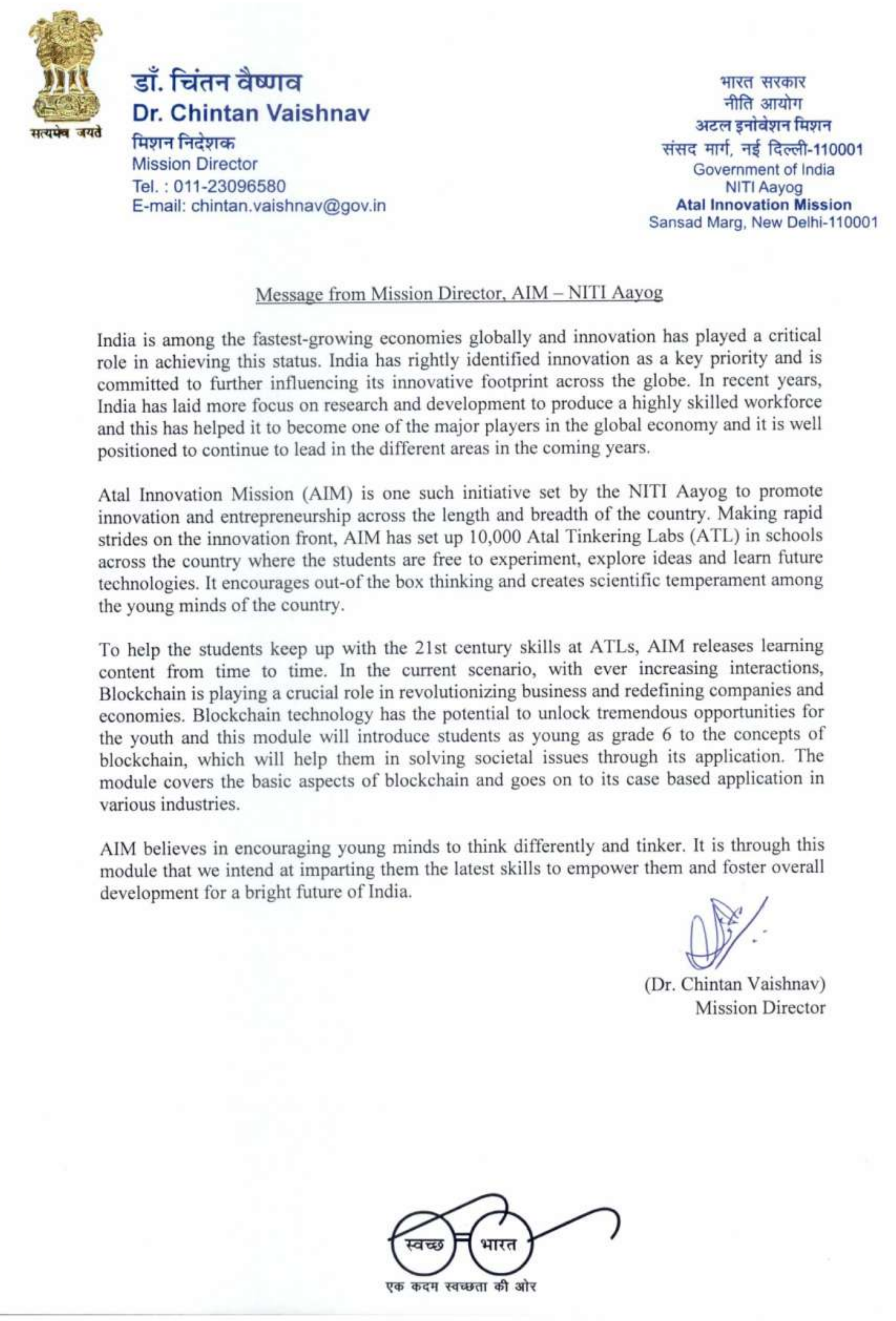
NITI Aayog | ATAL INNOVATION MISSION | 5ire | Network Capital

ATL Blockchain Module

Dr. Chintan Vaishnav

Mission Director



डॉ. चिंतन वैष्णव
Dr. Chintan Vaishnav
मिशन निदेशक
Mission Director
Tel. : 011-23096580
E-mail: chintan.vaishnav@gov.in

भारत सरकार
नीति आयोग
अटल इनोवेशन मिशन
संसद मार्ग, नई दिल्ली-110001
Government of India
NITI Aayog
Atal Innovation Mission
Sansad Marg, New Delhi-110001

Message from Mission Director, AIM – NITI Aayog

India is among the fastest-growing economies globally and innovation has played a critical role in achieving this status. India has rightly identified innovation as a key priority and is committed to further influencing its innovative footprint across the globe. In recent years, India has laid more focus on research and development to produce a highly skilled workforce and this has helped it to become one of the major players in the global economy and it is well positioned to continue to lead in the different areas in the coming years.

Atal Innovation Mission (AIM) is one such initiative set by the NITI Aayog to promote innovation and entrepreneurship across the length and breadth of the country. Making rapid strides on the innovation front, AIM has set up 10,000 Atal Tinkering Labs (ATL) in schools across the country where the students are free to experiment, explore ideas and learn future technologies. It encourages out-of the box thinking and creates scientific temperament among the young minds of the country.

To help the students keep up with the 21st century skills at ATLs, AIM releases learning content from time to time. In the current scenario, with ever increasing interactions, Blockchain is playing a crucial role in revolutionizing business and redefining companies and economies. Blockchain technology has the potential to unlock tremendous opportunities for the youth and this module will introduce students as young as grade 6 to the concepts of blockchain, which will help them in solving societal issues through its application. The module covers the basic aspects of blockchain and goes on to its case based application in various industries.

AIM believes in encouraging young minds to think differently and tinker. It is through this module that we intend at imparting them the latest skills to empower them and foster overall development for a bright future of India.

(Dr. Chintan Vaishnav)
Mission Director

स्वच्छ भारत
एक कदम स्वच्छता की ओर

MESSAGE FROM PRATIK GAURI

Pratik Gauri

Founder & Chief Executive officer - 5ire

It is our pleasure to collaborate with Atal Innovation Mission to produce the ATL Blockchain Module. At 5ire, we strive to be at the forefront of the 5th industrial revolution by creating a blockchain ecosystem that empowers self-sovereign decentralized organizations and incentivizes them to accelerate the implementation of the United Nations 2030 Agenda for Sustainable Development.

Investing in the education of young students today is not only an investment in their future, but also in the future of our planet.

By educating the next generation about blockchain technology and its potential to promote sustainable development, we are not only empowering them with the knowledge and skills needed to tackle environmental challenges, but also inspiring them to come up with innovative solutions to address these issues. At 5ire, we believe that by working together and supporting education initiatives, we can make a real difference in the world and achieve our mission of creating a sustainable future for all.

Blockchain education is crucial for students in today's world as it opens a plethora of opportunities for their future careers and entrepreneurial endeavors. A deep understanding of blockchain technology and its potential impact on various industries can give students a competitive edge in the job market. Furthermore, blockchain technology has the potential to revolutionize various industries, creating new opportunities for entrepreneurs. By educating students about blockchain, they can gain the knowledge and skills needed to start their own blockchain-based businesses and shape the future with innovative solutions. Investing in blockchain education is not just investing in the future of individual students, but also in the future of the society and the planet as a whole.

As the CEO of 5ire, I am proud to say that we are committed to creating a sustainable future through blockchain technology. Our goal is to empower self-sovereign decentralized organizations and incentivize them to accelerate the implementation of the United Nations 2030 Agenda for Sustainable Development. We believe that through education, innovation and collaboration, we can create a more transparent, secure and decentralized ecosystem that can promote sustainable development and make a real difference in the world.
Let's work together to shape a better future for all.

MESSAGE FROM UTKARSH AMITABH

As the CMO of 5ire.org and the CEO of Network Capital, I am energised to see the blockchain module come to life. Network Capital has served as a partner for Atal Innovation Mission since 2016. Through these years of partnership, it has been a matter of pride to see India's mentoring movement scale and reach 7.5 millions school students. Both 5ire and Network Capital are committed to enabling a new generation of innovators and entrepreneurs in India by supporting their upskilling in new technologies such as web 3.0 and blockchain.

Utkarsh Amitabh
CMO of 5ire & CEO of
Network Capital

The Atal Tinkering Labs play a critical role in preparing the young minds of India for a technologically mediated 21st century. It provides them a constructive space to follow their curiosity, tinker and build projects that solve actual social problems. With the launch of the ATL Blockchain Module, I would like to invite all ATL students to leverage the power of blockchain for change.

In my second book 'Passion Economy and the Side Hustle Revolution', I write about the future of ownership driven and decentralised Internet. I study some of the most interesting artists, entrepreneurs and scholars to see how Blockchain and Web3 are revolutionising the future of work and employment. The fundamental promise of ownership, transparency, decentralisation and trust that blockchain holds is important for the next era of Indian technology pioneers. Building on the findings and insights from the book, our goal for the ATL Blockchain Module is to help our students build meaningful avenues of work and job creation. Understanding technology is an important component of this process.

As the ATL students and Mentors of Change learn from our blockchain module, I would urge them to consider important and practical use-cases for the technology. Building anything meaningful is an iterative process, and I wish all students an adventurous and insightful tinkering journey.

FOREWORD

Deepali Upadhya
Program Director,
Atal Innovation Mission

Under the aegis of Atal Innovation Mission, Atal Tinkering Labs were set up with the goal of inspiring a generation of neoteric innovators and entrepreneurs in India. The underlying philosophy of our ATLs has been to equip the young minds of India with all the knowledge and skills necessary to thrive in the twenty-first century. The idea is to allow children to explore the world of research and innovation, and contribute towards nation development, by developing innovative and disruptive solutions to India's biggest community problems.

In 2022, the Atal Tinkering Labs achieved the milestone of setting up 10,000 labs across India. Today over 75 lakh students in India get to learn in these ATLs. With this accomplished, in the next stage of development our goal is to ensure that the ATL students have the best tools and resources to learn from.

Towards this end, we are thrilled to launch the ATL Blockchain Module in partnership with 5ire and Network Capital. Blockchain technology has emerged as a driving force in the world of data technologies and interest services. It is fundamentally transforming how we look at collaboration, information exchange and institution building in the twenty-first century. With the ATL Blockchain Module, we hope our ATL students will be able to learn and apply the various facets of blockchain in their innovation and entrepreneurship activities to build sophisticated and useful solutions and products for their communities.

Happy tinkering!

TABLE OF CONTENTS*

*This book is purely for educational use and doesn't intend any copyright infringement

TABLE OF CONTENTS*

PAGE NO

*This book is purely for educational use and doesn't intend any copyright infringement

TABLE OF CONTENTS*

*This book is purely for educational use and doesn't intend any copyright infringement

01

Introduction to **Blockchain**

01 —— Introduction to Blockchain

A blockchain is a distributed software network that functions as a digital ledger and a mechanism that allows the safe and secure transfer of assets without requiring an intermediary. Blockchain could be defined as a technology that helps to facilitate the digital exchange of units of value. Various assets such as currencies and real estate etc can be stored, tokenized, and exchanged on a blockchain network.

Apart from the safe and secure transfer of value, blockchain technology provides a permanent record of transactions. It shows a network state that is highly transparent and can be displayed in real-time to provide benefits to all participants.

The key distinguishing factor between blockchain and traditional databases is decentralization. In the latter, information is stored in centralized servers and managed by a central authority. Blockchain, however, includes independent nodes, which are equivalent to servers in the traditional setting. Each node in a blockchain possesses an exact copy of the information stored in other nodes.

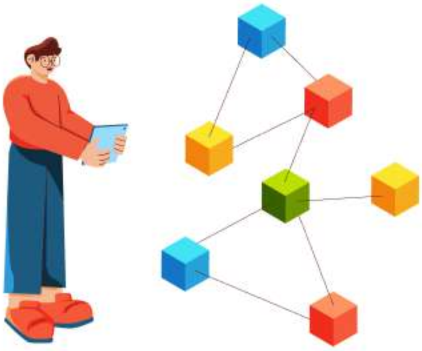
Example:

Let us understand Blockchain technology through an example. Think of a situation where a 6-year-old Kushi wants a video game for Christmas. As a result, she writes a letter to Santa Claus sharing her wish for the video game. However, Khushi is unsure how to get the letter to Santa. She asks his father to send the letter. Before mailing the letter to Santa, Khushi’s father reads out the letter. Khushi’s father doesn't want her to waste her time playing video games.

Khushi’s father changes the letter's content and replaces them with books on science and technology. Khushi gets heartbroken after receiving her Christmas gift. She is sad that Santa did not fulfill her wish by giving her a video game. The middleman (Khushi’s father) disrupted Khushi’s intended delivery to Santa.

Now let's analyze Khushi’s situation from a different scenario. Let us assume that Khushi uses a blockchain network known as "The North Pole blockchain network." This network has Santa, his kids, and elves from all over the world as well as their parents as participants. John can now send his letter asking for a video game on the blockchain network. As a result, everyone on the network can view his request. When Khushi’s father views the request and tries to change it, the network doesn't approve his changes. Therefore, the final transaction on the blockchain is Khushi’s wish in the letter asking for a video game. The blockchain makes sure that Khushi can get her transaction completed precisely in the manner in which he wants to.

Key elements of blockchain:



Distributed ledger technology:
All participants within the network have access to the distributed ledger as well as the immutable record of transactions. In the shared ledger, transactions are only recorded once. This results in the removal of any duplication of effort similar to traditional business networks.

Immutable records:
No participant can change any transaction after it is recorded in the shared ledger. If there is an error in a transaction record, a new transaction should be added for the purpose of reversing the error. As a result, both transactions are evident.

Smart contracts:
For the purpose of speeding up transactions, a specific set of rules — called a smart contract — is stored on the blockchain and automatically executed.

How blockchain technology works

Each transaction is recorded as a block of data:
All the transactions on a blockchain show the movement of an asset that can be tangible (a product) or intangible (intellectual). The data block also records the specific information of your choice.

Every block is connected to the ones before and after it:
These blocks create a chain of data as an asset moves from place to place or ownership changes hands. The blocks also confirm the specific time and sequence of transactions. Moreover, the blocks securely link together to prevent any block from being altered or a block inserted between two existing blocks.

Transactions are blocked together in the Blockchain:
Every additional block results in verifying the previous block. This also results in verifying the entire blockchain. This makes the blockchain tamper-evident as it results in creating immutability. It also removes the potential of tampering by a malicious actor and creates a ledger of transactions you and other network members can trust.

02

Benefits and Challenges of **Blockchain**

02 —— Benefits and Challenges of Blockchain

Blockchain shows a promising future in the emerging tech landscape. It increases trust, transparency, security, and traceability of data shown across a business network - delivering cost savings with efficiencies.

Benefits of blockchain

Enhanced Security:
Digital transformation has been a success in ushering in the new era of virtualization. However, it accompanies the threat of personal data theft. The Equifax data breach in 2017 cost the firm at least $575 million to settle charges, while Morgan Stanley paid $120 million over failed encryption that identified current and former clients.

This data breach is essentially the result of financial institutions storing large amounts of confidential data on centralized servers, creating a single point of vulnerability.

With blockchain taking the security charge, it can significantly change how critical information is viewed. By creating a record that can't be altered and is encrypted end-to-end, blockchain helps prevent fraud and unauthorized activity. Information is stored across a network of computers rather than a single server, making it difficult for hackers to view data. Blockchain also caters to privacy concerns by anonymizing data and user permissions to control access. Further, blockchain also addresses privacy issues by anonymizing personal data and limiting the available information via users' permission access.

Greater Transparency:
Blockchain makes data transparent in a way that has not existed in financial systems, which is why many argue that blockchain could be used as the new standard for transparency. But how exactly is data made transparent on the blockchain?
A blockchain is an immutable distributed ledger (date and time-stamped) allowing every transaction to be viewed.

Blockchain distributes information across a network of connected computer systems making it more secure and less prone to unauthorized data tampering. It maintains a complete history of past transactions within the network, which means the user can track the data with complete transparency.

Instant Traceability:

As an asset travels through its lifecycle, a blockchain-based audit trail records each step of its origin. This helps to prove in industries where customers are worried about environmental or human rights issues surrounding a product — or in industries plagued by fraud and counterfeiting. Customers can directly access provenance information thanks to blockchain technology. Traceability data can reveal weak points in any supply chain where goods can be sitting on a loading dock waiting to be transported.

Increasing efficiency and speed:

Traditional paper-intensive procedures are time-taking, subject to human errors, and frequently call for third-party mediation. Blockchain facilitates quick transactions by automating these operations with blockchain technology. Documentation and transaction details can be stored on the blockchain, eliminating the need to exchange paper. Subsequently, clearing and settlement no longer require reconciling various ledgers with blockchain holding power to store data.

Automation:

Blockchain technology and smart contracts eliminate the need for intermediaries to enforce contracts, verify transactions, or perform background checks. The next phase of a transaction or process is initiated automatically after pre-specified requirements are satisfied. Smart contracts lessen the need for third parties and human intervention to confirm that a contract's provisions have been followed. For instance, if a customer files an insurance claim and provides the required supporting evidence, the claim may be automatically resolved and paid.

Challenges of Blockchain Adoption

Blockchain is a new technology with its own set of challenges. While this cutting-edge technology may assist level the playing field for firms of all sizes, it also has drawbacks and risks for consumers and companies who want to utilize it. Some of these challenges include:

Security:
Security is another crucial topic here. We all know how every blockchain technology boasts about its security. But like any other technology, blockchain also comes with a few security loops. In 2018, three renowned cryptocurrency platforms experienced issues from 51% of attacks. Furthermore, enterprises recently lost around 20 million dollars annually due to 51% of attacks. It identifies the need for additional security layers to overcome such scenarios. While there's a lot of effort to create new privacy protocols, such as proof of zero-knowledge, we're still a long way from a new identity structure.

Lack of Adequate Skill Sets:
Blockchain is an emerging technology; however, its adoption is still in its infancy. There aren't enough people with the right abilities to create and utilize it. According to the Blockchain Council, demand for blockchain engineers increased by more than 500% in 2019 over the previous year, and base pay for blockchain developers increased in lockstep with this growth.

Scalability:
One of the most significant issues with blockchain technology, and consequently enterprise blockchain technology, is its inability to support many users. Although transaction networks can process hundreds of transactions per second without experiencing any problems, processing transactions for Bitcoin and Ethereum (which each process about 3–7 transactions per second and 15-20 transactions per second, respectively) is very slow, rendering blockchain unusable for large-scale applications.

Criminal Activities:
The anonymous feature of blockchain technology attracted experts and criminal personnel. Why? Well, the nature of the network is decentralized, so no one can know your true identity. This makes bitcoin the primary target used as a currency in the black market and the dark web.

Criminals now use these cryptocurrencies to purchase limited illegal equipment and payment methods. They also ask for cryptocurrencies in exchange for a ransom. Further, the absence of stringent legislation and the fact that blockchain is still a developing technology have fueled the rise of fraudulent projects and other bad actors seeking to profit from inexperienced investors.

There have also been several high-profile cryptocurrency exchange hacks, including Mt. Gox's infamous bitcoin theft in 2014, nearly destroying the entire cryptocurrency industry.

High Energy Consumption:

Energy consumption is another blockchain adoption challenge. Most of the blockchain technology follows bitcoin's infrastructure and uses Proof of Work as a consensus algorithm which is energy intensive. This restricts entry for regular people into PoW networks, encourages the formation of big mining pools, prevents decentralization by pushing individuals to join large mining pools, and raises environmental concerns.

Blockchain Interoperability:

Interoperability between blockchain networks refers to the capacity to exchange, see, and access data without the aid of a middleman or centralized authority. As more businesses utilize blockchain, there is a propensity for many companies to create their systems with different features (governance rules, blockchain technology versions, consensus models, etc.). There is no global standard to allow various networks to connect; therefore, these many blockchains cannot cooperate.

Given the number and complexity of these blockchain issues, it would be unrealistic to think they are not significant roadblocks to its adoption. However, blockchain is an advancing field, and these limitations could highlight new opportunities for various blockchain networks to focus on and improve.

03

Understanding **Blockchain's** Decentralised Model

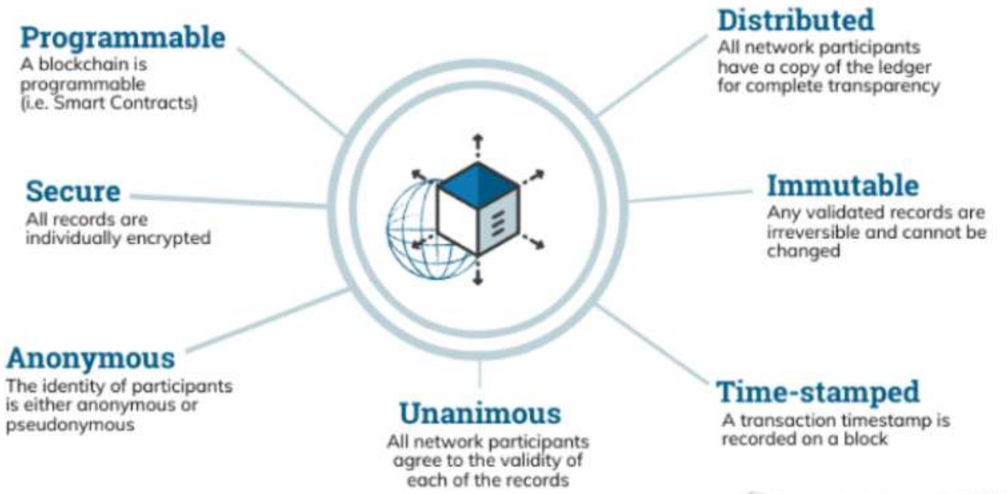
03 —— Understanding Blockchain’s Decentralized Model

In the blockchain, decentralization alludes to the transfer of supervision and decision-making from a centralized association (individual, corporation, or group of people) to a dispersed network.

A blockchain is a decentralized network made up of multiple nodes or members. It does not have a central authority. Instead, control over the network is distributed among various participants. In a centralized structure, the entire system fails if the primary node is compromised. However, a decentralized distribution ensures that the blockchain network continues functioning even if one or more nodes are compromised.

Besides the fundamentals of a blockchain protocol, the decentralized ledger incorporates eight key features that streamline the data storage and management process.

The Properties of Distributed Ledger Technology (DLT)


Programmable
A blockchain is programmable (i.e. Smart Contracts)
Distributed
All network participants have a copy of the ledger for complete transparency
Secure
All records are individually encrypted
Immutable
Any validated records are irreversible and cannot be changed
Anonymous
The identity of participants is either anonymous or pseudonymous
Unanimous
All network participants agree to the validity of each of the records
Time-stamped
A transaction timestamp is recorded on a block

© Euromoney Learning 2020

Advantages of the Decentralisation:

There are various advantages to decentralization. One significant advantage of decentralization is that the users control their transactions entirely. This implies that individuals don't need permission from a centralized authority to begin a transaction whenever they wish. Simply said, a decentralized network uses consensus mechanisms to validate the information, and the verification process is not dependent on outside parties. Second, the data structure of blockchain technology is append-only. This means that anyone cannot change or alter the data once it is stored. Further, the way decentralized networks manage data and transactions makes them secure. To make sure that the data ledgers are secure, they employ cryptography.

04

Uses of **Blockchain** in Different Industries

04 —— Uses of Blockchain in different industries

Just a couple of years ago, the public image of blockchain was inextricably linked with cryptocurrencies. Today, the technology finds its way to businesses representing various industries, addressing such hot spots as data security and anonymity along with publicity and consistency of transactions. Multiple sectors have started adopting blockchain as a part of their strategic planning. Some of these include:

Automotive:
Every part of the complex automotive business ecosystem — from parts suppliers and manufacturers to customers and safety regulators — relies on a network of transactions and knowledge that starts long before a vehicle is manufactured and extends far beyond its purchase.
With a shared record of ownership, location, and movement of components and items, blockchain can foster efficiency, transparency, and trust. Additionally, the flexibility of blockchain records is ideal for advancing alongside cutting-edge new business models.

Example: A prominent example of an automotive company using blockchain is Porsche. In 2018, Porsche paired up with blockchain startup "XAIN" to implement blockchain technology within their vehicles. The blockchain would allow users to unlock their vehicles with an app and provide more accessible automated payment systems.

Banking and Financial Services:
According to an IBM report, 91% of the banks invested in blockchain in 2018. Financial firms can use blockchains for record-keeping and bookkeeping to comply with regulatory bodies and distribute unchangeable transaction records unaffected by outside influences. Blockchain-based financial apps provide faster transaction settlements, which can enhance the quality of current financial services. Lenders, for instance, will be able to fund loans more quickly, vendors will receive payments more quickly, and stock exchanges can settle securities purchases and trades instantly.

Example: Ripple, a real-time currency exchange, gross settlement system, and remittance network created by Ripple Labs Inc., allows financial institutions to transfer money. The company's payment platform, RippleNet, enable financial institutions from across the globe to access a standardized network of institutions for transparent transactions.

Government:
With globalization and technological advancements improving business operations, digital financial crimes, especially money laundering, have also taken advantage of the new technologies. According to extensive research conducted by Zippia, approximately $300 billion is laundered annually in the US.
Government blockchain applications can improve local political engagement, improve bureaucratic efficiency and accountability, and reduce massive financial burdens. Like Illinois, some state governments in the USA are already using the technology to secure government documents.

Example: The UAE government digitizes paper records of all services, such as visa applications, bill payments, and license renewals. These records will now be smoothly transacted through the use of blockchain technology.

Healthcare and Life Sciences:
Though early in its adoption, blockchain in healthcare already shows promising results. Keeping medical data safe and secure is the most popular blockchain healthcare application, which isn't surprising. Security is a significant issue in the healthcare industry. 692 large healthcare data breaches were reported between July 2021 and June 2022. Blockchain prevents data breaches as it leaves no room for any forged data due to its immutability. Blockchain offers a solution to cyberattacks by decentralising the domain name system (DNS) entries. BIS Research has revealed estimated reports that the immediate application and integration of blockchain in healthcare could save more than $100 billion per year in costs related to IT, operations, support functions, personnel, and health data breaches by 2025.

Example: One of the leading examples of a company working with healthcare providers to implement blockchain-enabled EMR is Medicalchain. They allow patients to view their medical records updated by providing explicit consent every time they have been shared with healthcare providers or others.

Media and Entertainment Industries:
Digital media has changed the world for consumers, artists, and brands — yet major business problems persist. Media companies have already started to adopt blockchain technology to eliminate fraud, reduce costs, and even protect Intellectual Property (IP) rights of content – like music records. MarketWatch estimates that the global market for blockchain in media and entertainment will be $1.54 billion by 2024.

Example: One platform that has taken the spotlight in leveraging blockchain for media is **Eluvio, Inc.** Formally launched in 2019, Eluvio Content Fabric uses blockchain technology to enable content producers to manage and distribute premium video to consumers and business partners without content delivery networks.

Supply Chain:

A key concern in the supply chain and logistics sector is the lack of communication and transparency due to the plethora of logistics companies within the industry. Furthermore, data is skewed or manipulated as every logistics company uses its terms, making it hard for non-specialists. A joint study by Accenture and DHL found that more than 500,000 shipping companies in the US alone are causing data siloing and transparency issues. Blockchain's immutable ledger suits it well for real-time tracking of goods as they move and change hands throughout the supply chain. Using a blockchain opens up several options for companies transporting these goods. Entries on a blockchain can be used to queue up events with a supply chain — allocating goods newly arrived at a port to different shipping containers, for example. Blockchain provides a new and dynamic means of organizing, tracking data, and putting it to use.

Example: A prominent example of blockchain in supply chain management is the payment of suppliers in the coffee industry. Bext360 is utilizing blockchain technology to track elements of the worldwide coffee trade—from farmer to consumer—thereby boosting the supply chain's productivity.

Manufacturing:

Manufacturing is often stretched across the world to best exploit the availability of raw materials, labour, funding, and consumer markets at the most competitive rates. A single critical link can test the resilience of the entire operation because companies are bound closely together by long, international supply and demand chains.

From sourcing raw materials to delivering the finished product, blockchain can increase transparency and trust at every stage of the industrial value chain. Blockchain technology streamlines many business activities extending a company's potential time to market. With blockchain applications, supplier order accuracy improves, and product quality and delivery rates improve, resulting in higher customer satisfaction and increased revenue. It wouldn't be wrong to say that blockchain technology has become integral to every business realm and is shaping the future. Industries are rapidly adopting its advantages, signifying blockchain technology's future potential.

Example: For example, Honeywell Aerospace created a digital marketplace known as "GoDirect Trade" and sold used aircraft parts through the use of blockchain for storing the history of features in a trustful manner to protect market participants.

05

Blocks, Chains, and **Block header**

05 — Blocks, Chains, and Block Header

The information recorded on the blockchain is stored in blocks. Each data block contains a stipulated number of transactions and is cryptographically linked to the previously filled block. The continuous linking of blocks creates a chain of transactions– the blockchain.

The block header is a specific section within a block that serves as a summary of the rest of the block. It comprises all the metadata, which can further be described in detail as follows:

Block height: The block height of a particular block is defined as the number of blocks preceding it in the blockchain. A blockchain is an encrypted database that records a ledger of transactions sequentially in data structures known as blocks.

Block hash: The block header hash serves as Proof-of-Work for this block.

Previous block hash: The previous block hash makes sure that past blocks cannot be altered.

Timestamp: The timestamp illustrates the date when the block was published.

Merkle root: A Merkle root indicates the hash of all the transactions that have been included in this block.

Difficulty: The difficulty is encoded and is known as the “bits”.

Nonce: A nonce is a random number. It helps miners to satisfy the Proof-of-Work.

The block header serves as an efficient summary of a block. It can be sent throughout the network and can be processed when compared with a full block. When miners hash their block on a consistent basis, searching for a valid hash as Proof-of-Work, they are actually hashing the block header, not the entire block.

A block header is what the miners hash for trying and making the block valid. It is certainly much more efficient than hashing the entire block, which is made up of thousands of transactions.

06

Understanding **Blockchain** Consensus Algorithms

06 — Understanding Blockchain Consensus Algorithms

What is Blockchain

It is essential to grasp the idea of blockchain before delving deeper into consensus mechanisms.

Simply put, blockchain is a decentralized ledger for recording transactions. It is decentralized because no one entity is responsible for recording transactions on the ledger.

To put it into perspective, consider a big enterprise that employs accountants for their expenditures. Here the ledger is managed by a single authority. Irrespective of their number, all accountants are answerable to one employer.

On the blockchain, the opposite is the case. Nodes in the network update a blockchain ledger. Anyone who meets the requirement can function as a node on the blockchain and get rewards for doing so. The accountants described above are synonymous with the nodes in the blockchain but, in this case, independent. Since a central authority does not control the nodes on the blockchain, it is decentralized, hence the name– decentralized ledger technology.

Each node on the blockchain network possesses a copy of the entire ledger of the blockchain. Upon the validation of a transaction, the nodes in the network update their ledger to include the details of the concluded transaction.

With decentralization comes another challenge. How are the nodes in the network compelled to record the correct data on the ledger and how do all the nodes agree to this record? Since there is no single source of truth, a process is required to keep the nodes in check and ensure the accuracy of the recorded data. This process is known as the blockchain consensus mechanism.

It is important to note that the data recorded on the ledger is grouped in blocks. Once a particular block is filled up, the following transaction goes to the next block. Each block is linked to the preceding block through cryptography, hence the name– blockchain.

What is Blockchain Consensus Mechanism?

Blockchain consensus mechanism is a protocol used in decentralized ledger technologies to arrive at a unanimous agreement over transactions recorded on the ledger.

Another purpose of the blockchain consensus is to ensure the accuracy of the data recorded on the ledger. Usually, when a node validates a transaction, the rest of the nodes in the network attest to the validity before the transaction is finalized and added to the chain. This protocol prevents the manipulation of the data recorded on the blockchain.

The consensus mechanism is defined during blockchain development. There are different blockchain consensus mechanisms, as to be seen shortly.

Different Consensus Algorithms

There are quite a several consensus mechanisms deployed in different blockchain networks. However, proof-of-work is the first consensus ever created and the mechanism behind bitcoin. Other consensus mechanisms include but are not limited to proof-of-stake and proof-of-5ire.

The distinguishing factor across the consensus mechanisms is the method of node selection. Bitcoin's proof-of-work requires a node to get the correct answer to a mathematical puzzle to mine the next block. On the other hand, proof-of-stake checks for factors like staked amount while selecting a node to validate the next transaction. The nodes in the proof-of-work mechanism are regarded as miners, while those in the proof-of-stake mechanism are called validators.

Remember that irrespective of the consensus mechanism in play, after a node validates a transaction, it must be attested to by other nodes in the network before the transaction is finalized. If a node validates a fraudulent transaction, it will be discovered during attestation, and the offending node will then be punished.

Proof of Work

The PoW consensus mechanism requires miners to compete for the answer to a mathematical puzzle. The winner of the puzzle adds the next transaction to the chain, while others testify to its validity. Miners with enormous computing power stand a better chance of guessing the answer to the mathematical puzzle. Once the answer to the puzzle is found, the lucky node validates the next transaction and gets rewarded.

Proof of Stake

As already mentioned above, nodes in a proof-of-stake blockchain are called validators. To become a validator, a stipulated amount of the native cryptocurrency of the blockchain is locked up. This is regarded as staking. It serves as collateral for any misbehavior of the nodes, persuading the nodes to act honestly.

In PoS blockchains, nodes are selected by considering some weighting factors. One factor that comes into play is the staked amount of the nodes. Nodes with higher stakes stand a better chance of being selected as a validator. The staked amount, however, is not the only criterion considered during this selection. Another factor that comes into play when selecting validators is the node's age.

Conclusion

The consensus mechanism is a protocol blockchains use to verify and add new transactions to the blockchain ledger through node selection. It secures the blockchain from fraudulent transactions and malicious actors in the network.

07

Understanding the Basics of **Cryptocurrency** and **Blockchain** Wallets

07 —— Understanding the Basics of Cryptocurrency and Blockchain Wallets

Cryptocurrency may have gained unprecedented attention in the last few years. Yet, not many understand how the technology works. While many regard it as a viable alternative to fiat money or traditional currency, others see it as an investment opportunity to profit from. What are they exactly?

What are Cryptocurrencies?

Cryptocurrencies have assumed several definitions since bursting into the global scene. In their early days, different opinions existed on what they actually were. Cryptocurrencies were mostly considered as a shady innovation because people found them complex to understand. Thus, the technology was poorly received and heavily criticized. Nowadays, cryptocurrencies are easily defined or identified. But the most common definition is that they are digital assets.

However, cryptocurrencies are not just digital assets since anything can be a digital asset. For example, a domain name registered by an internet user is a digital asset. Cryptocurrencies are digital currencies, similar to fiat money— a currency in the traditional space. While cryptocurrencies exist only digitally, they are also a medium of exchange, like the traditional dollar ($) or Euros (€) or Pounds (£).

According to Coinbase, a cryptocurrency is typically decentralized digital money designed to be used over the internet. Cryptocurrency are decentralized because they operate on a permissionless platform known as blockchain. Because the blockchain is an independent technology, cryptocurrencies exist and are issued without the control and supervision of a centralized entity or third party. In addition, cryptocurrencies are stored and spent independently, without the interference of banks. They are stored in digital wallets.

History of Cryptocurrency

Although the history of cryptocurrencies dates back to the '90s, the first known digital currency is Bitcoin, founded in 2008. Satoshi Nakamoto (an unknown entity) is the brains behind Bitcoin. Satoshi proposed Bitcoin in the Bitcoin whitepaper as a viable and more efficient alternative to fiat money, controlled by the government and banks.

In the whitepaper, Satoshi pitched the idea of a decentralized currency that was not subject to government control and thus, was immune to challenges like inflation and excessive supply. At the time, Bitcoin was a timely alternative because the world had recovered from the 2008 financial crisis that crippled economies globally, causing inflation and financial depression. Thus, Satoshi considered Bitcoin as a "beacon of light" amid pitch darkness.

Since blockchain preceded cryptocurrencies, it became the appropriate platform for Bitcoin given its trustless architecture. Bitcoin relied on the technology as its strong edge, among other features like limited supply, faster transactions and decentralization. These features have endeared Bitcoin and thousands of other digital currencies to several cryptocurrency proponents today.

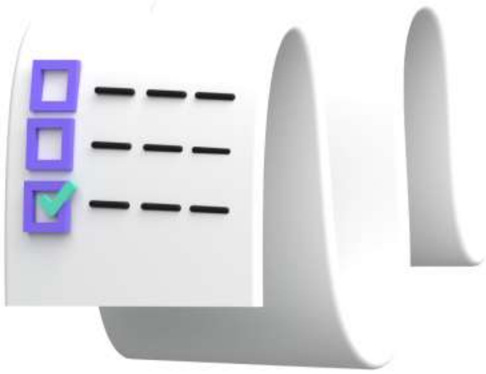
Cryptocurrency Wallets

Cryptocurrency wallets serve as storage facilities for digital currencies, similar to how fiat money is stored in banks. However, Cryptocurrency wallets are controlled by individuals, allowing stored cryptocurrencies to be spent at any instance. Cryptocurrency wallets contain public and private keys unique to each user.

A private key is likened to a password used to access a user's blockchain wallet. Thus, it must be protected at all costs. Loss of the private key could lead to a loss of digital assets. Meanwhile, a public address is used to send and receive cryptocurrencies. Public addresses can be likened to account numbers in traditional finance.

Summary

Cryptocurrencies continue to witness mass adoption, a proof that they have been widely accepted. Their unique features have been a driving force. Moreover, the investment opportunity they present is an endearing factor. However, investing in them comes with the risk of volatility— sudden increase or decrease in value.



08

Coins, Tokens, and **Smart Contracts**

08 —— Coins, Tokens, and Smart Contracts

The blockchain industry is new and emerging, so it is only normal to have confusing terms flying around. Countless blockchain jargon is thrown at users. The less tech-savvy ones grapple with the challenges of drawing a line across the new vocabularies.

Some of the most widely used terms are coin, token and smart contract. Despite their ubiquitous use across the cryptocurrency world, their exact meaning remains unclear, even to veteran users.

In this article, the myths surrounding these terms– coin, token and smart contract– will be untied. The clarity of terms will encourage more users to associate with the novel technology as it matures into household usage.

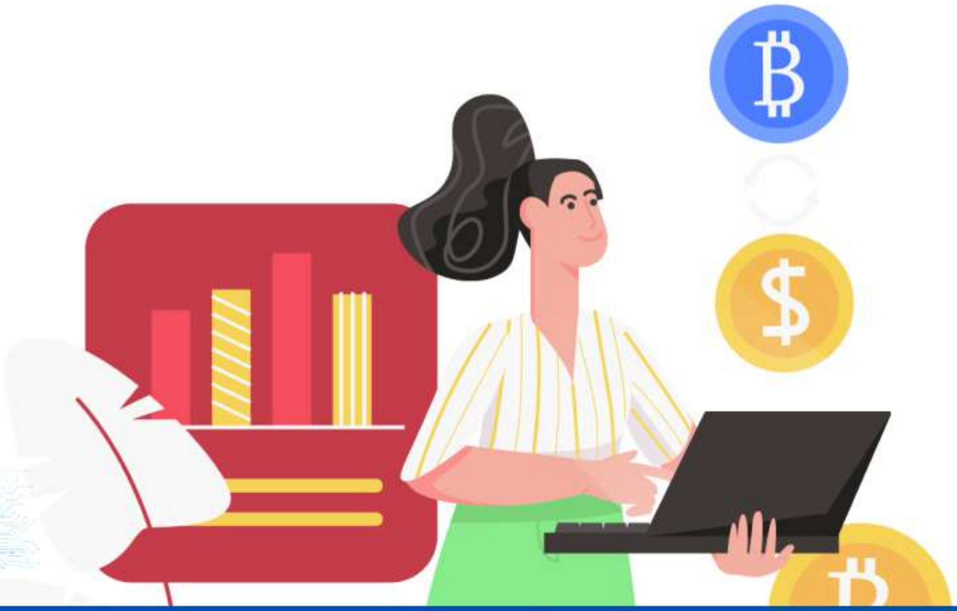
Coin and Token

These are arguably the most wrongly used terms in the entire crypto-sphere. The reason is not far-fetched. On the surface level, both concepts offer a similar meaning. More so, many crypto users are interested in solving their problems with the technology and not necessarily understanding the intricacies that bind it together.

Coins are cryptocurrencies that serve as the native currency of a blockchain ecosystem. They are used for paying the gas fees and staking and are accepted across all the applications within the ecosystem.

Each blockchain ecosystem has a native currency - the $ETH for Ethereum, $BTC for Bitcoin, and $BNB for Binance Smart Chain. These currencies are all coins because they are developed for a blockchain ecosystem.

Interestingly, blockchain ecosystems do not exist for themselves alone. They serve as the framework for developing blockchain applications.



The smaller applications inherit some of the features of their base blockchain. For example, a blockchain ecosystem with high-level security will confer such quality to applications hosted on top of it. This also depends on how they are deployed.

When a project is built on a blockchain ecosystem, it could have its own currency which would be regarded as a token. To put it into perspective, Polygon is a layer-2 protocol built on top of Ethereum, and its token is the $MATIC token. PancakeSwap is DEX on the Binance Smart Chain, and their token is $CAKE.

Technically, coins have more use cases compared to tokens. While coins are used to pay gas fees across the entire ecosystem, tokens are used only within the relevant project.

Smart Contracts

One unique application of blockchain technology is the smart contract. This feature facilitates the concept of transactional agreement between two or more persons without the interference of a third party.

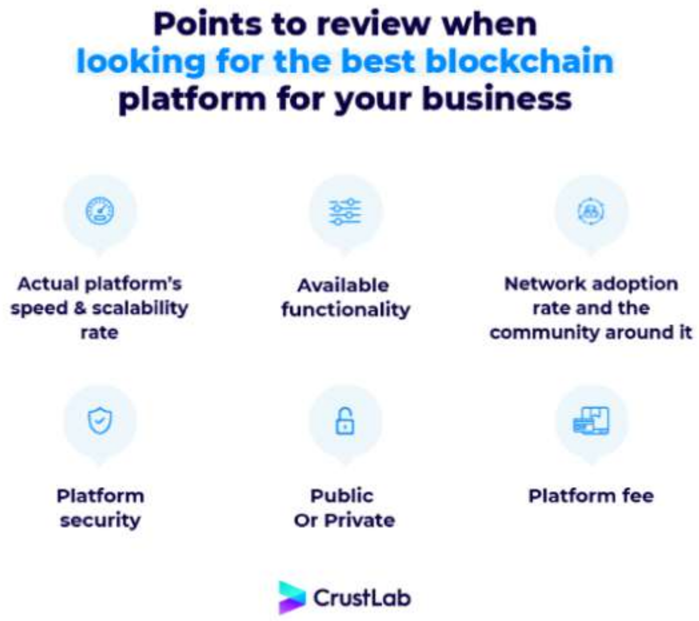
A smart contract refers to a set of programs that executes automatically when certain predefined conditions are met and validated. Using a smart contract, the involved parties do not have to go through a broker or even sign a chunk of paper-based agreements, as seen in traditional contract arrangements, which are tedious and time-consuming. More so, smart contracts are immutable and transparent because they are deployed on the blockchain.

With smart contracts, the terms of the agreement are represented by lines of code and deployed on the blockchain, making such contracts safer, more secure, and seamless.

To shed light on how smart contracts work, consider an imaginary yet possible application in the real estate sector. A property owner who decides to sell their real estate provides digital documents that confer ownership of the property. The smart contract makes the provision for the payment of the agreed price for the real estate and executes when the accurate amount is sent to the seller’s address, otherwise the contract is terminated. When the payment is validated, automatically the documents are sent to the buyer, conferring them with the ownership of the property.

Platform Selection for designing Blockchain Solutions

The rising blockchain technology has also led to a surge in the availability of platforms. Over 12,000 distinct digital currencies and at least a thousand blockchain networks are already available.
More than blockchain technology is needed, one must also decide which platform to employ. We made a list of things you should verify before joining the blockchain bandwagon to ease your research burden.



Points to review when looking for the best blockchain platform for your business

- Actual platform's speed & scalability rate
- Available functionality
- Network adoption rate and the community around it
- Platform security
- Public Or Private
- Platform fee

CrustLab

Actual Platform's Speed & Scalability Rate

Blockchain scalability indicates the maximum number of transactions per second (TPS) that a blockchain network can process. However, this varies from platform to platform; Ethereum (due to its smart contracts) can process 25 transactions per second, whereas Bitcoin can only process 7. In comparison, Litecoin can manage 56, Cardano 250, Ripple 1500, and Solana, even 29,000 transactions per second.

That depends on the information you want to feed into the network. More transactions per second (TPS) platforms are ideal for businesses creating payment software or a high-transaction gaming game. A platform with a relatively low TPS may be enough for a relatively basic data management system.

Availability Functionality

While every blockchain relies on the same underlying technology, each offer's benefits differ substantially. Let's look at some examples and contrast the Bitcoin, Ethereum, and Ripple cryptocurrencies. Bitcoin is primarily used as decentralised cyber money. Ethereum's primary purpose is to facilitate the development of smart contracts, which may be used to automate corporate operations and create decentralised applications. Similar to SWIFT, Ripple was developed as a means of facilitating inexpensive and efficient international money transfers.

Since they serve such distinct ends, it stands to reason that the method data is processed, the amount of time it takes, and the capabilities they may give would also vary greatly. That's why it's crucial to do some homework and figure out what kind of blockchain network could be best for your company and what features it should have.

Network Adoption Rate

The number of businesses adopting a blockchain network, the number of users, and the existence of a dedicated community are all factors to consider. The larger the group of people that use and care about the network, the more likely it is that you will be able to get the help you need if you run into any problems.
Moreover, needs and expectations change as time goes on. A platform with a large user base is more likely to get frequent updates that fix any known faults and prevent future vulnerabilities.

Platform Security

Blockchains are designed to be a safer default option for storing and exchanging information. However, this does not imply that the security of your data is irrelevant or that you can expect the same level of security across all platforms. Especially if your organisation deals with sensitive or private information, you should thoroughly investigate the safety measures provided by each platform.
You may secure the security of your money and data by investigating the platform's cryptography techniques, the network's verification of records, the platform's update frequency, and user verification procedures.

Public or Private

Private blockchains are popular with corporations because they provide administrators control over who may use the network, what information users can view, and how they can conduct transactions.

Consequently, an individual requires an invitation to join a private network. They will also need to be verified by the network administrator or by a set of rules defined by the administrators before being permitted access to the network.

In contrast, public blockchains prioritise user input and openness. When verifying transactions on a public network, anybody may join and have the same privileges as any other user. In addition, the software's source code is freely accessible to anybody who wants to utilise it. One advantage of public blockchains is that they protect users' privacy by requiring them to employ cryptographic codes known as public and private keys to verify their identities.

In other words, Private blockchains provide their owners more freedom than their public counterparts, allowing them to change or remove records as needed.

Enterprise blockchains are also far quicker than public blockchains. Private blockchains may process and verify transactions and activities far more rapidly than public blockchains since fewer people are needed to attain an agreement.

Several Nodes

Because they ensure the network's integrity and functionality, nodes play a crucial role in blockchain systems. Each node (shorthand for a computer or other networked device) provides that the blockchain operates according to to set protocols and standards. If there are a lot of nodes in the network, it's more difficult to tamper with the data in the blockchain or the node itself. However, the more extensive the network, the longer it takes for a transaction to be verified and for agreement to be reached among the nodes. Especially problematic are the hundreds of nodes that make up the most popular open public blockchain networks; they may be safe, but their performance leaves much to be desired.

Since only a small number of previously validated nodes need to accept each transaction, enterprise blockchains are often significantly more efficient. However, this speed comes at the expense of a little reduction in security. Here, you'll want to prioritize your needs; if transaction verification and storage speed are paramount, an enterprise network is the way to go. However, public blockchain solutions are superior if you value security above speed in the blockchain or want to employ a genuinely decentralized network.

Conclusion

By 2026, the worldwide blockchain market will have grown to $67.4 billion. Also, the fast development of blockchain technology suggests that many innovative applications will emerge in the commercial world. However, because there are several platforms to choose from, businesses must research their possibilities. Considering the potential versatility of blockchain systems, this is of paramount importance.

09

Case Study: Introducing Civil Identity on the **Blockchain**

09 —— Case Study: Introducing civil identity on the blockchain

The Challenge

The United Nations predicts that by 2050, 68% of people will live in urban areas. This mass influx of citizens stresses current governmental systems and processes. To ensure cities are well equipped to deal with the myriad of upcoming challenges, many cities are making steps towards becoming "smart" cities.

Zug, aka Crypto Valley, explored blockchain-based digital identities to improve access to digital government services while increasing efficiency, data security, and voting accessibility.

Streamlining Direct Democracy

In most democracies, citizens are called to vote for a few presidential, parliamentary or local elections. The representative they choose takes political decisions on their behalf. This is called an indirect democracy.

The Swiss have a direct democracy, which takes them to the ballot box around four times per year to vote on a myriad of issues relevant to their particular canton, e.g. smoking in restaurants, funding museums, and extending local bus routes. Although this is the most democratic government in modern times, it also creates a cumbersome, expensive, and time-consuming process.

The Enterprise Ethereum Solution

Zug leveraged uPort, a decentralized identity platform, to create the world's first live implementation of a self-sovereign government-issued identity project on the Ethereum blockchain, along with the city of Zug, the Institute for Financial Services Zug (IFZ) of the Lucerne University, along with integrator TI&M for the platform and Luxoft to implement voting. In the summer of 2017, they launched a pilot program to register resident IDs on the public Ethereum blockchain. After the pilot program, Zug officially launched the program in November 2017.

uPort's identity model returns identity ownership to the individual by allowing users to register their identity on Ethereum, send and request credentials, sign transactions, and securely manage keys and data on its open identity system.

How did it work?

Zug created their identity on the public Ethereum network, which gave them the power to sign and verify data. Access to the Zug city identity was delegated to the city clerk, who used their uPort identity with specific admin rights.

User experience

1. A Zug resident downloaded the uPort ID app from the Apple App Store and created an account.
2. The uPort app generated a unique private key representing the user's identity on their phone, which acted as the user's identity agent.
3. The resident had the opportunity to back up their private key, allowing them to recover access to their identity should they lose access to their phone. The resident gained complete control of their identity and all its associated data with this setup.
4. The resident visited Zug's website to register by scanning a QR code to interact with Zug's e-governmental platform for the first time.
5. The resident entered their date of birth and passport number on Zug's website. The request was cryptographically signed and sent to the city as a new Zug ID application request.
6. The resident was required to visit the City's Einwohnerkontrolle (citizen registration office) for an in-person verification of their details within 14 days.
7. Once confirmed, the city clerk issued them a verifiable credential that contained their Zug ID signed by the city's identity. Other organisations, public and private, could offer services to use the Zug ID in the user's uPort app.
8. Citizens gained access to several services by showing their ZUG ID in the user's uPort App, in this case, voting on an upcoming festival.

Goals Achieved

Secure digital interactions between people and governments:
350 registered citizens successfully created a digital ID, verified by uPort. 70 citizens participated in voting on the presence of fireworks at an upcoming festival. Users skipped the cumbersome login process, logged in with their uPort account, voted, and logged off without heading to a polling station. It was possible to verify who voted without reliance upon intermediaries or vote-counting infrastructure. The pilot demonstrated that user-controlled identities support the modernization of e-voting initiatives, which could save the city millions in people and productivity costs.

Next Steps:
In the future, citizens of Zug could use digital IDs to gain access to specific services around the city. For example, AirBie is a bike-sharing service that only allows access to their bikes through uPort decentralised identities. Users skip the tedious sign-up process and simply log in to their uPort-enabled Zug ID to gain free access to AirBie cryptobikes for up to 20 hours. At the time of this post, their bikes had been used more than 1,600 times by 90 users. The uPort decentralised ID is the first, secure step in enabling the creation of many "smart city" services, i.e. access to autonomous buses, luxury car-sharing apps, and checking out books from the library.

Ethical Challenges of Blockchain

The ethical consideration of blockchain as well as its applications is pivotal for its successful adoption. As blockchains find application throughout various domains and sectors, the requirement to have a comprehensive understanding of the potential impact of the technology as well as its moral and ethical dilemmas consistently emerges. Some of the ethical challenges of blockchain can be discussed in detail as follows:

Privacy and data ownership:
The decentralised structure of blockchain provides significant authority to the users or nodes for exercising control over their personal data. Yet, some issues such as who controls the data and exercises control over how data would be processed and stored are significant in blockchains and depict an ethical dilemma. Moreover, issues related to data subjects having the authority to access their private data, verifying the accuracy, and requesting correction are essential. Despite the decentralised nature of the operation, the ethical dilemma surrounding digital literacy and the practical ability to access the system also becomes significant in a blockchain context.

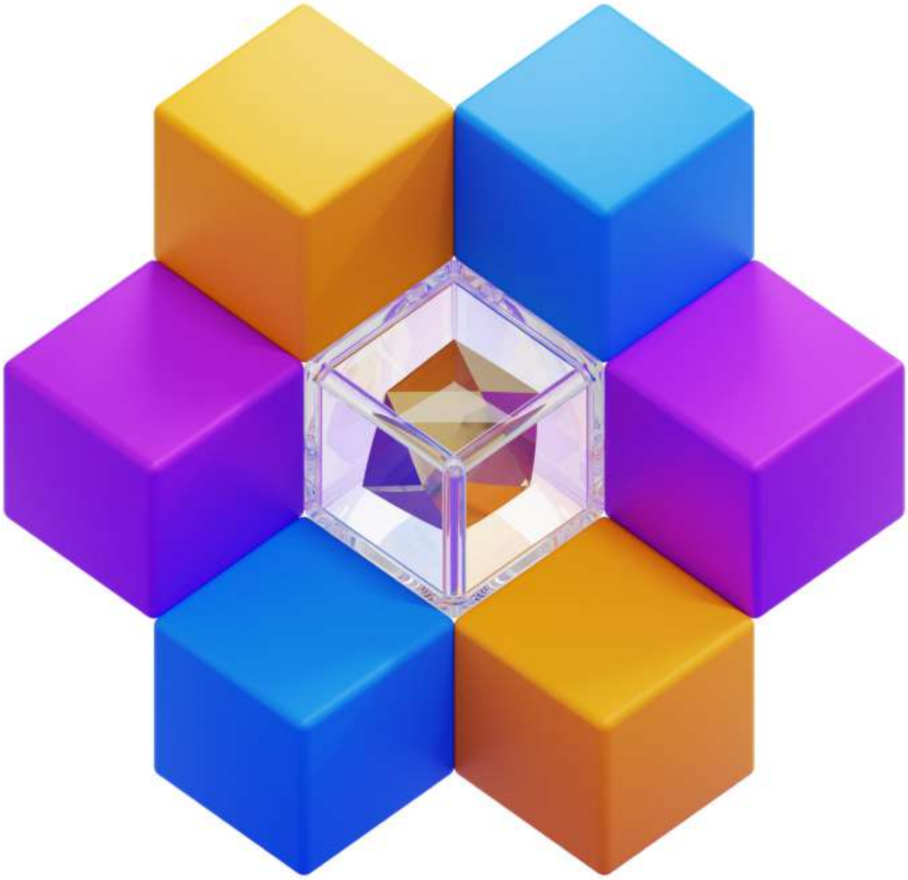
Accuracy:
When it comes to accuracy, personal data collected must be relevant, correct, and up to date. Although the primary blockchain consensus mechanism provides accuracy, the problem of zero-state still exists. Zero-state is a situation where the accuracy of initial items that predate the blockchain existence comes into question. For instance, consider an example of blockchain for land title registry. As a result of the inherent immutability, falsification of land titles that predate the blockchain could result in creating a version of the truth that is incorrect and could have negative consequences.

Fairness:
The decentralised structure as well as the mode of operation of the blockchain has been designed for enforcing inclusion and non-discrimination. Even though blockchains could result in ensuring democracy, they could also be used for consolidating and exerting power over individuals and their personal information. Blockchains can exacerbate current negative social dynamics. This could result in codifying disparities and biases.

Fairness:
The decentralised structure as well as the mode of operation of the blockchain has been designed for enforcing inclusion and non-discrimination. Even though blockchains could result in ensuring democracy, they could also be used for consolidating and exerting power over individuals and their personal information. Blockchains can exacerbate current negative social dynamics. This could result in codifying disparities and biases.

Closing Thought

It is only usual that a nascent technology introduces new sets of vocabulary. Blockchain is not only a complex innovation but also different from what internet users are used to. This makes the technology a bit challenging to grasp. However, it is not rocket science. As more users develop an interest in blockchain, the technology gradually unravels itself.



Keep Tinkering 😊