هيئة الاتصالات والفضاء والتقنية
Communications, Space & Technology Commission

Overview and Opportunities of Blockchain Technology

CST.GOV.SA

Table of Contents

List of Abbreviations

AI	Artificial Intelligence
BaaS	Blockchain-as-a-Service
BFSI	Banking, Financial Services and Insurance
BFT	Byzantine Fault Tolerance
CBDC	Central Bank Digital Currency
DAO	Decentralised Autonomous Organisations
dApps	Decentralised Applications
DeFi	Decentralised Finance
DLT	Distributed Ledger Technology
NFT	Non-Fungible Tokens
P2P	Peer-to-peer
PoA	Proof of Authority
PoS	Proof of Stake
PoW	Proof of Work
SSI	Self-Sovereign Identity
TPS	Transaction per second

1 Introduction

Blockchain technology is disrupting the economic and business models across different sectors, making it a potential technology to further KSA's digital transformation agenda. Its ability to deliver productivity gains in the existing value chains, deliver better customer experience, challenge revenue models, and unlock new markets differentiates itself from other emerging technologies. A study conducted by Gartner estimates a business value generation of US$3.1t worldwide with Blockchain adoption by 2030.[1]

The Communications, Space & Technology Commission (CST) aims to empower and develop the KSA's emerging technology market by contributing towards the creation of a robust ecosystem. To further this objective, a study of the Blockchain market globally and in the KSA was conducted.

The study intends to raise awareness of Blockchain technology and highlight the potential opportunities for Blockchain adoption globally and in the KSA context. It covers the following:

Technology overview	Blockchain Opportunities
• Blockchain Definition • Blockchain Components • Blockchain Technology Landscape	• Drivers of Blockchain Adoption • Blockchain Applications across Sectors • KSA Blockchain Opportunities

1 The CIO's Guide to Blockchain, https://www.gartner.com/smarterwithgartner/the-cios-guide-to-blockchain

2 Technology Overview

2.1 Blockchain Definition

Distributed Ledger Technology (DLT)

DLT refers to the technology used to enable the secure operation of a ledger that is distributed among multiple nodes. The nodes agree on and ensure consistency of ledger information using consensus.

Blockchain

Blockchain is one type of DLT that allows to record transactions in “blocks”, and each block is connected to the previous, forming a chain of blocks.

2.2 Blockchain Components

The Blockchain network, as shown in Figure 1 below, is mainly composed of connected **Nodes**, where each node stores a copy of the **Ledger** and **Smart Contracts**.

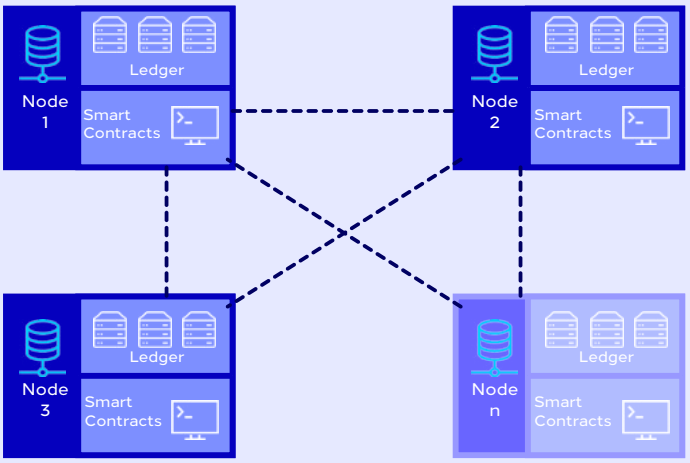

Figure 1: Blockchain Components

2.2.1 Ledger

Ledger in accounting refers to the registry of debit and credit transactions.

Likewise, in blockchain, the ledger includes transaction records. However, the difference is in

the way of storing such transactions.

A ledger in blockchain is defined as a chain of blocks. Each block includes 0 to n transactions based on the block size. The transaction initiation invokes smart contracts. Then, the block of transactions will be appended to the chain based on a specific consensus algorithm.

Blocks

Block content might differ slightly depending on the used platform. However, mainly blocks, as shown in Figure 2 below, contain Data and Hash of the previous block.

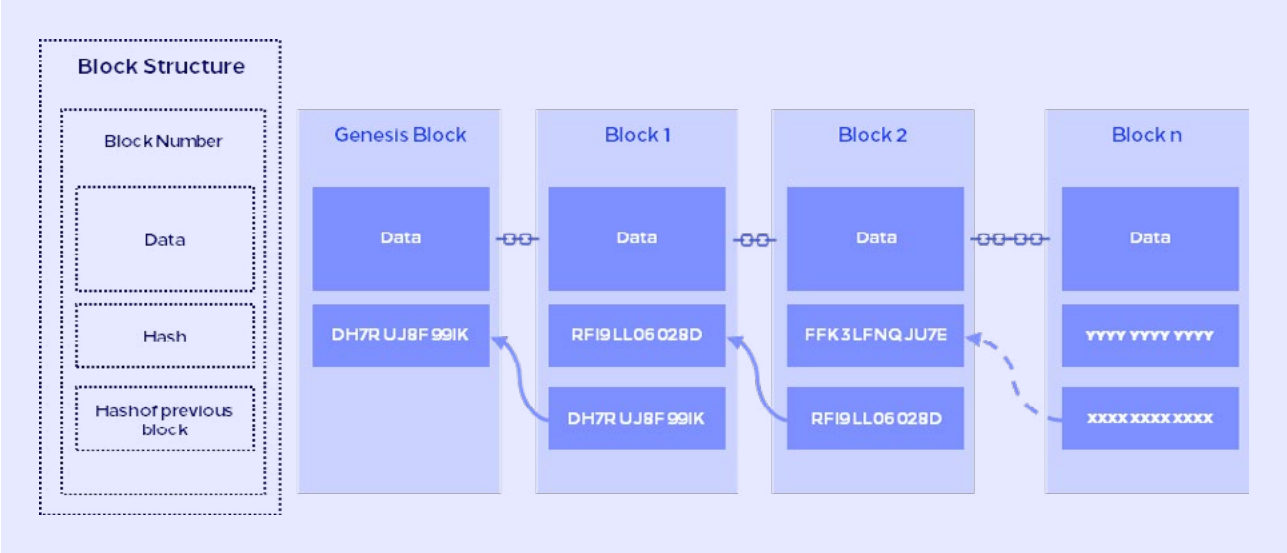

Figure 2: Chain of blocks in a Blockchain linked by a hash of the previous block

Data:

Typically including data about transactions such as creating a new asset or transferring an asset between nodes.[2] For example, in the case of currency, the transaction data might include the sender signature, recipient address and amount of transfer. In the case of perishable assets like medicine, transaction data can also include the medicine's temperature at the time of the transaction.

Hash:

Each block's content is hashed, and that hash will be included in the next block. If block content changes, the block hash will change, and thus the chain will be broken.

Linking each block to the previous block by referencing its cryptographic hash is key to the fact that a Blockchain is a chain of records that cannot be tampered with. Once a block is added and accepted in the network, it cannot be changed. Any required change to the data means another block should be added to reflect the change.

2 NISTIR 8202
https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf

Assets

Assets being tracked on blockchain refers to anything that can be owned or controlled by a stakeholder. Assets can be physical or digital.

Tokens are digital representations of assets in a Blockchain. Tokens are traded, exchanged, and dealt with digitally, ensuring secure ownership and transfer.

Tokens are categorised as:

Type	Description
Fungible Tokens	They have the same characteristics and value as a cryptocurrency
Non-Fungible Tokens (NFTs)	They are unique such as a unique artwork or real estate
Semi-Fungible Tokens (SFTs)	They are a blend of fungible and non-fungible as batches of the same type of goods. NFTs can be used to distinguish between batches. While Fungible Tokens can represent the goods within each batch.

Cryptocurrencies

Cryptocurrencies are a type of digital currency represented as fungible tokens whose transactions are validated and recorded in a distributed ledger. Cryptocurrencies utilise cryptography to secure transactions.

An example of cryptocurrency is Bitcoin, which is the native currency of the Bitcoin network.

Stablecoins

Stablecoins are a type of cryptocurrency designed to achieve stable prices. The following are different categories of the Stablecoins:

Custodial: Stablecoins backed by off-chain collateral assets, such as:

- Fiat currencies (i.e., USD)
- Commodities (i.e., Gold)
- Other cryptocurrencies (i.e., ETH)

Algorithmic: Stablecoins use algorithms and smart contracts to ensure stable value through managing the supply of coins.

It is noteworthy that stablecoins are not fully tested beyond experiments, and the implications of their full-scale mass adoption are not well researched.

2.2.2 Smart Contracts

Smart contracts are programs stored in blockchain whose inputs and outputs are verifiable by everyone, at any time, in the distributed ledger.

They can also be used to adjust or enforce the terms and conditions of business agreements automatically. Smart contract execution happens automatically after verifying that the conditions are met.

Smart contracts, for example, can be used to automate, compute, and schedule payments.

2.2.3 Nodes

Blockchain's trust mechanism is built on the fact that a single owner does not maintain the ledger; instead, it is maintained by many owners called 'nodes' or 'peers'.

Nodes refers to any device that participates in a Blockchain network by storing a copy of the ledger. Such device connects to the existing network of nodes, synchronises data, and remains in synchronisation in real-time.

Some nodes also participate in the validation and acceptance of the newly added blocks through a specific consensus mechanism.

Consensus mechanisms

The mechanism used by Blockchains to maintain the distributed agreement on each newly added block is called 'consensus'.

Following are some of the most popular consensus mechanisms:

- **Proof of Work (PoW)**
  In PoW consensus, nodes, known as miners, use computational power and compete against each other to create a new block. The newly created block will be then broadcasted to all nodes. If all transactions within the block are valid, the block will be accepted and the miner receives a reward in the blockchain's native currency.

- **Proof of Stake (PoS)**
  In PoS consensus, nodes commit a cryptocurrency stake (for example, 32 ETH in Ethereum Blockchain) to become a validator. Then, validators are chosen randomly to create a new block. PoS requires users to use reduced computational power because they don't need to mine blocks; instead, they only validate proposed blocks when elected.

- **Proof of Authority (PoA)**
  In PoA consensus, specific nodes have 'authority' to add or accept new blocks. PoA validators are not staking cryptocurrencies but are elected based on their identity and reputation. The criteria to accept the new block can vary depending on the configuration of the blockchain. PoA eliminates the need for excessive mining; therefore, it is an energy-efficient, performant and scalable consensus mechanism compared to PoW. However, to provide such benefits, it compromises the degree of decentralisation compared to PoS.

- **Practical Byzantine Fault Tolerance (PBFT)** [3]
  PBFT is a type of PoA algorithm that makes a network fault-tolerant by allowing consensus to be obtained only if the number of faulty nodes is less than one-third of the total nodes available in the network.

2.3 Blockchain Technology Landscape

On top of the core components, Blockchain solutions mainly span over three layers: Networks, Platforms and Applications.

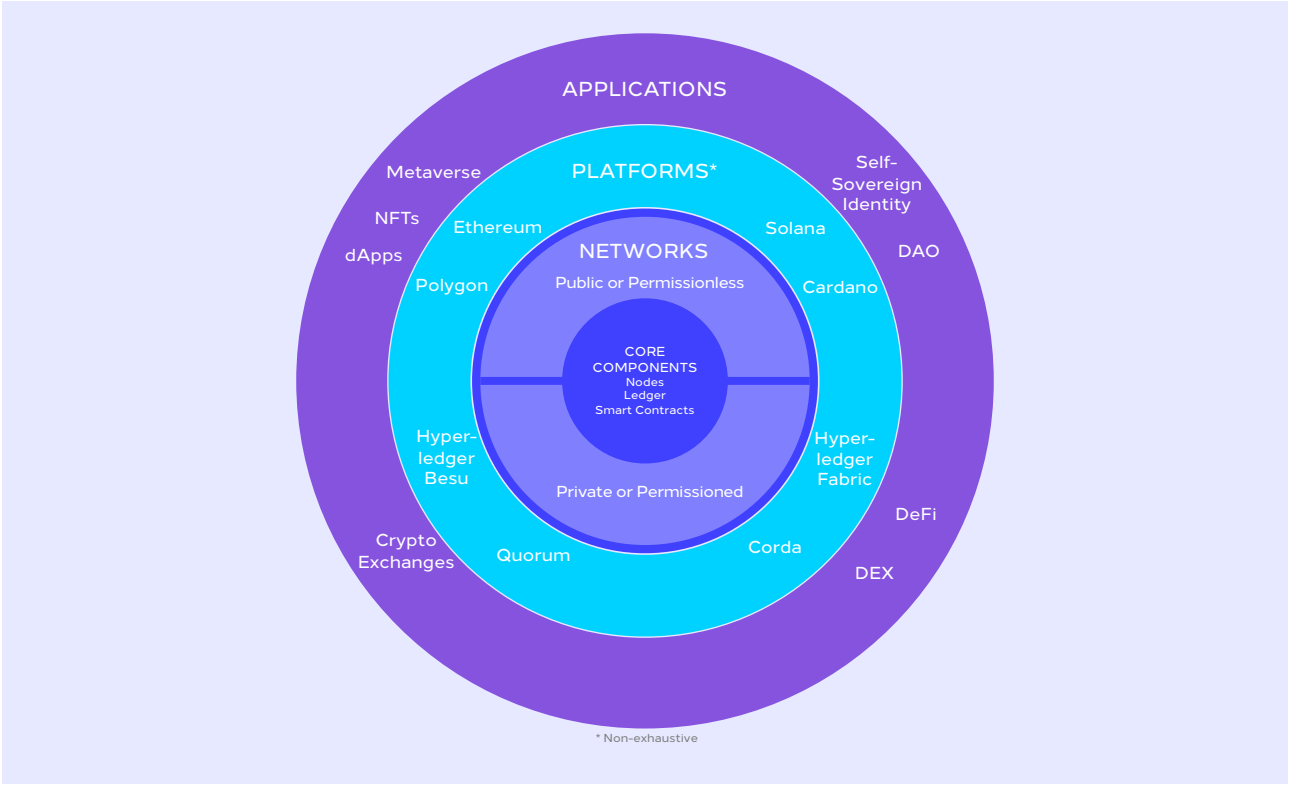

Figure 3: Blockchain Technology Landscape

2.3.1 Networks

As with many other technologies, networks form the fundamental layer including the infrastructure for running applications. Blockchain networks are formed by multiple nodes, where each node is connected to each other, creating a P2P network.

3 Byzantine Fault: Byzantine Fault refers to a problem were establishing consensus between army generals on whether to attack or retreat becomes difficult with each general not directly contacting other generals. The generals need to agree on a mechanism to reach consensus. This is typically done by agreeing on an algorithm which favours majority, but also must ensure there are no traitors who may jeopardise the consensus. Byzantine Fault Tolerance is the characteristic of solution or system which tolerates the set of problems similar to Byzantine Fault. In Blockchain, PoW, PoS and PBFT are approaches for BFT but PBFT aims to reach conseses even when there is a malicious behaviour by a small number of nodes.

Byzantine Fault Tolerance (BFT)

https://medium.com/loom-network/understanding-blockchain-fundamentals-part-1-byzantine-fault-tolerance-245f46fe8419

Blockchain networks can be categorised based on their accessibility and permission model into the following categories:

Public or Permissionless Blockchain Network

Public or Permissionless Blockchain Network

Public Blockchain networks are open to everyone to join the network and participate in the consensus process without requiring permission. Bitcoin and Ethereum are the most popular public Blockchain network examples.

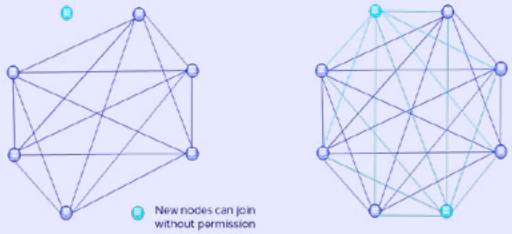

Figure 4: Public Blockchain

Private or Permissioned Blockchain Network

Private or Permissioned Blockchain Network

Private or Permissioned Blockchain networks can be owned by one or multiple entities that hold control over providing authority to new members either to only access the network or also to validate the transactions.

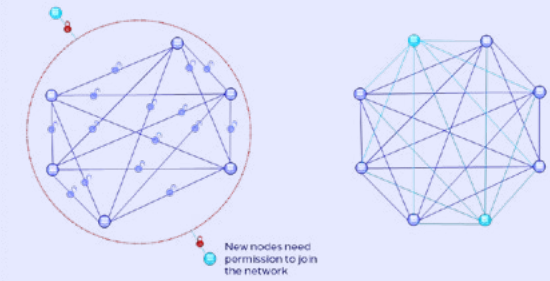

Figure 5: Private Blockchain

2.3.2 Platforms

This section compares some of the mostly adopted or fast-growing platforms as follows: Ethereum, Ethereum-forked Consensys Quorum, Ethereum scaling platform (Polygon), Hyperledger platforms (Besu and Fabric), Corda and Solana.

Platforms Comparison

Blockchain platforms vary in attributes and metrics. This table compares some of these platform's characteristics:

Platforms	Network Type	Consensus Mechanism
Ethereum	Public	PoS
Polygon	Public	PoS
Solana	Public	Proof of History
Consensys Quorum	Private	PoA: (IBFT, QBFT, Raft, and Clique)
Hyperledger Besu	Private	PoW, PoS and PoA: (IBFT, QBFT and Clique)
Hyperledger Fabric	Private	PoA (PBFT)
Corda	Private	Validity and Uniqueness

2.3.3 Enablers

Blockchain enablers include several technological components that can expand the capabilities of the technology, overcome limits or extend current functionalities.

Those components are used in the definition of business applications as:

- **Wallet:** Provide a means of identification and storage for cryptocurrency and tokens
- **Oracles:** Extend data on the blockchain with reliable data coming from outside
- **Scaling solutions:** Overcome scalability limits in blockchain
- **Zero-knowledge proof-based techniques:** Promote private transactions on public networks

Wallets

Wallets allow users to submit transactions on the blockchain (i.e. trade cryptocurrencies and tokens) by signing those with the wallet itself. Digital signatures, which are used to encrypt transactions, are computational schemes divided into two parts: the algorithm for creating the signature, which utilises a private key to sign the message, and an algorithm for verifying the signature, which uses the public key. Private keys are in the only control of the individuals and can be thought of as a password. In contrast, public keys work as a public address and can be tied up to decentralised identity and used to be identified by service providers.

The following diagram represents the relation between Private Key, Public Key and Wallet Address.

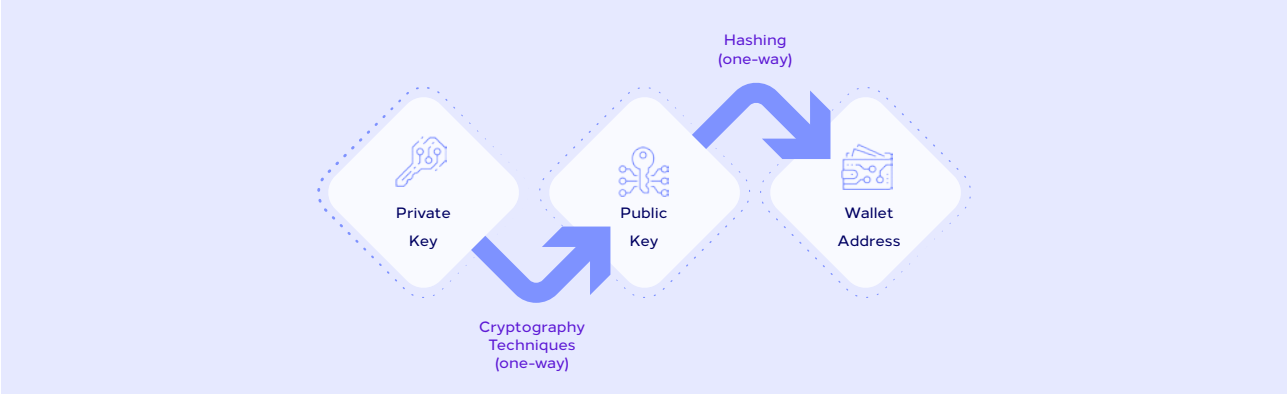

Figure 6: Use of cryptography and hashing for wallet address

Wallets can be in the form of a browser extension, a hardware wallet, a mobile app or a web wallet. Moreover, wallets can be of two types: Custodial, where a third party hold the private keys, and non-custodial, where users have total control of the assets in their wallets and their private keys.

Oracles

Oracles are a middleware between Blockchain networks and real-world external data (i.e., weather data).

Off-chain oracles query APIs and periodically publish response data as transactions on the blockchain, making the data reliable.[4]

For example, oracles can be used to register on-chain updates of a product's price to automate purchase via a smart contract when the price reaches a specific threshold.

There are several industry-leading implementations of oracles technology. An example is Chainlink, which provides decentralised oracles.

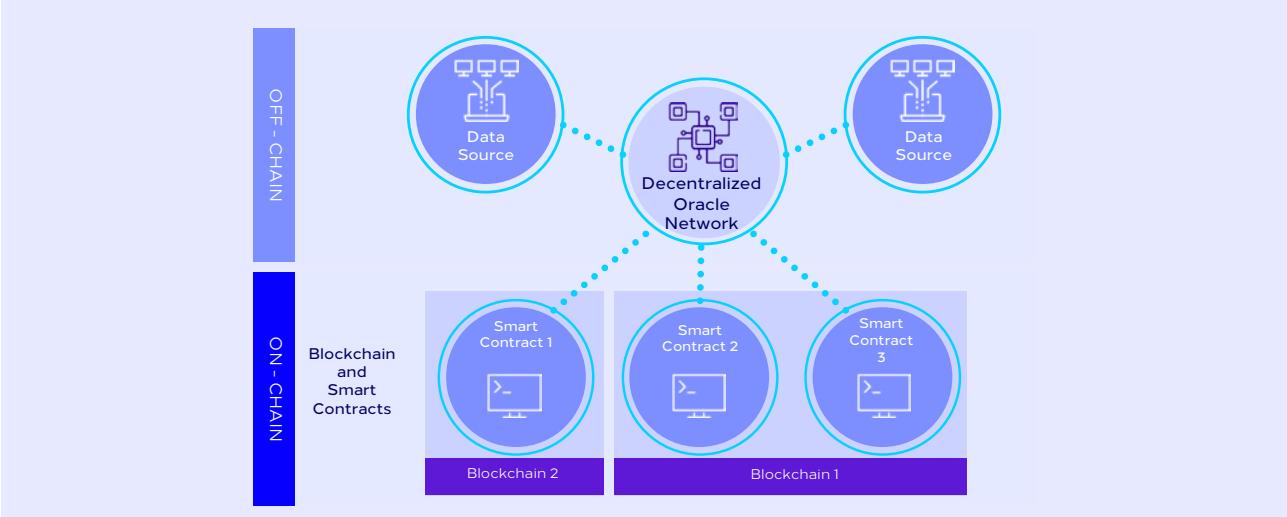

Figure 7: Decentralised Oracles

4 https://ethereum.org/en/developers/docs/oracles/

Scaling solutions

Blockchain scalability is mainly measured by the number of transactions per second (TPS). Initial versions of Blockchain technology implied a protocol layer, referred to as Layer 1, that defines the Blockchain rules. The scalability of Layer 1 Blockchains is challenging. Ethereum, as an example of Layer 1 Blockchains, processes 15 TPS on average, whereas VISA processes 1700 TPS. [5]

The scalability problem introduced the Blockchain Trilemma[6] , which means one of the three Blockchain features (security, decentralization, and scalability) must be sacrificed in order to increase the other two.

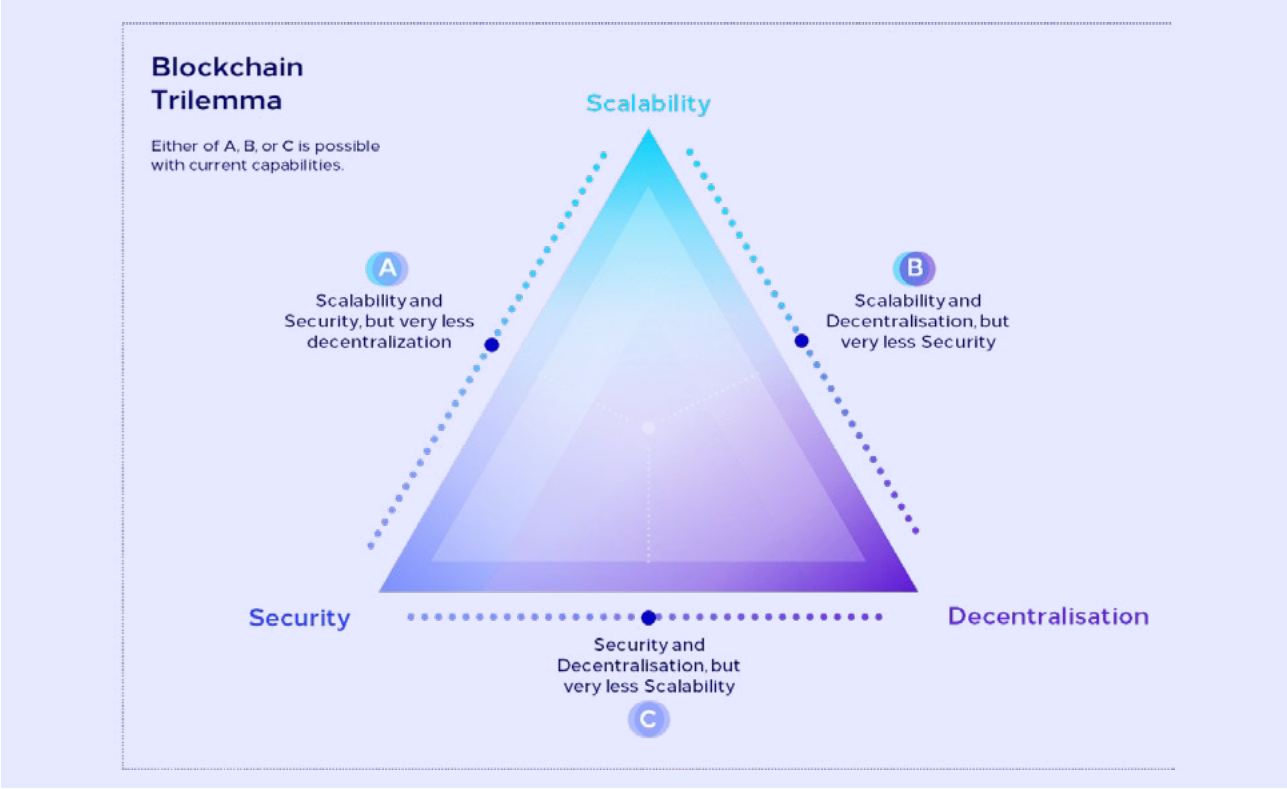

Figure 8: Blockchain Trilemma

The above figure shows a visualisation of the trilemma that emphasises the challenge where only position A, B or C can be achieved. For example, with position B, the blockchain can have scalability and decentralisation but will have to compromise on security. This constraint is due to blockchain design and computing capabilities, which engineers are attempting to solve.

While security and decentralisation are native characteristics which define the blockchains, the majority of the attempts to solve the trilemma are about finding ways to make

5 Yadav, Jyoti & Shevkar, Ranjana. (2021). Performance-Based Analysis of Blockchain Scalability Metric. Tehnički glasnik. 15. 133-142. 10.31803/tg-20210205103310.
Researchgate | Performance-Based Analysis of Blockchain Scalability Metric | March 2021
https://www.researchgate.net/publication/349846413_Performance-Based_Analysis_of_Blockchain_Scalability_Metric

6 The Scalability Trilemma, https://vitalik.ca/general/2021/04/07/sharding.html

blockchain technology more scalable.

Scalability on Layer 1 Blockchains can be improved by changing the protocol rules to increase transaction speed. PoS consensus, for example, is a scaling solution for Layer 1 Blockchains.

Whereas layer 2 refers to a secondary protocol or solution built on top of Layer 1 that aims to improve scaling without compromising on security or decentralisation.

One example of Layer 2 solutions is Rollups, where multiple transactions are bundled into one transaction on Layer 1.

Layer 2 enables faster transaction processing, which contributes to delivering innovation and attracting investment to make blockchain viable for business solutions.

Zero-knowledge proofs (ZKPs)

ZKPs are cryptographic techniques that enable a prover to prove knowing a statement without disclosing information about the statement to a verifier. ZKPs are used as a solution to maintain transaction privacy in a public Blockchain.

One type of rollups scaling solution is zero-knowledge rollups (ZK-rollups) which uses ZKPs to validate off-chain transactions before bundling them to Layer 1.

One relevant example is Nightfall, developed by Polygon and EY, which combines ZKPs with a 'ZK-Optimistic Rollup,' which reduces ERC-20 token transfer fees by up to 86%. Nightfall 3 consolidates ZKP transactions into rollups based on the assumption that transactions are valid unless proven otherwise. The mechanism eliminates the verification process by all participants, thereby aiding in an enormous improvement in transaction efficiency and reducing gas fees. Users are incentivised to challenge bad blocks to ensure that only correctly formed Layer 2 blocks are included in the blockchain.

2.3.4 Applications

This section sheds light on fast-growing Blockchain application types, including:

- Decentralised Apps (dApps)
- Decentralised Finance (DeFi)
- Decentralised Exchanges (DEXs)
- Decentralised Autonomous Organisations (DAOs)
- Asset tokenisation through NFTs
- Metaverse
- Self-Sovereign Identity (SSI)

2.3.4.1 dApps

dApps are applications whose key business logic resides on the blockchain, specifically on

the smart contracts, and is executed directly by the user client through its blockchain wallet. Major Blockchain platforms provide featured dApps and a marketplace for dApps built on their platform.

The decentralised nature of the applications also ensures the code is immutable and highly available since code exists on multiple nodes. It offers a disruptive way of developing and deploying applications over the traditional server, cloud or serverless models. Some of the challenges linked to application maintenance and performance degradation due to rogue code are still to be overcome.

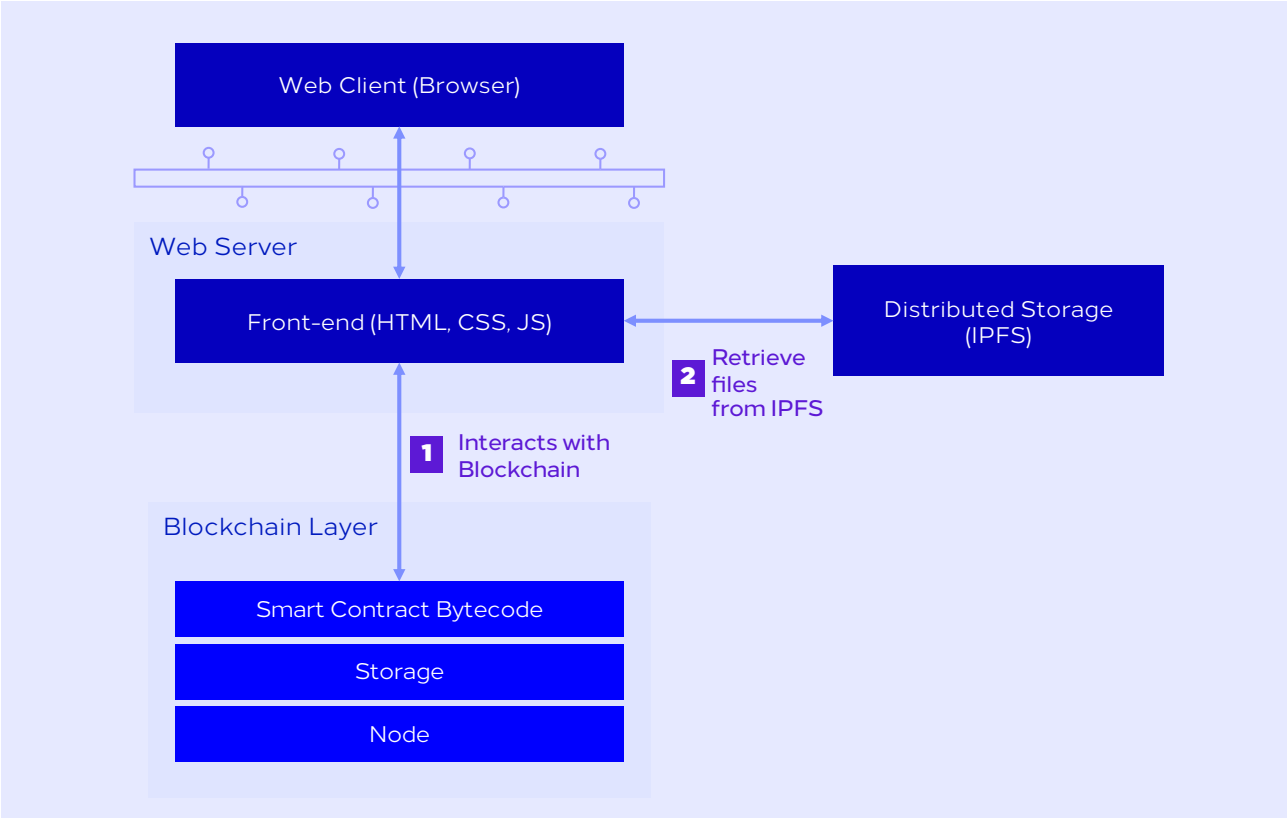

Figure 9: dApps Architecture

2.3.4.2 DeFi

Decentralised finance (DeFi) is one type of dApps specialised for financial services such as trading, payments and lending. The following diagram represents a conceptual architecture of the DeFi stack, starting from the assets through use cases protocols to applications and then to platforms aggregating multiple applications.

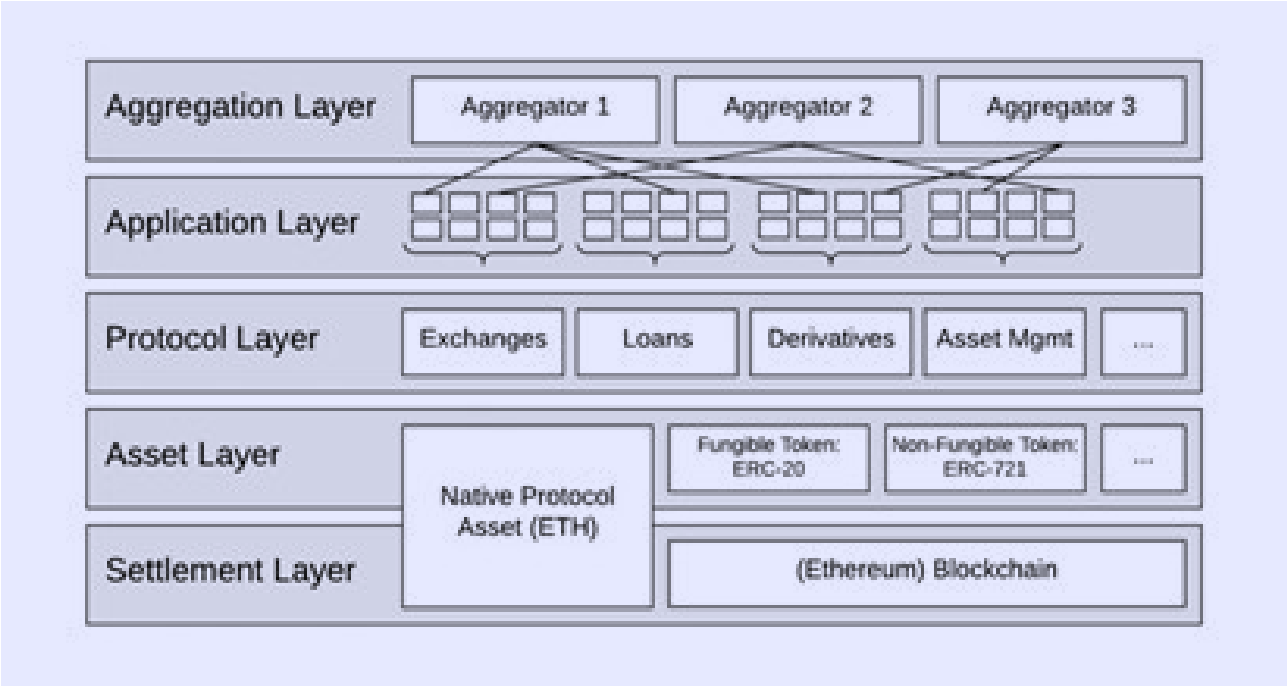

Figure 10: DeFi Stack[7]
(Image Credit: ResearchGate.net | Fabian Schar)

2.3.4.3 Characteristics of DeFi:

- DeFi can have similar instruments as traditional financial services in a decentralised network removing the intermediation of a central authority.
- DeFi systems operate with minimal trust as protocols are implemented using smart contracts. Such protocols dictate how transactions are executed.
- Owners of tokenised assets are in total control over the ownership of their assets and can cancel transactions at will. Intermediaries and third parties can neither take temporal ownership nor modify the asset.

2.3.4.4 DEXs

After crypto invention, multiple marketplaces exist for crypto exchange and trade. Initially, most crypto trades are executed via centralised exchanges. However, the risk of a single point of attack arises with centralised exchanges. DEXs try to mitigate that risk by enabling direct transactions between traders without dependency on a centralised exchange operator.

DEXs utilise smart contracts to secure transactions. DEX marketplaces expand beyond trading crypto to tokens like NFTs. DEX can be considered as an application of DeFi.

2.3.4.5 DAOs

DAOs are organisations on the internet, organised by rules encoded as smart contracts and

7 Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets - Scientific Figure on ResearchGate (2021), https://www.researchgate.net/figure/The-Decentralized-Finance-DeFi-Stack_fig4_340061422

governed by organisation owners instead of central leadership. DAOs can be considered as a type of dApps where the application is for organisation, and it is fully autonomous.

DAO governance and rules changing are conducted by voting using tokens. Only owners of governance tokens can participate in the voting.

Therefore, it is noteworthy that DAO is not a business model or a type of organisation but a concept that can be used for automated, decentralised and autonomous governance of anything.

A DAO, for example, can be used for charities, crowd-funding, venture-capital funding and asset management.

> DAO is not a technology, business model or a particular type of organisation but a concept that can be used for automated, decentralised and autonomous governance of anything.

2.3.4.6 Asset tokenisation through NFTs

Managing unique real-world things is a natural fit for blockchain, considering its ability to ensure immutability, auditability, anonymity, and ownership.

Use cases for NFTs include:

- Attributes represented by NFTs can be used for incorporating unique serial numbers and more dynamic information such as location, temperature, and size. For inventory management purposes, tokens can also be combined with other tokens to represent an assembled product with multiple parts.
- In software licensing, alphanumeric keys represent software licenses. In the future, NFTs will represent keys and will be held in digital wallets and serve as the key providing access to the software resource.
- Property and land represented as NFTs allow for its safe and secure trade.
- Organisations can use NFTs for access control and identity management.
- Occupation-specific credentials such as medical licenses, law degrees and other certifications are unique to an individual and can be issued, maintained, and tracked as NFTs on Blockchain networks.

> Managing unique real-world things is a natural fit for blockchain, considering its ability to ensure immutability, auditability, anonymity, and ownership.

2.3.4.7 Metaverse

The metaverse enables people to interact with each other in a virtual reality space. Blockchain forms the foundation layer for metaverse through using NFTs and dApps. Through the metaverse, individuals and organisations can create and trade digital assets such as virtual lands and tickets for virtual events.

Metaverses such as Decenterland are governed by the users through the use of DAOs.[8] Another example of Metaverse is NIKELAND which is created by NIKE and inspired by the company's real-world buildings. [9]

2.3.4.8 Self-Sovereign Identity

Self-sovereign identity (SSI) is an approach in which individuals maintain control and access over their identity and its information.

Blockchain empowers SSIs by having a trusted distributed registry between ID issuer, holder and verifier.

Using SSI systems, issuers can issue verifiable credentials of their identities. However, credentials may represent other claims about the holder, such as driving licenses and certificates. ID holders can manage their credentials through digital wallets. As a result, ID holders can show their verifiable credentials to prove their identities, while verifiers can ensure their identity is certified by the related issuer using blockchain. This effectively transfers the verifier's faith in the issuer to the credential holder achieving disintermediation.

> Self-Sovereign identity puts the user at the centre by eliminating intermediaries to access services, thus replicating the physical world experience and adding a layer of trust on interactions.

2.3.5 Blockchain Ecosystem

Initially, the Blockchain ecosystem was mostly comprised of market players offering Bitcoin mining and trading solutions. Following the release of Ethereum and the introduction of smart contracts, often known as Blockchain 2.0, the Blockchain ecosystem has blossomed with market players spanning technology, sectors, and use-cases.

Following are examples of the ecosystem participants categorised based on the services they provide:

Service Category	Service Description
Consulting	Providing access to expertise to either consult or build a strategy for Blockchain adoption.
Blockchain Solutions	Offering Blockchain solutions for specific use cases.
Blockchain Development	Building custom Blockchain solutions.
Blockchain Platforms	Offering frameworks and platforms to build Blockchain solutions and applications.

8 Decenterland, https://decentraland.org/

9 NIKELAND, https://www.roblox.com/nikeland

Development Tools	Providing tools for developers to develop Blockchain applications. These include: - Blockchain as a service - APIs - Security - Computing resources - Off-chain storage resources

3 Blockchain Opportunities

3.1 Introduction

Blockchain's ability to increase transparency, enable fraud resistance and enhance privacy unleashes different opportunities among different industries. The need for financial inclusion in developed and developing economies, the surge of NFTs for content creators, the increased interest in cryptocurrencies, and managing renewable energy are also directed toward more adoption of blockchain.

Blockchain has the power to make a positive impact on business, society, the economy and the environment, which would lead to an increase in the adoption of blockchain.

The World Economic Forum (WEF) expects an increase in the trade volume of up to US$1t with the adoption of blockchain and related technologies. WEF also states the need to remove barriers to adopting the technology and streamlining trade processes to witness the increased trade volume.[10]

According to Gartner, the business value generated by blockchain would be around US$176b by 2025 and US$3.1t by 2030.[11] Blockchain is bringing in new opportunities for players in the market.

This section highlights key drivers of adoption and success stories and then explores blockchain-related developments in KSA and the future potential of blockchain within the nation.

3.2 Drivers of Blockchain Adoption

The key factors influencing the global adoption of Blockchain technology across sectors are:

Increased Transparency

Having one ledger distributed among business network stakeholders, including real-time information about product transactions, ultimately increase transparency. And given the immutability nature of blockchain, stakeholders can view the full history of the product lifecycle and ensure ledger records are resistant to corruption.

For example, Walmart used a Blockchain-based supply chain to trace foodborne illnesses effectively. The technology enabled the retailer to transparently trace the product lifecycle in 2.2 seconds instead of 7 days.[12]

10 Blockchain set to increase global trade by 1million, Weforum (2018), https://www.weforum.org/agenda/2018/09/blockchain-set-to-increase-global-trade-by-1-trillion/

11 Digital Disruption Profile, Gartner (2018), https://www.gartner.com/en/doc/3855708-digital-disruption-profile-block-chains-radical-promise-spans-business-and-society

12 Walmart and Sam's Club to Require Real-Time, End-to-End Food Traceability with Blockchain, https://corporate.walmart.com/media-library/document/leafy-greens-on-blockchain-press-release/_proxyDocument?id=00000166-0c4c-d96e-a3ff-8f7c09b50001

Fraud Resistance

Blockchain eliminates the requirement of trusted third parties (TTP) and relies on trustless integrity. This characteristic is instrumental in minimising the potential of fraud done by central authorities and rogue players. Therefore, organisations or entities that are part of an ecosystem and conduct business with each other are motivated to trust Blockchain technology instead of TTPs or central authority.

For example, using blockchain in tax fraud detection and prevention targets to reduce fraud by ~30%.[13]

Increased Data Privacy Protection

Governments and rights authorities have increased demands to protect individuals' private data. Developments in Blockchain capabilities provide a mechanism to rely on the integrity of the information while maintaining individuals' privacy. Capabilities include ZKPs, pseudonym wallet addresses and channel subnets in Fabric. Such capabilities drive wider adoption of blockchain with adherence to the principles of data privacy protection.[14]

3.3 Blockchain Applications Across Sectors

Beyond the leading use cases in the top three market sectors, this section explores two success stories in Government and Media & Entertainment.

3.3.1 Government

Blockchain use cases for the Government sector include SSI, land registry, CBDC and patent protection. Many countries also are currently focusing on creating a national Blockchain network. These types of networks will provide a trusted ecosystem for cross-sector organisations to work safely and develop Blockchain-based applications with transparency.

European Blockchain Services Infrastructure (EBSI) [15]

Digitising documents can raise the risk of fraud and increase the difficulty of verifying documents' authenticity. Blockchain-based applications address those challenges by providing proof of authenticity of a document. Blockchain enables tamper-proof storage of document data and secure access to the documents, and elimination of third-party verification. Thus, blockchain contributes to the reduction of time and cost of verification.

Document verification is one of the applications or use cases supported by EBSI, a Blockchain network of distributed nodes across Europe to deliver cross-border services for public administrations.

Through EBSI Blockchain, a trusted entity can issue a digitally verifiable document. A

13 Two practical cases of blockchain for tax compliance, https://www.pwc.nl/nl/tax/assets/documents/pwc-two-practical-cases-of-blockchain-for-tax-compliance.pdf

14 How is Blockchain verifiable by the public and yet anonymous https://consensys.net/blog/enterprise-blockchain/how-is-blockchain-verifiable-by-the-public-and-yet-anonymous/

15 EBSI https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI

competent authority confirms and records verification on the blockchain. The end-user, be it a citizen or a business, can then can share a representation of the verified document when needed.

Unified Inspection Network (Ittisaq) [16]

A national initiative by Elm and Riyadh Municipality aims to build a secure and decentralised blockchain network dedicated to connecting all regulators conducting inspection activities, to achieve the goals of future integration of the oversight engagements and raise the efficiency of work which is in the interest of all parties.

3.3.2 Media & Entertainment

The media & entertainment sector can unleash Blockchain potential in preventing fraud in content and advertising, removing intermediaries between consumers and creators and automating royalty payments.

Microsoft XBOX Royalty Processing [17]

The traditional method for protecting and managing royalty processing at Microsoft Xbox was inefficient, taking 45 days to obtain verified financial information about royalties earned. The challenge is bigger for game publishers, particularly those with tiny firms and little resources.

Microsoft created a Blockchain-based solution to reduce the manual labour and operational hours associated with processing royalties for publishers by automating the process.

The legal terms of royalty contracts were encoded as smart contracts in the Blockchain network to automate the process. The system's automation sped up the process, decreased effort, and gave participants more transparency while retaining a high level of secrecy and confidentiality between Microsoft and the game publisher. A user-centric interface for game makers adds a simple, well-designed interaction layer to the royalty distribution system.

After using smart contracts to accurately and transparently process royalties for Microsoft Xbox's partners, the next step was to safely and transparently share the information with them in near real-time, reducing royalties access from 45 days to 4 minutes.

When customers buy Xbox games, digital material or other items, the smart contracts automatically apply the contractual logic and determine the royalty. Then royalty data is recorded in the distributed ledger that is secure and confidential.

Using Blockchain for Royalty improves processing time by 99%. It provides game publishers with near-real-time royalty statements, reduces operational effort by 40%, and removes the need for reconciliation.

16 IBM and Ilm to implement Riyadh municipality blockchain roadmap (2018), https://www.unlock-bc.com/news/2018-07-11/ibm-and-elm-to-implement-riyadh-municipalitys-blockchain-roadmap

17 Microsoft XBOX Royalty Processing https://www.ey.com/en_gl/consulting/how-blockchain-helped-a-gaming-platform-become-a-game-changer

3.4 KSA Blockchain Opportunities

Interest in the adoption of Blockchain technology in the region began in 2016. It started with the UAE, Bahrain, and KSA, interest in evolving the financial and government services sectors. KSA has remained focused since then through continuous research and examining current and future applications of Blockchain systems for government, financial, and commercial services. Though blockchain is evolving in due course of time, KSA is making significant efforts to encourage adoption in key industry sectors.

3.4.1 Less Cash-Dependent Society

SAMA, the Saudi Central Bank, is testing Blockchain technology for money transactions as it aims to boost e-payments to 70% of total transactions by 2030. Advancements in this initiative provide an opportunity for ecosystem players to provide services and build Blockchain applications for banks and other entities dealing in currency exchange. As part of the effort to become a less cash-dependent society, SAMA partnered with Ripple to help KSA banks to improve their payment infrastructure and enable banks to use Ripple's xCurrent Blockchain technology for instant cross-border payments. [18]

3.4.2 Digitisation in Booming Real-Estate Market

Blockchain-based smart contracts could play a significant role in KSA's real estate sector, where multiple mega projects like NEOM, Qiddiya, Amaala etc., are being developed. Smart contracts can automate tasks that would otherwise consume hours of paperwork and processing. It can also define the rules and penalties around an agreement and help exchange money or property in a traceable and transparent way while cutting costs, speeding up transactions, and improving the trust among the parties.

3.4.3 Blockchain Academy for Talent Development

BSV blockchain association has partnered with the Saudi Digital Academy (SDA) to launch a BSV Blockchain Academy. The SDA was established by the Ministry of Communications and Information Technology (MCIT) to develop the digital capabilities of Saudi youth. The blockchain academy will provide Blockchain learning and development resources for various audiences. This initiative will help businesses and start-ups to leverage talent, and create an opportunity for individuals to further their careers.[19]

3.5 Blockchain Enablement in KSA

CST is keen to support entrepreneurs and enterprises that would like to play a role in building the Blockchain ecosystem of the KSA. The rapid transformation of the nation will be possible only with the active participation of all ecosystem players.

The fast-paced adoption of Blockchain technology in the KSA will require collaboration between market players, leveraging their capabilities to arrive at solutions driven by market

18 https://www.arabnews.com/node/1954151/business-economy

19 http://www.tradearabia.com/news/IT_392727.html

needs. The initiatives and investments of KSA emphasise the technology-driven development to be the country's focus for the next decade and more. There are countless opportunities for market players to seize and grow their market share through expansion and diversification.

CST aims to actively contribute to the prosperity of KSA's technology sector by accelerating the uptake of blockchain and other emerging technologies. Accordingly, it has taken the following steps to develop a robust Blockchain ecosystem in KSA.

- Developing guidelines for blockchain
- Publications on the KSA Blockchain market
- Organise and conduct events and workshops with leaders in Blockchain technologies, government, academics and local Blockchain innovators to discuss possibilities in KSA's Blockchain market.

CST encourages businesses that have questions, concerns and comments – or that want to explore the possibilities of Blockchain technology – to reach us at

info@cst.gov.sa.

هيئة الاتصالات والفضاء والتقنية
Communications, Space &
Technology Commission