of online and offline data transfer methods may be required to ensure efficient and secure data transfer. For example, a hybrid approach can be used for large healthcare organisations transferring patient data to the cloud while maintaining system uptime.

Validation of data accuracy and integrity: Validating the accuracy and integrity of transferred data is crucial to ensure a successful migration. Different methods can be employed for this. Thorough validation helps identify discrepancies or errors, and ensures the integrity of the data in the cloud environment.

Manual validation: This method involves manually comparing the data in the cloud environment with the original data source. It can be time-consuming, but is typically the most accurate method.

Automated validation: Automated tools can be used to compare the data in the cloud environment with the original data source. This method is typically faster than manual validation, but it may not be as accurate.

Sampling validation: In some cases, it may be impractical to validate all the data in the cloud environment. In these cases, a sampling of the data can be validated to ensure that it is accurate and consistent with the original data source.

Integration and interoperability

Integrating cloud services with on-premises applications and systems is critical to ensuring seamless operation. Proper integration can help businesses maximise the benefits of cloud migration and minimise disruption to operations.

Integrating cloud services with on-premises applications and systems: This is a critical step in the migrating process. It enables seamless access and use of data and applications between the cloud and on-premises environments. Organisations must identify the suitable integration patterns and protocols that align with their existing infrastructure. Examples include point-to-point integration, middleware-based integration, and API-based integration. Each pattern has its own benefits and drawbacks, and organisations need to choose the one that best fits their requirements. A hybrid integration platform can provide a unified solution. It typically includes a set of pre-built connectors, adapters, and APIs facilitating smooth integration between cloud services and on-premises systems.

Ensuring interoperability with third-party solutions: In addition to integrating on-premises systems, businesses must ensure interoperability with third-party solutions. These solutions can include software applications, platforms, and services that are not part of the organisation's IT infrastructure. Compatibility with third-party solutions is essential to leverage the benefits of the cloud and these external offerings.

Evaluation of integration patterns and protocols that are compatible with the third-party solutions. such as point-to-point integration, middleware-based integration, and API-based integration, is necessary. Organisations need to choose the pattern that best fits their requirements.

Utilising an API management platform can provide a unified solution for seamless integration between cloud services and third-party solutions. Such a platform typically includes a set of pre-built connectors, adapters, and APIs.

Let's take the example of a company that uses biometric devices to track employee attendance. The biometric devices are connected to the company's on-premises system, which is responsible for collecting and storing the data. When migrating to the cloud, the company must ensure that the biometric devices can seamlessly integrate with the cloud-based attendance tracking system. This requires a thorough evaluation of the existing system to identify any potential issues or challenges that may arise during the migration process.

One approach is to use a middleware layer to act as a bridge between the on-premises system and the cloud-based system. The middleware can convert data formats and protocols, enabling communication between the two systems.

To ensure interoperability with third-party solutions, the company must consider the compatibility of the biometric devices with the cloud-based attendance tracking system and any third-party solutions that are being used, such as payroll or HR management software. This requires a comprehensive evaluation of the API compatibility and data exchange formats.

The company may also need to consider additional factors such as device firmware updates, compatibility with cloud-based biometric authentication services, and security considerations when transmitting sensitive employee data from on-premises to cloud-based systems.

Table 2: Ensuring interoperability with third-party solutions

Considerations	Description
Identify third-party solutions	Determine which third-party solutions will be used in conjunction with cloud services.
Evaluate compatibility	Check if the third-party solutions are compatible with the cloud provider and the cloud services being used.
Verify API availability	Verify that the third-party solutions have APIs that are available for integration with the cloud services.
Test integration	Test the integration of the third-party solutions with the cloud services to ensure they are working as expected.
Ensure data security	Ensure that the third-party solutions comply with the necessary security and compliance regulations.
Monitor performance	Monitor the performance of the third-party solutions and the cloud services to ensure that they are working seamlessly together.

Cost considerations

The total cost of ownership of cloud solutions includes infrastructure costs, licensing fees, and maintenance expenses. Proper cost analysis and planning are crucial to ensure cost-effective cloud solutions.

Analysing the total cost of ownership of cloud solutions: Considering the total cost of ownership (TCO) is crucial when evaluating cloud solutions. TCO encompasses upfront migration costs, ongoing subscription fees, support costs, and expenses associated with scaling the solution.

By carefully analysing TCO, businesses can make informed solutions to adopt and effectively manage ongoing cloud costs.

Understanding the pricing models and payment options of cloud providers: Cloud providers offer various pricing models and payment options to suit different business needs. Familiarising yourself with these models, such as pay-as-you-go, reserved instances, spot instances, and available discounts, allows businesses to select options aligned with their requirements and budget.

Network connectivity

Adequate network bandwidth and connectivity are critical to the success of cloud services. Proper network testing and monitoring are important to ensure that network connectivity meets business requirements.

Ensuring adequate network bandwidth and connectivity for cloud services: Before migrating, it is crucial to understand the network requirements of your workloads and applications. Assess your organisation's existing network infrastructure to ensure compatibility with cloud-based services. Evaluate the bandwidth requirements of your cloud-based applications and services to ensure that they can function effectively. Take into account the location of your end users and how they will access the cloud-based services. Ensure there is sufficient network connectivity between them and the cloud provider to maintain optimal performance.

Let's consider the stock broking industry as an example. Stock brokers heavily rely on network connectivity for timely access to market data, news, and other critical information. To ensure adequate network bandwidth and connectivity for cloud services, stock brokers can utilise a dedicated network connection between their on-premises infrastructure and the cloud provider's network. For instance, they can use Direct Connect to establish a reliable and cost-effective network connection.

Evaluating the performance and availability of cloud providers' networks: Evaluate the network performance of different cloud providers. Factors such as latency, packet loss, and jitter should be considered to ensure

optimal performance for your application and services. Evaluate the availability and reliability of the cloud providers' network infrastructure. Consider factors such as data centre redundancy, network architecture, and the geographical location of the data centres.

Check for potential network security risks or vulnerabilities. Ensure that the cloud provider has robust security measures in place to protect your data and network.

Continuing with the stock broking industry example, stock brokers require high levels of network performance and availability to support their trading operations. They can evaluate the performance and availability of cloud providers' networks by monitoring service level agreements (SLAs) and conducting regular network testing. For example, they can use SaaS based monitoring solutions to measure network latency and packet loss, and Amazon Route 53 DNS services for high availability and reliability of their applications running on the cloud infrastructure.

Business continuity and disaster recovery

Business continuity and disaster recovery planning are essential to ensure uninterrupted operations in the event of a disruption.

Implementing a robust business continuity and disaster recovery plan for cloud services: Implementing comprehensive business continuity planning (BCP) and a disaster recovery (DR) plan is crucial when migrating critical workloads to the cloud. Cloud service providers offer several disaster recovery options, but it is important to evaluate them and choose the one that best suits the organisation's needs. The BCP/DR plan should be tested periodically to ensure that it is effective and up-to-date.

As an example, in the event of a disaster, stock brokerage firms should have a BCP/DR plan in place to ensure the availability of their trading platforms and customer data. This may involve data replication, automatic failover to secondary data centres, or using third-party disaster recovery services. Multi-specialty hospitals relying on cloud services for critical applications like electronic health records (EHRs) need a comprehensive BCP/DR plan. This ensures availability of applications even in the face of natural disasters or cyber-attacks.

Ensuring compliance with service level agreements (SLAs): When selecting a cloud service provider, organisations must review and understand the service level agreements (SLAs) offered. SLAs define the terms and conditions of the service, including performance, uptime guarantees, and remedies in case of service interruptions. Organisations should ensure that the SLAs offered by the provider meet their business requirements and provide adequate protection in the event of service disruptions.

For example, in the stock brokerage industry, it is important to ensure that the trading platform and customer data are always available. The SLA with the cloud service provider must guarantee high uptime and performance for trading platforms and customer data. The SLA should also include provisions for compensation in case of service disruptions affecting business operations.

Key takeaways

Here are the key takeaways to remember when considering cloud migration.

- Cloud offers benefits such as cost savings, scalability, and access to cutting-edge technologies.
- Before migrating, assess business requirements, evaluate existing IT infrastructure, choose the right deployment model, and address security and compliance concerns.
- Adequate network bandwidth, connectivity, a comprehensive BCP/DR plan, analysing TCO, and understanding pricing models are crucial for successful cloud implementation.

Future directions and trends

The future of cloud computing presents exciting opportunities for organisations. Consider the following trends:

- The cloud computing market is expected to continue growing, with increased adoption of multi-cloud and hybrid cloud environments.
- Artificial intelligence and machine learning will play a larger role in cloud computing, with providers offering AI-driven services and solutions.
- Edge computing and edge data centres are gaining popularity as organisations seek to process data closer to the source, improving latency and performance.
- Security and compliance will remain top concerns, driving automation and proactive measures to mitigate risks.

Overall, the future of cloud computing looks promising, offering organisations opportunities to improve efficiency, reduce costs, and leverage innovative technologies. However, it is essential to evaluate each organisation's unique needs before embarking on a cloud migration journey. END

By: Deepen Dhulla

The author has over 21 years of experience in the Linux and open source realm. He specialises in assisting clients in setting up private clouds using HCI based on ProxmoxVE and Ceph SDS.

Do I/O Schedulers Perform Better in Virtual Machines or in Docker Containers?

The I/O schedulers in Linux manage the order in which the I/O requests of processes are handled by the disk subsystem. This article compares the performance of different I/O schedulers in Linux virtual machines and Docker containers, offering insights into optimising disk access for improved system performance.



Process schedulers are essential to the functionality and responsiveness of Linux systems and are well-known to the majority of users. Their primary role is to manage the distribution of system resources among processes, including the CPU, memory, and I/O hardware. The process scheduler's objective is to maximise system throughput, reduce response time, and ensure fairness among all active processes.

In addition to process schedulers, Linux also has I/O schedulers that manage the order in which processes' I/O requests are handled by the disk subsystem. The I/O scheduler performs a similar role to the process scheduler, but instead manages the processes' disk access rather than the CPU. In situations where multiple I/O requests from different processes compete for disk access, the I/O scheduler is crucial to the system's overall performance.

Despite the use of flash and solid-state storage, disk access remains the most expensive form of data access, being slower than data access from RAM. I/O schedulers optimise disk access requests to improve performance.

This article compares the efficiency of different I/O schedulers when SSDs are used, and the results are particularly relevant for processes that involve intensive disk access. The comparison is made between running benchmarks on Ubuntu 20.04 and using Docker and containers (where files must first be copied into the container to run the benchmarks).

"Prior to Ubuntu 19.04 with Linux 5.0 or Ubuntu 18.04.3 with Linux 4.15, the multiqueue I/O scheduling was not enabled by default and just the deadline, cfq and noop I/O schedulers were available by default. For Ubuntu 19.10 with Linux 5.0 or Ubuntu 18.04.3 with Linux 5.0 onwards, multiqueue is enabled by default providing the bfq, kyber, mq-deadline and none I/O schedulers. For Ubuntu 19.10 with Linux 5.3 the deadline, cfq and noop I/O schedulers are deprecated." *(Ubuntu Wiki, 2019)*

The above statement can be taken as true for Ubuntu 20.04 too. Hence, for the comparison only the following I/O schedulers were taken into account:

- none I/O scheduler
- mq-deadline I/O scheduler
- bfq I/O scheduler
- kyber I/O scheduler

I/O scheduler commands

To check the available I/O schedulers, run the following command:

```
$ cat /sys/block/sda/queue/scheduler
```

The output would be something like:

```
[mq-deadline] none
```

This means that the currently selected I/O scheduler is *mq-deadline*, and other options are available in the I/O scheduler, for example, *none*.

(Ubuntu Wiki, 2019). Usually, *mq-deadline* and *none* are available by default. If the other I/O schedulers are missing you could use the following commands:

```
$ sudo modprobe bfq
$ sudo modprobe kyber-iosched
```

Now run the following command to check the available I/O schedulers:

```
$ cat /sys/block/sda/queue/scheduler
```

The output would be something like:

```
[mq-deadline] none bfq kyber
```

Let's now move on to the benchmarks.

Test 1: writes-starving-reads

This test evaluates the performance of the I/O schedulers when there is a write operation going on in the background and how efficiently the read operations can be completed without starvation. Benchmark Test 1 is designed in a way to get results for better comparison.

You can perform the write operation in the background, using the following command:

```
$ while true; do dd if=/dev/zero of=file
bs=1M; done &
```

This command runs a write operation in the background due to the '&' symbol used at the end of the command. The above command is an infinite *while* loop.

After the testing on benchmarks is done, remember to kill this process using its process ID.

The code for changing to the *none* scheduler and then running Benchmark Test 1 is given below.

Step 1: Perform the write operation in the background.

Step 2: Find out how long does it

Table 1: *none* I/O scheduler results

File size	Real-time in Ubuntu 20.04 (in seconds)	Real-time in Docker and container (in seconds)	Percentage improvement
10MB	0.003	0.002	33.33
20MB	0.005	0.003	40.00
30MB	0.006	0.005	16.67
40MB	0.008	0.006	25.00
50MB	0.009	0.007	22.22
60MB	0.01	0.008	20.00
70MB	0.012	0.01	16.67
80MB	0.013	0.011	15.38
90MB	0.015	0.012	20.00
100MB	0.017	0.013	23.53

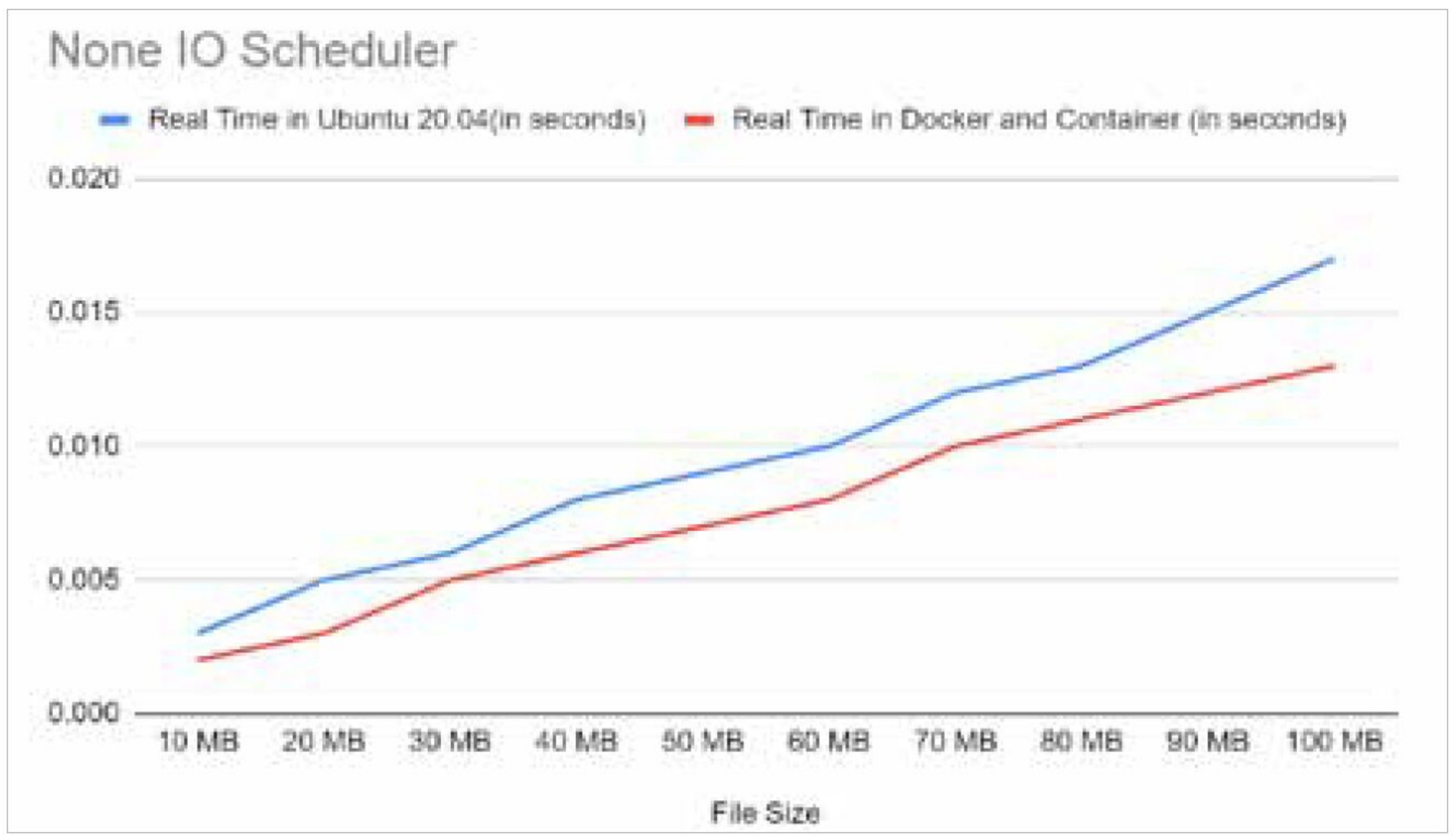


Figure 1: Graphical performance comparison of *none* I/O schedulers in VM vs Docker container

Table 2: *mq-deadline* I/O scheduler results

File size	Real-time in Ubuntu 20.04 (in seconds)	Real-time in Docker and container (in seconds)	Percentage improvement
10MB	0.012	0.002	83.33
20MB	0.018	0.003	83.33
30MB	0.024	0.004	83.33
40MB	0.036	0.005	86.11
50MB	0.046	0.007	84.78
60MB	0.051	0.008	84.31
70MB	0.059	0.01	83.05
80MB	0.062	0.012	80.65
90MB	0.072	0.013	81.94
100MB	0.076	0.013	82.89

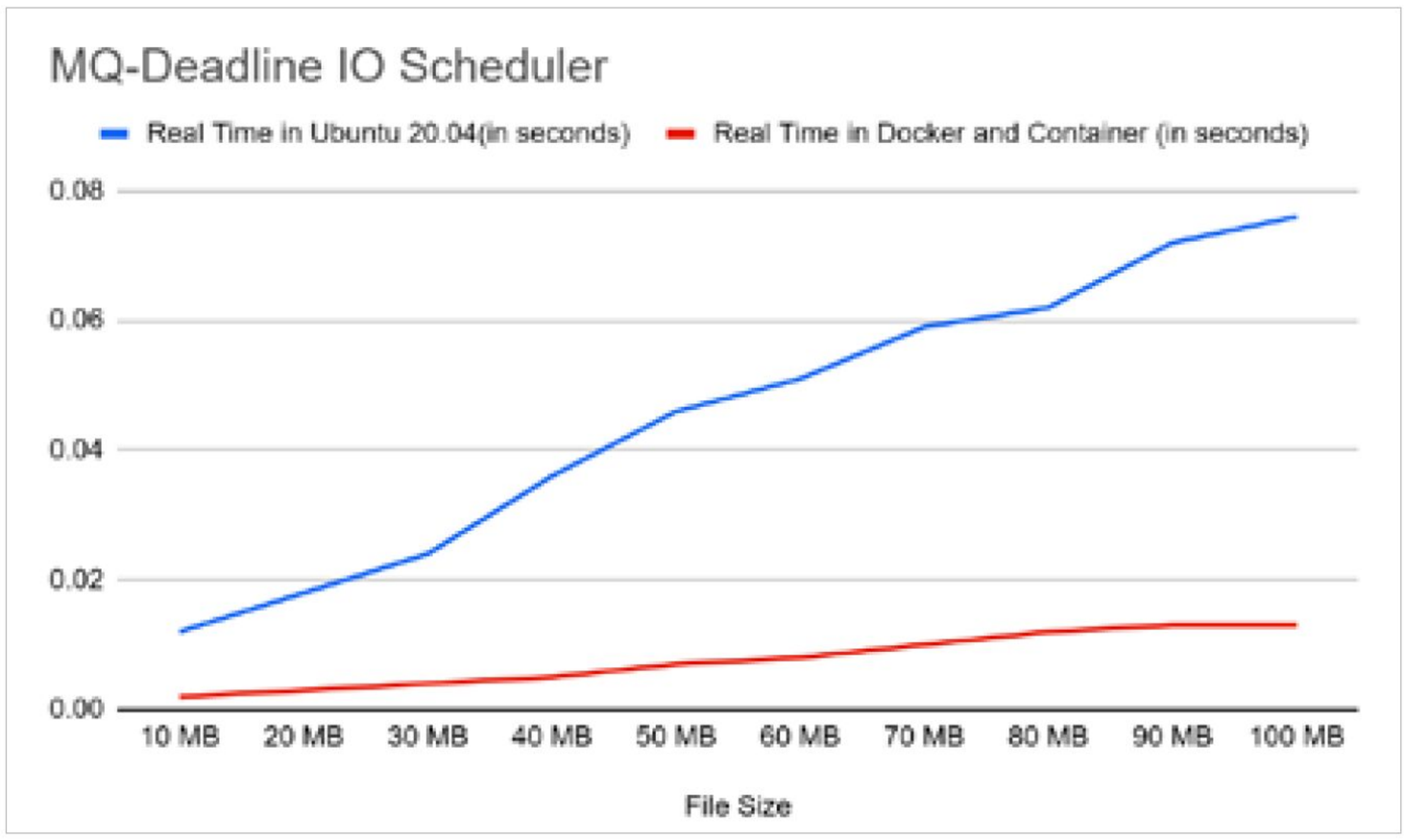


Figure 2: Graphical performance comparison of *mq-deadline* I/O schedulers in VM vs Docker container

take to read a file of various sizes.

```
echo none
while true; do dd if=/dev/zero of=file
bs=1M; done &
echo none > /sys/block/sda/queue/
scheduler
time cat 10MB.txt > /dev/null
time cat 20MB.txt > /dev/null
time cat 30MB.txt > /dev/null
time cat 40MB.txt > /dev/null
time cat 50MB.txt > /dev/null
time cat 60MB.txt > /dev/null
time cat 70MB.txt > /dev/null
time cat 80MB.txt > /dev/null
time cat 90MB.txt > /dev/null
time cat 100MB.txt > /dev/null
```

Table 3: *bfq* I/O scheduler results

File size	Real-time in Ubuntu 20.04 (in seconds)	Real-time in Docker and container (in seconds)	Percentage improvement
10MB	0.012	0.002	83.33
20MB	0.017	0.003	82.35
30MB	0.023	0.004	82.61
40MB	0.038	0.005	86.84
50MB	0.038	0.007	81.58
60MB	0.052	0.008	84.62
70MB	0.058	0.01	82.76
80MB	0.092	0.012	86.96
90MB	0.122	0.013	89.34
100MB	0.128	0.014	89.06

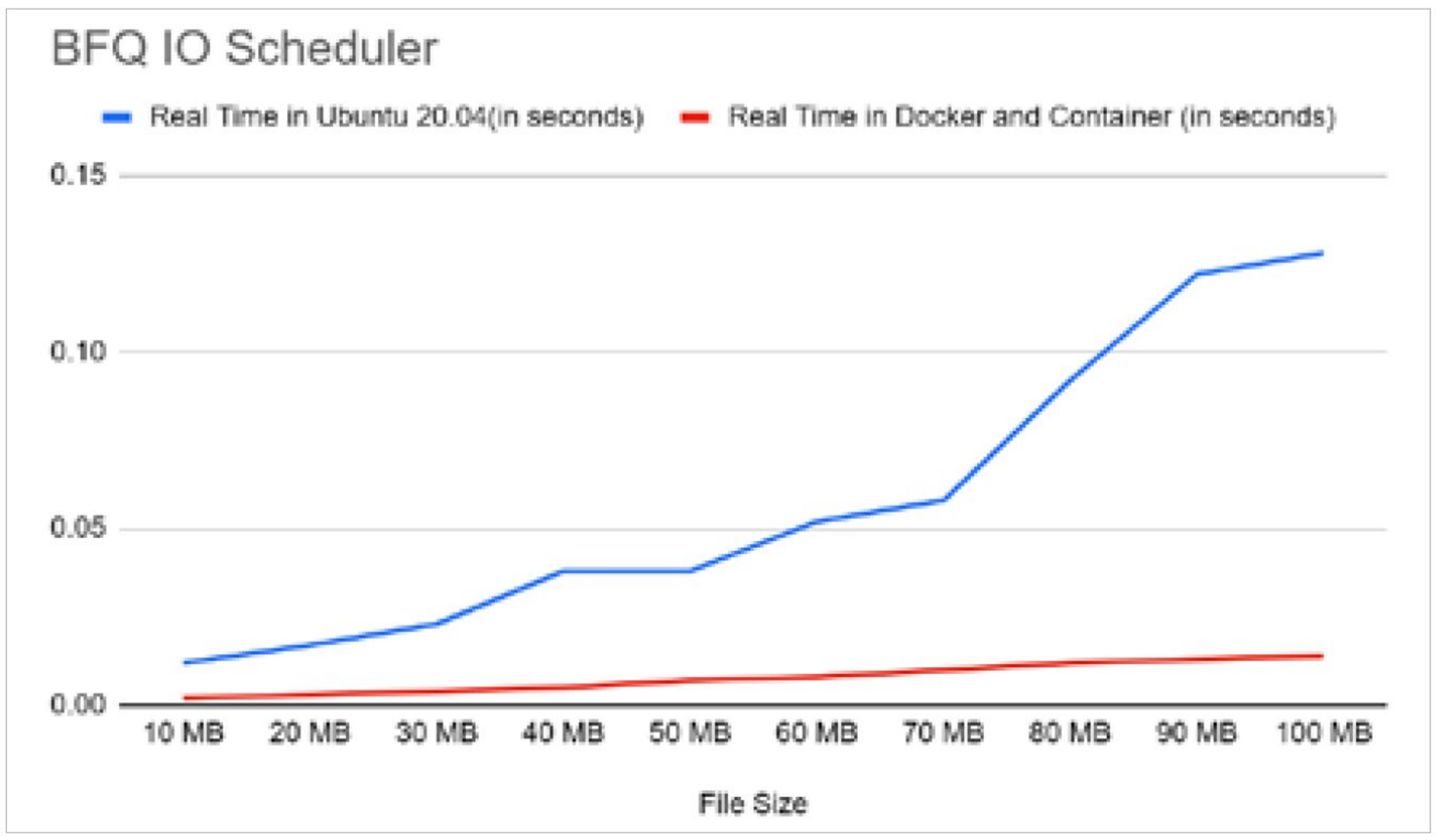


Figure 3: Graphical performance comparison of *bfq* I/O schedulers in VM vs Docker container

We executed the read and write operations test cases in a virtual machine and Docker container, and the results are tabulated in Tables 1 to 4 for various schedulers.

Figure 1 shows the performance comparison of *none* I/O schedulers in a virtual machine versus a Docker container.

Figure 2 shows the performance comparison of *mq-deadline* I/O schedulers in a virtual machine versus a Docker container.

Figure 3 shows the performance comparison of *bfq* I/O schedulers in a virtual machine versus a Docker container.

Figure 4 compares the performance of *kyber* I/O schedulers in VM vs Docker container.

Test 2: Effects of high read latency

This benchmark checks how well the I/O scheduler works when reading several small files while also reading a large file.

The code for changing to *none* scheduler and then running the Benchmark Test 2 is given below.

Step 1: Perform the read operation in the background.

Step 2: Record the time taken to read every file in the Android SDK.

```
$ while true; do cat BigFile.txt > /
dev/null;done &

$ echo
$ echo none
$ echo none > /sys/block/sda/queue/
scheduler

$ time find ../../../Android/Sdk/. -type
f -exec cat '{}' ';' > /dev/null # path
to Android Sdk
```

The test results obtained for various I/O schedulers are given in Table 5.

The performance evaluation of different I/O schedulers (*none*, *kyber*, *bfq*, and *mq-deadline*) was conducted, and the results showed that the *none* I/O scheduler outperformed the others in both Test 1 and Test 2. Interestingly, all the I/O schedulers performed better when used inside a container. However, the *none* I/O scheduler proved to be the most suitable choice for the given test conditions, as it provided the best results for both tests.

These findings are particularly relevant for processes that involve intensive disk access. In such cases, reading from a Docker container is faster and can significantly improve performance. For instance, if there are numerous reading and writing operations, such as reading a *.csv* file for data analytics and storing the results in a file, the *none* I/O scheduler can be particularly useful in enhancing performance. END

Table 4: *kyber* I/O scheduler results

File size	Real-time in Ubuntu 20.04 (in seconds)	Real-time in Docker and container (in seconds)	Percentage improvement
10MB	0.013	0.002	84.62
20MB	0.018	0.004	77.78
30MB	0.093	0.004	95.70
40MB	0.073	0.006	91.78
50MB	0.074	0.006	91.89
60MB	0.144	0.009	93.75
70MB	0.111	0.01	90.99
80MB	0.072	0.014	80.56
90MB	0.259	0.014	94.59
100MB	0.162	0.016	90.12

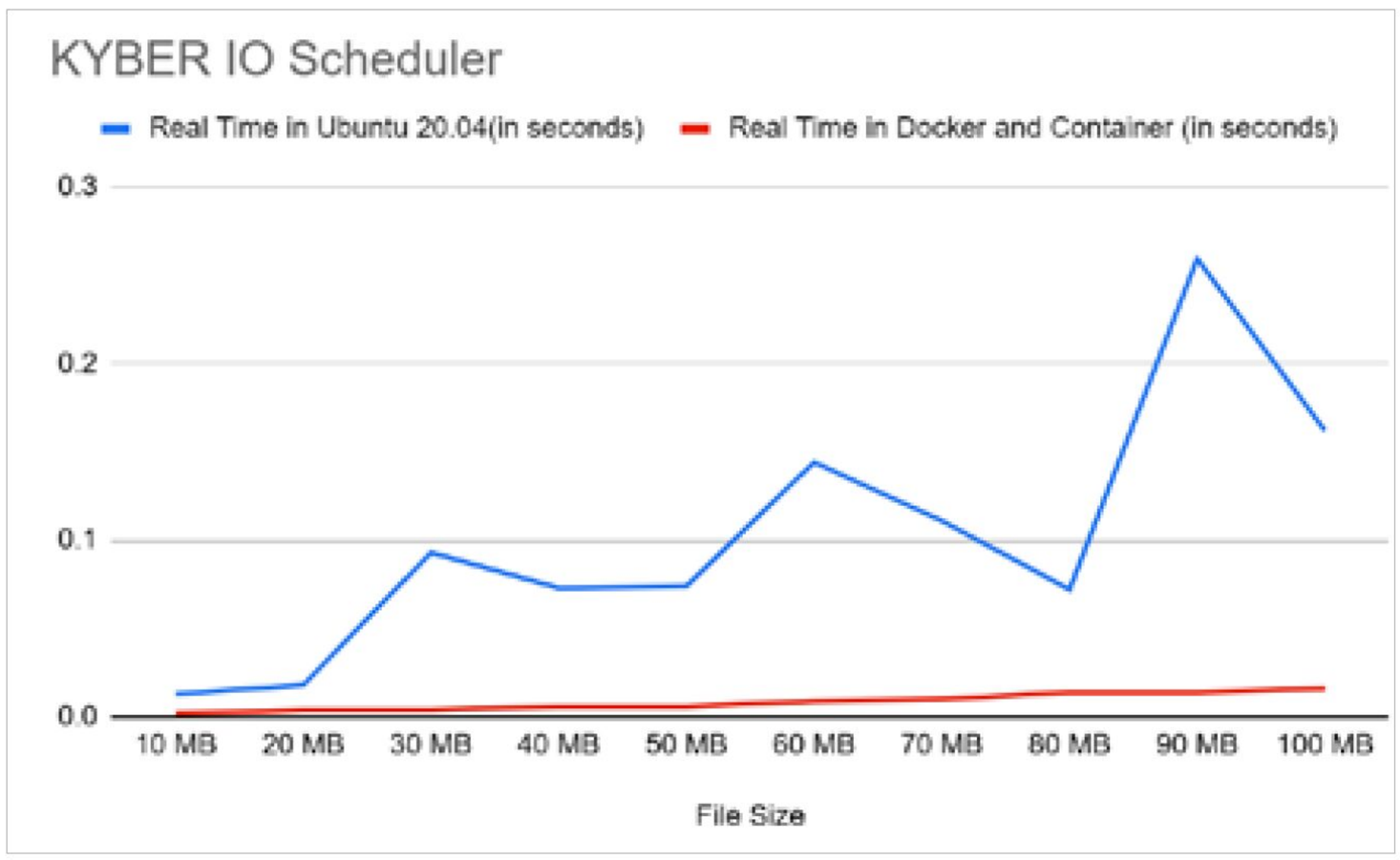


Figure 4: Graphical performance comparison of *kyber* I/O schedulers in VM vs Docker container

Table 5: Test results obtained for various I/O schedulers

I/O scheduler	VM (in seconds)	Container (in seconds)	Percentage improvement
none	94.133	79.805	17.9537623
mq-deadline	99.765	82.228	21.32728511
kyber	100.315	86.747	15.64088672
bfq	114.214	92.577	23.37189583

References

- Love, R. (2004, February 1). Kernel Korner - I/O Schedulers. Linux Journal. Retrieved January 14, 2023, from *https://www.linuxjournal.com/article/6931*
- Ubuntu Wiki (2019, September 10). Kernel/Reference/IOSchedulers. Ubuntu Wiki. Retrieved January 14, 2023, from *https://wiki.ubuntu.com/Kernel/Reference/IOSchedulers*

By: Archit Sangal and Dr B. Thangaraju

The authors are associated with the Open Source Technology Lab at the international Institute of Information Technology, Bengaluru.

Why Security and Cost go Hand-in-Hand in the Enterprise Cloud

Applying security principles to address cloud cost challenges is the need of the hour. This first part in the series on security and cost optimisation in the enterprise cloud explains that these are not isolated concerns but are truly interconnected in a well-managed cloud environment.



As an enterprise cloud security architect and cloud cost consultant, I have had the opportunity to explore the intersection of cloud security and cost optimisation. Initially, I approached these areas separately, but I soon realised the synergies between them. In this article, I will explore the challenges of complex cloud cost optimisation and the benefits of adopting a combined approach. This approach proves effective, especially in scenarios where no single solution exists and there are limitations in control and visibility.

Enterprises have prioritised cloud migration in the past decade. However, they have often underestimated the challenges that arise when it comes to effectively managing security and cost post-transition. The distributed and dynamic nature of the cloud presents unique and unforeseen hurdles for enterprises in their pursuit of implementing robust security controls and optimised cost management.

To better comprehend an enterprise cloud environment, enterprises commonly utilise one or more cloud service providers, manage multiple cloud accounts, and leverage multiple regions, availability zones, and hybrid on-premises extensions to provision their infrastructure. Within this intricate environment, multiple teams, applications, and users with varying skillsets and business objectives interact with the cloud, utilising different methods. Additionally,

the dynamic nature of cloud environments enables changes to be made by anyone, from anywhere, through various means of interaction with the cloud.

In this landscape, dynamic provisioning is performed by individuals with varying levels of understanding. Hence, any misconfigurations or misprovisioning are easily exposed to the cloud provider, potentially leading to cost leakage and security risks when exposed to the internet. This amplifies the security and cost challenges compared to traditional on-premises setups. Regrettably, many enterprises face increased expenses or compromised security postures in the cloud compared to on-premises environments due to these reasons.

The challenges

Let's explore why cloud security and cost optimisation are closely intertwined challenges.

Design flaws

Both security and cost optimisation are fundamental aspects that should be deeply rooted in the design, architecture, development practices, and implementation of the cloud environment. When the architecture is not optimised for cost efficiency and security, it can result in unnecessary resource utilisation, inefficient workflows, misconfigurations or overprovisioning of cloud resources. Enterprises often treat security and cost as afterthoughts.

Complexity and obscurity

The dynamic nature of the cloud, with its vast array of services, configurations, and data, can create a lack of visibility and understanding. The obscurity inherent in the cloud environment can contribute to misconfigurations that can expose sensitive data or lead to unauthorised access.

Inefficient resource allocation is another consequence of the lack of understanding and visibility. Without clear insights into resource utilisation and performance, enterprises may inadvertently provision resources with higher capacity than necessary, leading to cost leakage.

Limited control

Enterprises often rely on distributed teams to handle security implementation and cost optimisation. However, limited control over these decentralised teams can hamper the effectiveness of security monitoring and cost optimisation efforts.

In an enterprise cloud landscape, ensuring coordination across teams, implementing unified controls and enforcing best practices becomes difficult, leading to inconsistencies in security practices and cost optimisation strategies.

Varying business objectives

Enterprises and business units often have diverse business objectives when it comes to cloud usage. Some prioritise agility, while others prioritise cost optimisation or compliance. However, aligning these divergent priorities and goals can be challenging, resulting in fragmented security practices and inefficient cost management.

This misalignment can occur due to the varying needs, priorities, and perspectives of different stakeholders within the enterprise. This can lead to a lack of cohesive strategy, inconsistent implementation of security measures, and suboptimal cost management approaches.

Reactive approach

Enterprises often prioritise security and cost only when situations escalate beyond their control, such as a security breach or cost bleed. Addressing security and cost considerations reactively when situations escalate beyond control can be extremely expensive.

Potholes

Enterprises often overlook the importance of being aware of potential cost leakage that can be exploited by cloud service providers due to misprovisioning or misconfigurations in their cloud implementations, similar to how attackers continuously exploit vulnerabilities in security systems.

Assumptions

Failing to validate the effectiveness of security controls or the capacity of provisioned resources can pose risks and negatively impact both security and cost management. When assumptions are made without proper benchmarking or validations, vulnerabilities may arise, potentially compromising the system's security.

Likewise, assuming resource capacity without adequate benchmarking can result in overprovisioned and underutilised resources, leading to unavoidable expenses or performance issues.

The right approaches

While there are similarities in the challenges, there are also similarities in the approaches to remediate them. Embracing this synergy empowers enterprises to not only conquer challenges but to architect a cloud environment that thrives on proactive enhancements.

Proactive approach

Integrating security and cost considerations early in the design and implementation stages is vital for a secure and cost-efficient cloud environment. By incorporating multilayered security controls and comprehensive cost controls from the start, enterprises can prevent vulnerabilities and inefficiencies. Proper benchmarking and capacity planning enable understanding of

resource needs, optimising allocation, and avoiding unnecessary expenses.

Governance and policies

Establishing governance frameworks and policies ensures consistent implementation of security measures and cost optimisation strategies. These policies act as guardrails, enforcing compliance across all enterprise teams and promoting consistency. Continuous evaluation and refinement of these policies enhance cloud operations, strengthen security and risk management, and optimise costs effectively.

Continuous improvement

Real-time monitoring is essential for both security and cost optimisation. In security, it helps to identify and respond to threats and vulnerabilities. In cost optimisation, it helps to identify areas for improvement and cost-saving opportunities.

Achieving the right balance between security and user experience is important in cloud security. Enterprises must avoid unnecessary restrictions while ensuring adequate protection. In cloud cost optimisation, enterprises strive to achieve an optimal equilibrium between resource requirements and cost efficiency.

By actively pursuing continuous improvement, enterprises can strengthen their cloud security posture, minimise cost leaks, and effectively adapt to evolving threats and changing business requirements in the cloud environment.

Risk management

Both cloud security and cost optimisation require assessing potential risks. Enterprises need to prioritise security measures and provision resources diligently to mitigate identified risks. Similarly, in cost optimisation, enterprises assess their cloud environment to identify potential sources of cost leakage and inefficiencies. Conducting risk assessments in both disciplines allows enterprises to focus efforts on critical areas of failure and make informed decisions for enhanced security and cost efficiency.

Anomaly detection

Cloud security anomaly detection involves identifying abnormal or suspicious activities in a cloud environment to detect potential security threats or breaches. By analysing security data, logs, and events, enterprises can spot anomalies that deviate from expected behaviour. Implementing effective cloud security anomaly detection enables proactive threat response, data protection, and a strong security posture.

Likewise, monitoring and analysing factors like resource utilisation, service usage, data transfer, and billing data help identify anomalies in cloud costs. This allows enterprises to uncover cost inefficiencies, billing errors and unauthorised usage, and mitigate unexpected expenses.

Automation and tools

Automation is essential for improving cloud security and cost management. It enables consistent implementation and management of security controls, provides insights into resource utilisation and cost allocation, and enhances operational efficiency.

In cloud security, automation tools monitor for threats, detect anomalies, and facilitate swift incident response. Similarly, for cost management, these tools analyse usage data, identify cost-saving opportunities, enforce budget controls, and generate detailed cost reports.

Embracing automation ensures continuous monitoring and optimisation of security and cost in the cloud environment, reducing manual effort and building visibility. Furthermore, automation can be calibrated to automatically address cost anomalies or leakages, like an automated response for security incidents.

Collaboration and awareness

Establishing central teams responsible for defining policies, approaches, and solutions is essential. These teams work in collaboration with decentralised development and operations teams to ensure effective implementation. Streamlined processes for resource allocation are necessary to maintain consistent security measures and optimised cost management across distributed teams and applications.

Training employees on security best practices and cost optimisation strategies creates a culture of security and cost consciousness. This empowers individuals to contribute to a secure environment and optimise cloud costs effectively.

Integrating cloud security principles into cost optimisation minimises risks and promotes consistent cost governance. Proactive analysis of potential leakage enhances financial performance and budget control, and leads to optimised cloud costs.

While cloud financial operations (FINOPS) is still a developing discipline, there is a lack of structured approaches to address cloud cost leakages. In the next article in this series, I will delve into how applying additional security principles can help to optimise cloud costs and mitigate financial risks. END

Arun Karthik Dharmalingam

The author is an enterprise cloud security architect working at Thoughtworks. He is experienced in strengthening the cloud infrastructure of businesses by adopting a combination of offensive and defensive strategies.

Some Advanced FFmpeg Tricks

FFmpeg is not just for video editing or video conversion. It's a versatile toolkit that has a world of creativity waiting at your fingertips. Try out some of its advanced tricks.



Image Source: https://www.freepik.com

Did you know that FFmpeg also includes a media player? Did you know that it can apply FFmpeg filters and play the output in real-time?

Early this year, my FFmpeg book was published by Apress. Interestingly, I continue to discover new FFmpeg tips and tricks every month. Here are some new ways with which I now use FFmpeg to automate my multimedia tasks.

FFplay

FFmpeg is a massive project. It is not just one executable. The FFmpeg project provides several executables for end users and several libraries for software developers. *ffmpeg*, *ffplay*, and *ffprobe* are the most popular programs for end users. Some other tools such as *ffescape* and *ffeval* appear to be available only for Windows users.

ffplay is a barebones media player. It does not have any main menu or context menu. Users must employ certain keys and mouse actions to control playback.

Action	Function
SPACE bar	Play or pause playback
LEFT and RIGHT	Fast-forward or re-wind by 10 seconds
UP and DOWN	Fast-forward or rewind by 1 minute
Double-click	Toggle between windowed and full screen view
Right-click	Move forward or backward using an invisible playback slider

Like *ffmpeg*, *ffplay* displays a huge banner and generates numerous text messages on the console. You can hide them using some switches:

```
ffplay -hide_banner -nodisp -autoexit \
       Nightfall-Stone-Ship.mp3
```

Even with this arrangement, *ffplay* is not entirely quiet because it also writes to *standard error*. For a clean console, try:

```
ffplay -loglevel quiet \
       Nightfall-Stone-Ship.mp3
```

FFmpeg integration with Caja file manager

Instead of GNOME 3, I use the user-friendly and customisable Mate desktop. The Mate project has forked the Nautilus file manager (from GNOME 2) and created a replacement called Caja. In Caja, I use *Caja Action Configurations* to create my custom menus for various multimedia file types. These custom menus make it easy to perform FFmpeg-related tasks on multimedia files.

Generating waveforms of audio streams

FFmpeg can create a variety of real-time graphics after analysing the waveforms of audio streams. To use the *showwavespic* filter, follow this script:

```
sInputFileName="$*"
sOutputFileName="${sInputFileName%.*}.
```

```
png"

ffmpeg -i "${sInputFileName}" \
       -lavfi "[0:a:0]
showwavespic=s=600x120:
                split_channels=1:
                colors=yellow|red:
                scale=sqrt" -update 1 \
       "${sOutputFileName}"
```

Audio normalisation and compression

Some multimedia files suffer from low audio volume. Rather than blindly increasing the volume, you should first use the 'volumedetect' filter to detect the highest decibel level and then use the 'volume' filter to expand or maximise the waveform accordingly.

```
ffmpeg -i low.mp3 -af "volumedetect" \
       -f null -

ffmpeg -i low.mp3 \
       -af 'volume=17dB' -f ogg \
       normalized.ogg
```

In this example, the 'volumedetect' filter found that the maximum volume was at -17dB. To bring it to 0dB, you can set the 'volume' filter to 17dB. This expands the waveform to the maximum safe level. If we expand the waveform beyond the maximum value (17dB) identified by the 'volumedetect' filter, some of the peaks of the waveform will start to get chopped off. Chopped-off waveform means a permanent loss of some audio content.

Normalisation may not always raise volume levels. Imagine a conversation recorded on a microphone placed on a desk. If someone jerks the desk, the microphone will wobble and introduce high-volume spikes into the recording. Since these spikes set the bar, the recording software will encode the conversation with low volume. Imagine another case where there is a speaker who is close to the microphone and his voice is recorded normally while that of someone in the audience is barely discernible. The low-volume sections caused by the audience member cannot be expanded unless the audio of the first speaker is compressed.

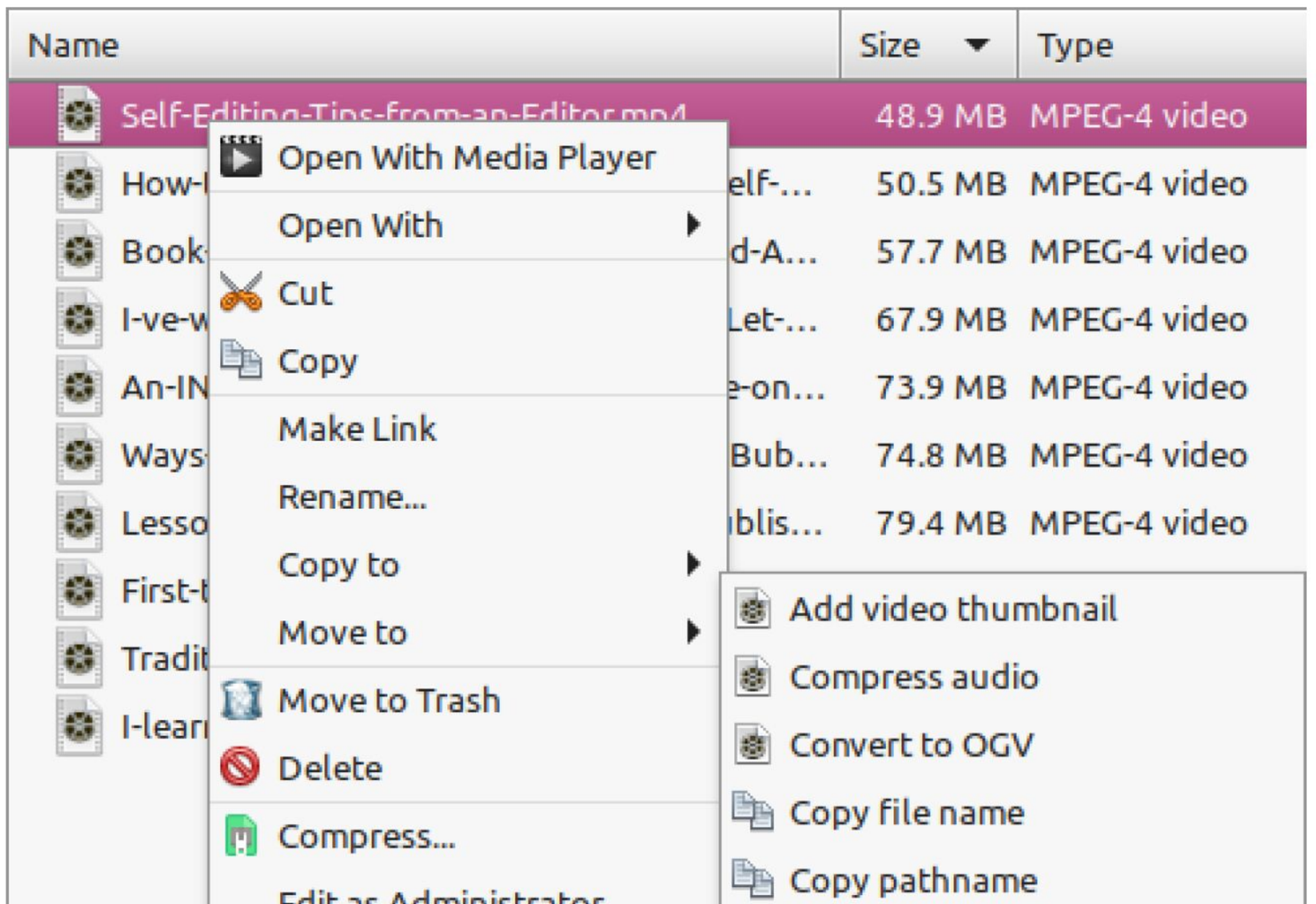


Figure 1: Caja context menus help automate FFmpeg tasks

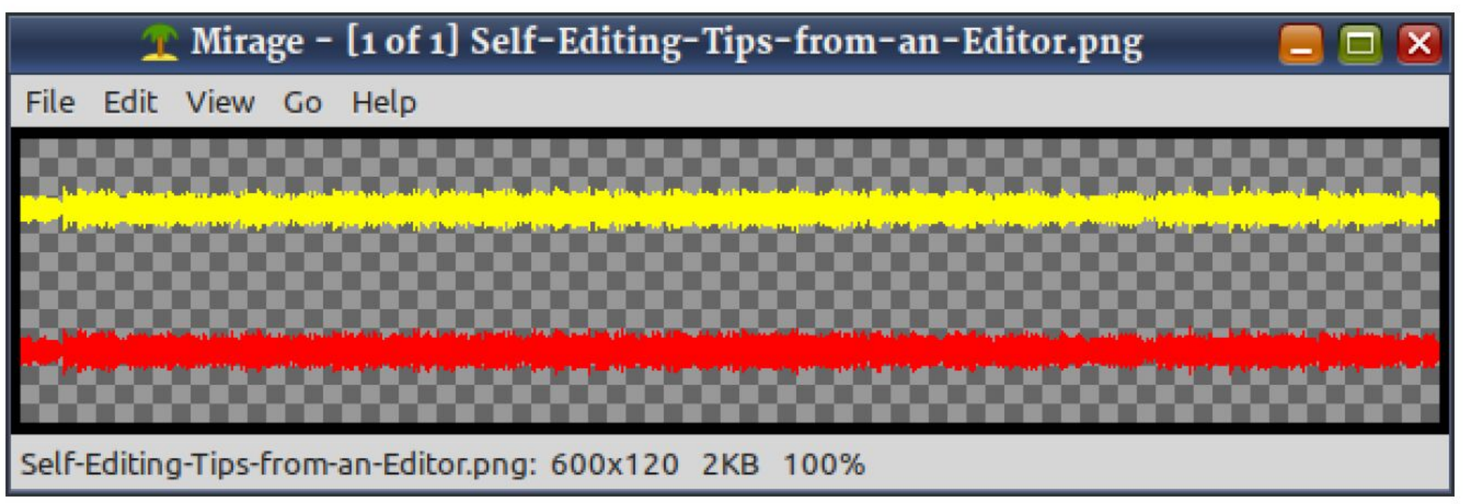


Figure 2: The output of the *showwavespic* filter can be saved as an image

Rather than considering the entire audio and not being able to normalise it, the smarter approach would be to take smaller chunks of the audio and dynamically expand or compress their waveforms. This is known as *dynamic audio normalisation* and *dynamic audio compression*, respectively.

The 'dynaudnorm' filter can perform both functions but the default

is normalisation. When the 'guasssize' filter option is set at the lower end of 3, it behaves like a typical compressor. At the other end of 300, it becomes a traditional normaliser.

```
ffmpeg -i train-trip.mp3 \
       -filter:a dynaudnorm=gausssize=3
\
       train-trip-normalized.mp3
```

Do not use the filter indiscriminately. *Dynamic audio compression* is also known as *dynamic range compression*. It is the bane of popular music today. It makes the recording very boring. In Carl Orff's composition of *O Fortuna* or Ryuichi Sakamoto's score for the end-credits of the movie *Femme Fatale*, the music starts on a low note, builds slowly in a steady crescendo and abruptly drops off a high cliff. Compressing such an audio will ruin the composer's intent.

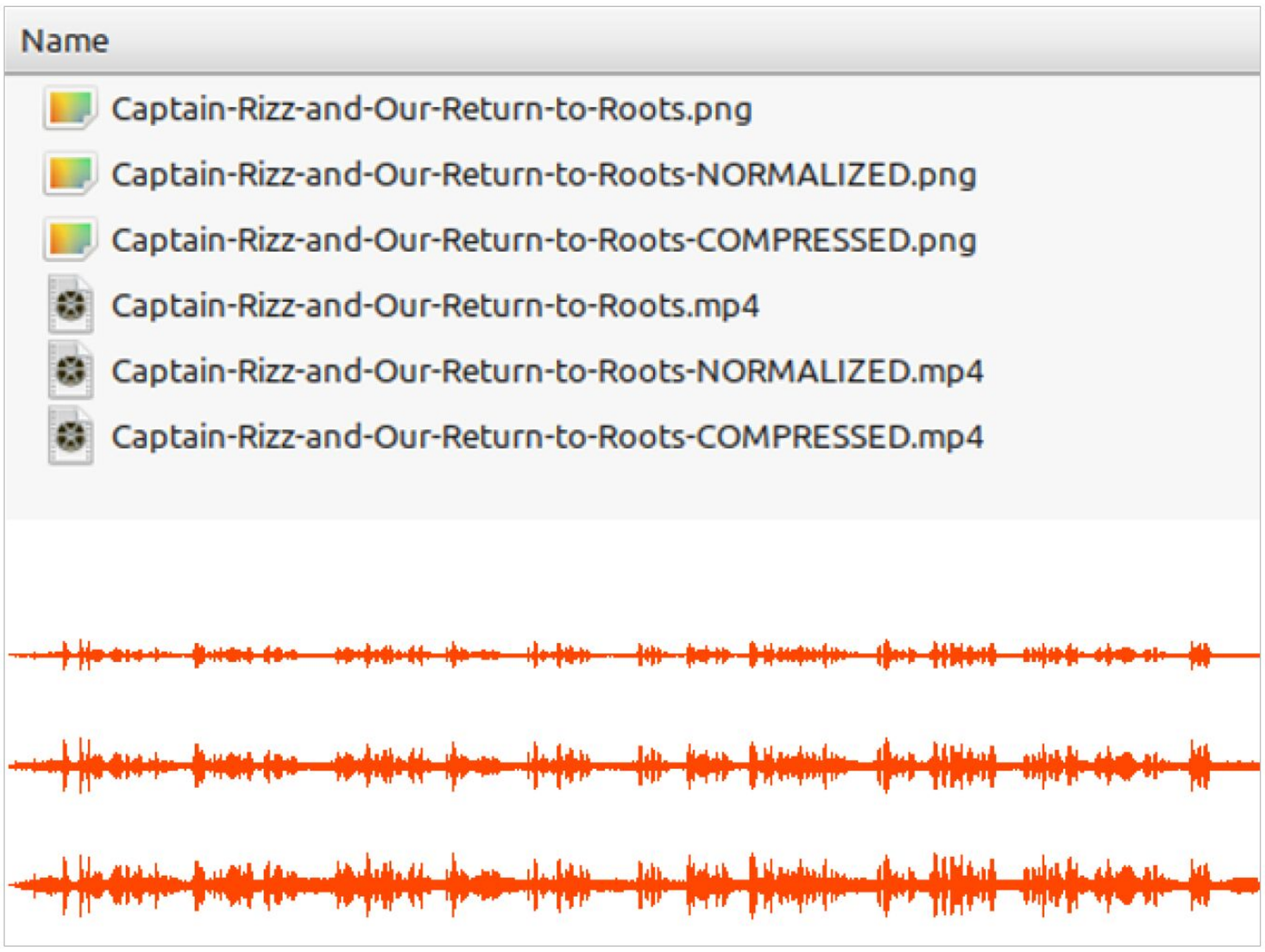


Figure 3: Waveform images of an audio file before and after normalisation and compression

Using FFplay and 'dynaudnorm'

Despite having a fibre internet connection, its challenging to play online videos on my PC, let alone stream them to my TV. To address this, I have written a browser script (*www.opensourceforu.com/2016/03/the-utility-of-user-scripts-js-and-user-styles-css*) that automatically detects online videos and displays their location (URL). Using this script and a download manager, I mass-download videos and see them offline.

Another problem with the videos (recorded mostly by other writers) is that they have very loud intro music and the useful content is recorded with low volume. Rather than fiddle with volume control for every video, I use a *Caja Action* that uses the 'dynaudnorm' filter and 'ffplay'. In addition to files, 'ffplay' can play the processed output of filters in real-time. I use the '-f lavfi' option for this.

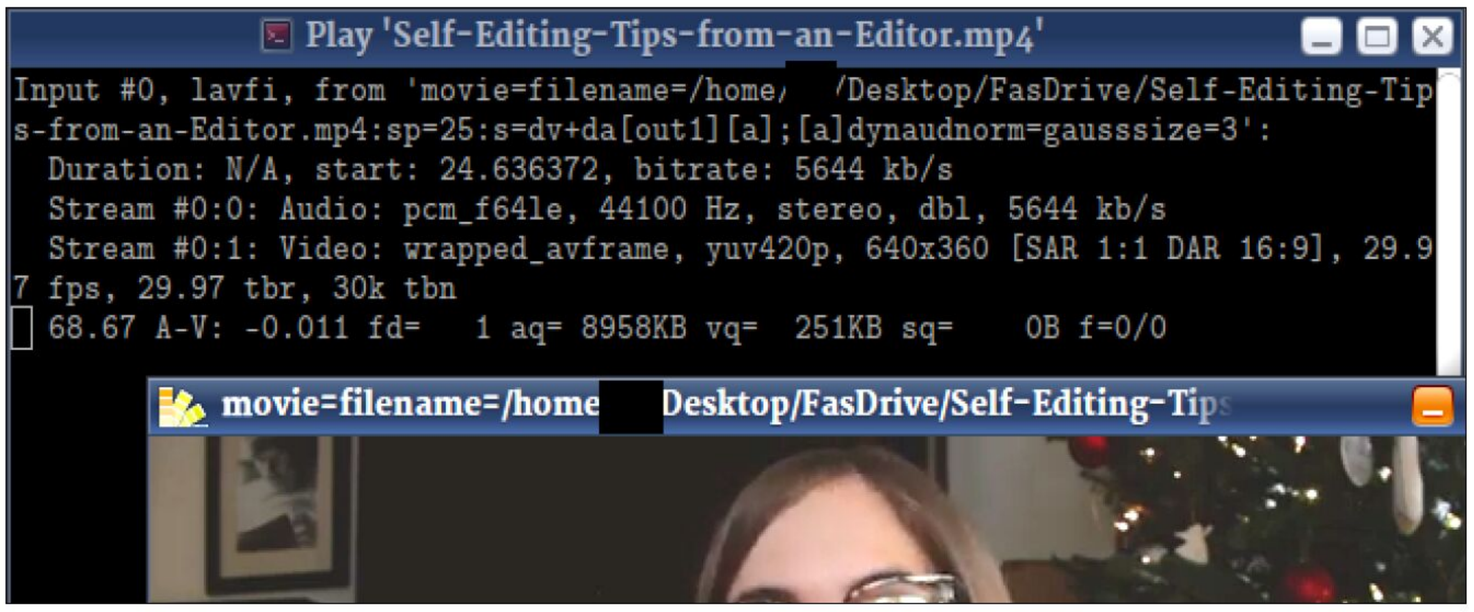


Figure 4: FFplay can play the output of filters in real-time

```
ffplay -hide_banner -autoexit -f lavfi \
       "movie=filename=${sFile}:sp=25:s=d
v+da[out1][a];
        [a]dynaudnorm=gausssize=3"
```

The 'movie' filter plays the video. Its 'sp' option skips the first 25 seconds. The 'dynaudnorm' dynamically compresses the remaining audio.

I am listening to other authors talking about their books. It is not classical music or some symphony orchestra. Compressing such videos is entirely justified.

Some online video creators use a microphone with an active compressor. Their videos have a constant volume. For content creators who mix intro or outro music, I recommend processing their videos with the 'dynaudnorm' filter before uploading the output. END

```
sFile=Self-Editing-Tips-from-an-Editor.
mp4
```

By: V. Subhash

The author has written over two dozen books including Linux Command-Line Tips & Tricks, CommonMark Ready Reference, Cool Electronic Projects and How To Install Solar.

IOTSHOW.IN

31ST JAN - 2ND FEB 2024 • KTPO • BENGALURU

PROFIT FROM IOT



INDIA'S ONLY EVENT FOR THE **CREATORS**
AND THE **SOLUTION PROVIDERS** OF IOT

IoTshow.in is India's biggest conference-cum-expo on Internet of Things.

Visitor Registration: www.iotshow.in. ***Special Offers for first 1000 Registrants!***

CO-LOCATED WITH:

INDIA ELECTRONICS WEEK

BROUGHT TO YOU BY:



MORE INFO:

Web: www.iotshow.in
Email: support@efy.in
Bulk Registration: iew@efy.in
Tel: +91-9811155335

R N I No. DELENG/2012/49440, Mailed on 27/28th of Advance month
Published on 27th September 2023
Delhi Postal Regd. No. DL(S)-01/3443/2022-24
Licenced to Post without Pre-Payment Licence No U(S)-56/2022-24
Posted at LPC Delhi RMS Delhi 110006

India's No.1 Electronics Magazine
RANKING AS PER ELCINA-IMRB REPORT

"I started reading it when I was a student...and I am still reading it, as a student"

—CEO, Design House



electronics YOURS SINCE 1969 FOR YOU

To Subscribe:
https://subscribe.efy.in

OR

Scan This Code

For any query, call: +91-98111-55335 or email: support@efy.in

