Issues in Information Systems
Volume 23, Issue 4, pp. 192-203, 2022

DOI: https://doi.org/10.48009/4_iis_2022_117

Blockchain fundamentals and classifications - A pathway to the moon

James J. Lee, Ph.D., *Seattle University, leej@seattleu.edu*
Swathi Bangalore Madhuranath, *Seattle University, sbangaloremadhuranat@seattleu.edu*

Abstract

Since the first successful cryptocurrency, bitcoin, appeared in 2009, more than 18,000 cryptocurrencies are available now, providing innovative consensus mechanisms with various use cases. With the world wide public ledger nature, it is truly following the paths of the Internet and world wide web technologies in the financial sectors. As it is as idealistic as a pathway to the Moon, this study examines the fundamentals of blockchain in hyperledger, mining, and consensus mechanisms. The paper proposed two findings. First, four generations of blockchain are discussed with the advancement in innovations. Second, the classifications of blockchain are proposed in terms of participant's openness (public vs private) and network's control scheme (decentralized vs centralized).

Keywords: blockchain, cryptocurrencies, consensus mechanism, cryptocurrency generations, blockchain classifications

Introduction

Cryptocurrencies have recently played interesting roles in early 2022 on both sides of the crisis triggered by Russia's invasion of Ukraine. Their capacity to traverse borders without respect for laws or regulations is assisting Ukrainian refugees in moving money out of the nation, but it may also give a method for Russian elites to avoid punishing economic sanctions. The cryptocurrency was meant to be Ukraine's future launchpad. Instead, it is proving to be a vital lifeline in a war-torn country. Ukraine has generated more than $63 million in donations since Russia's invasion on February 24th (2022), ranging across more than 120,000 crypto assets including Bitcoin, Ether, Polkadot, Solana, Dogecoin, Tether, and others. These monies have been used to assist humanitarian organizations in providing relief around the nation, as well as to purchase supplies for troops like food, clothing, and bullet-proof vests (Adria 2021).

Over the course of its brief life the cryptocurrency market has progressed intermittently and at an unprecedented rate since the release of the first successful cryptocurrency, bitcoin, in January 2009. However, cryptocurrencies are recently gaining attention of both investors and technology enthusiasts for a variety of reasons, including: (i) they facilitate transactions by lowering costs and time-spending; (ii) they are based on peer-to-peer structure, which eliminates intermediaries and makes the cryptocurrency-holder the account's governor; (iii) they provide privacy in transactions, which may be important for those concerned about account theft; and (iv) they have begun to be used as a medium of exchange, such that we can buy a cup of coffee with our coins. (v) Finally, they offer a relatively higher return on investment (Adam, B 2019).

This study starts with the brief history of Bitcoin Blockchain, discussing the concepts of blockchain as hyperledger which serves as a world wide spreadsheet. The section also discusses the fundamental

operations of blockchain in general, followed by the meaning of mining in blockchain. The following section provides overviews of cryptocurrencies in competition. The heart of cryptocurrencies is a consensus mechanism which underlines the total energies consumption by mining, the level of security/privacy, and transaction confirmation operations. The representative consensus mechanisms in public and private blockchains are introduced. In the last two sections, this paper proposed two findings. Initially, four generations of blockchain are discussed with the advancement in innovations. Lastly, the classifications of blockchain are proposed in terms of participant's openness (public vs private) and network's control scheme (decentralized vs centralized).

Literature Review - Brief History of Bitcoin Blockchain

Although the concept of electronic currency dates back to the late 1980s, Bitcoin, which was launched in 2009 by a pseudonymous developer named Satoshi Nakamoto, is the first successful decentralized cryptocurrency. In a nutshell, a cryptocurrency is a virtual coinage system that works similarly to a standard currency, allowing users to provide virtual payment for goods and services without the need for a central trusted authority. Cryptocurrencies rely on the transmission of digital data, with cryptographic methods used to ensure legitimate, one-of-a-kind transactions. Bitcoin advanced the digital coin market by decentralizing the currency and liberating it from hierarchical power structures. Individuals and businesses instead transact with the coin electronically through a peer-to-peer network. Beginning in 2011, it drew widespread attention, and a slew of altcoins – a catch-all term for all cryptocurrencies created after Bitcoin – sprang up. Litecoin was released in the fall of 2011, achieving modest success and holding the highest cryptocurrency market cap after Bitcoin until October 4th, 2014, when it was surpassed by Ripple. Litecoin altered Bitcoin's protocol, increasing transaction speed with the intention of making it more suitable for day-to-day transactions. Peercoin, another notable coin in the cryptocurrency evolutionary chain, employs a revolutionary technological development to secure and sustain its coinage. Peercoin employs a hybrid network security mechanism that combines the PoW technology used by Bitcoin and Litecoin with its own mechanism, proof-of-stake (PoS).

Blockchain is a Hyperledger - World Wide Spreadsheet

Bitcoin is not maintained in a centralized file; rather, it is represented by blockchain transactions, which are a form of a "global spreadsheet" that uses peer-to-peer technology to authenticate each transaction. One of the blockchain's biggest virtues is the transparency that comes with it being public (Herlihy, 2019). Every 10 minutes, all new Bitcoin transactions are "confirmed, cleared, and put in a block," which is then "connected to the previous block, forming a chain." If these blocks do not refer to one another, they are invalid; these blocks are also time-stamped to prevent them from being altered further. Similar to the World Wide Web's reach, such blockchains have the potential to become a "World Wide Ledger of value" over time (Ryan, C 2021).

While Bitcoin contains a lot of highly technical features, it is easy to comprehend with little technical understanding. Bitcoin's fundamental goal is to replace real cash by mimicking a massive global ledger system. Each user has an account with a specific number of Bitcoins. This procedure allows a system to simulate currency by permitting transactions, which update the ledger. If there is a global ledger that can be quickly updated in a safe and trustworthy manner, we can eliminate all physical cash which is an appealing possibility for many firms and investors in difficult economic times, and conduct all transactions via ledger updates. Bitcoin offers a technological solution for implementing such a global ledger (Homan, F 2018).

It's also worth noting that, while it's easier to conceive of a ledger as a collection of accounts with current balances, there's another way to look at it. Instead of retaining a basic table, one might sum up an individual's whole history of all transactions to establish their balance. While it is impracticable for a person to do so in practice, it gives the same semantic information and is straightforward for computers to comprehend, even over very large transaction lists. Bitcoin is in favor of the latter method. A distributed ledger is where a blockchain is defined as a "shared, trustworthy, public ledger that anybody may see but no single person controls." Participants in a specific blockchain system collaborate to keep the ledger up to date; it can only be changed through tight rules and consensus. Bitcoin's blockchain system "prevents double-spending and continually maintains track of transactions," which "allows for a currency without a central bank." Blockchains have also been described as "the latest example of the unexpected fruits of cryptography" (Don, T , Alex, T 2016).

Bitcoin is a blockchain

All transactions made during a specific time period are collected into what is known as a block under the Bitcoin protocol. This block is then broadcasted to all nodes connected to the Bitcoin network at the time. Bitcoin employs the PoW (proof of work) mechanism, which Adam Back proposed in 1997 (Adam and James, 2009). In order to agree on a set of broadcasted transactions, each node essentially takes the block and begins adding a piece of data called a nonce to the block, such that the (block+nonce) has a hash that meets certain requirements - in this case, it begins with a certain number of zeros. As a result, each node attempts to solve a complex mathematical computation, the outcome of which can be easily verified by computing a single hash. The Bitcoin protocol requires nodes to use the SHA-256 hashing function. Once a node solves the problem, the PoW requirements are met, and the new (block+nonce+hash) is added to the blockchain and broadcasted to all nodes. Because only one block can be verified at a time, the likelihood that a node will solve for the correct hash grows proportionally to the amount of CPU power expended. As a result, the resources consumed in this case are electricity and time, both of which are scarce.

Mining of Bitcoin

Mining refers to the entire process that each node goes through because, for each block that is verified, the node receives payment for its services. Miners are rational profit-seekers, so the Bitcoin protocol offers rewards in two forms: transaction fees and newly minted coins, known as mined coins, to incentivize individuals to mine. Each block verified by the Bitcoin protocol adds new coins to the market, which are given to the miner in exchange for the energy and time invested. This guesstimate decreases over time, so there will never be more than 21 million BTC in existence. In this regard, Bitcoin is analogous to commodities such as gold: the constant addition of a constant amount of new coins is analogous to gold miners expending resources to add gold to circulation. As a result, transaction fees will almost certainly have to rise in the long run in order to adequately compensate miners. The massive amounts of energy consumed by the PoW mechanism, with no other benefit other than transaction verification, is a major criticism. As the Bitcoin network's mint rate slows, eventually it could put pressure on raising transaction fees to maintain a preferred level of security. In this regard, Bitcoin is analogous to commodities such as gold: the constant addition of a constant amount of new coins is analogous to gold miners expending resources to add gold to circulation. As a result, transaction fees will almost certainly have to rise in the long run in order to adequately compensate miners. The massive amounts of energy consumed by the PoW mechanism, with no other benefit other than transaction verification, is a major criticism. As the Bitcoin network's mint rate slows, eventually it could put pressure on raising transaction fees to maintain a preferred level of security.

Fundamentals of Blockchain - Cryptocurrencies In Competition

At the time, there are a total of 18,000 or more cryptocurrencies as of March 2022, approximately 1583 distinct cryptocurrencies, according to coinmarketcap.com. As a result, the cryptocurrency industry encompasses far more than Bitcoin, despite the fact that Bitcoin has a market capitalization of approximately 800 billion. This section examines how competition in the cryptocurrency industry has evolved since Bitcoin's inception in 2009. It focuses on the evolution of coin economics.

In the domain of crypto, the goal of a consensus mechanism is to prevent bad actors from cheating on purpose. "Double-spending" is a famous example of cheating in the crypto realm. Consensus techniques alleviate the double-spending problem by making it costly and difficult for bad actors to propose a new block of approved transactions, discouraging them from doing so. Simultaneously, the algorithms encourage "good" nodes to propose blocks that they truly believe will be accepted in exchange for substantial incentives.

Blockchain technology is a decentralized method of keeping a virtually immutable ledger (Ramaswamy, 2020). Decentralization means that no single person or institution is in charge of checking and updating the ledger. The ecosystem's managers, i.e. miners/validators, are then responsible for its upkeep. They must deliberate among themselves (come to an agreement) on which transaction should be included to the block. The order in which the blocks are added. This is to ensure that they all have access to the same ledger. One of the most important parts of blockchain is the consensus mechanism, which helps it preserve its integrity and security. This is the sole reason why a Consensus Mechanism is required for the blockchain (Jordon, 2022).

How Consensus work?

Consensus on Proof-of-Work blockchains, such as Bitcoin, necessitates a substantial amount of energy, hardware, and computer power in order to propose a new set of transactions to the ledger, known as a block. Miners are the nodes that validate transactions and propose new blocks. Miners compete to generate a random number that will unlock the chain's next block. The miner who reaches that number first adds the next block and receives a block reward in exchange for their efforts. The only way to win is to create random numbers as quickly as possible (thus the word "work") and hope for the best. It's a competition of computing power, which necessitates the use of hardware and electricity.

The nodes – also known as validators – that validate transactions and propose new blocks on Proof-of-Stake blockchains are required to store a particular amount of value in the form of the blockchain's native token – this is their stake in the system. The more value a validator puts in, the better their chances of proposing a new block and earning the block reward. If a validator makes an error, it must pay a charge or risk being removed from the validation process. Most blockchains have a lot in common and function in similar ways. Consensus methods are procedures that ensure that all nodes on the blockchain, that maintain the blockchain and process transactions, are in sync with one another and agree on which transactions are valid and should be added to the blockchain. Because anybody can submit items to be added to the blockchain, all transactions must be regularly verified, and the blockchain must be constantly audited by all nodes. Blockchains are vulnerable to a variety of assaults if they lack adequate consensus mechanisms (Demelza, 2018).

There are numerous approaches to reach consensus. Most common ones are Proof of Work, Proof of Stake, Proof of Authority and Proof of History which are discussed below. Consensus mechanisms, however, can be public or private based on how to open to the participants in the network (Tate and Knapp, 2019). A public blockchain is completely open and anyone can join and participate in the network while a private network requires an invitation and must be validated by either the network operators or by a set of rules placed by them (Underwood, 2016).

Public Consensus Mechanisms

Proof of Work

"A Proof-of-Work (PoW) is a piece of data that is costly to produce in order to satisfy certain requirements but is trivial to verify," Cynthia Dwork and Moni Naor proposed in 1993. That is, PoW imposes an economic cost on the performance of a given function. Transactions in cryptocurrencies are not considered verified until a certain amount of energy has been expended. The majority of altcoins that use the PoW mechanism are exact copies of, or very similar to, the Bitcoin protocol. The following section will go over how Bitcoin implements the mechanism.

Blockchains using PoW: Bitcoin, Ehtereum, Dogecoin, Litecoin, Monero

Proof of Stake

The Proof-of-Stake mechanism is an alternative to the PoW mechanism. Instead of relying on computational power as a scarce resource, network security is dependent on coin ownership – proof-of-stake is a type of proof-of-ownership – which is also scarce. As a result, a miner must own some coin in order to verify a transaction and receive the coin reward. Furthermore, the likelihood that he will succeed in creating a new block is determined by the amount of coin he owns, not by computational power. As a result, there are very few energy costs in this transaction (Powell et al., 2021).

Furthermore, in order to undermine the system's integrity, one would need to own more than 50% of the coin currently being staked, in which case violating coin security would be extremely costly. Payment is typically made in the form of interest on the amount of coin staked to verify the transaction. As a result, most PoS coins lack a capped money supply and are thus inflationary. However, PoS systems face the problem of determining how to distribute the coin at first. Whereas PoW distributes coins to miners who add value to the network, a coin based solely on PoS must decide who receives the coins.

Blockchains using PoS: Cardano, Solana, Algorand, Tezos

PoS/PoW

The PoW technique is used for initial currency minting and distribution in a hybrid PoW/PoS system. In other words, PoW enables the network to distribute new currencies to miners. However, the PoS mechanism gradually phases out the PoW method, resulting in a long-term energy-efficient coin. Instead of depending on a single CPU per vote, block creation in this hybrid system is based on the notion of "coinage." Coinage is roughly equal to the amount of coin possessed multiplied by the present owner's life ownership of the coin. As a result, the block with the greatest coins is chosen for a generation. Furthermore, coins are created at a rate of one percent every coin-year used, serving as an interest rate for staking currency. The biggest advantage, however, is that this system does not use a lot of energy in the long term. As a result, the approach is cost-competitive with PoW and avoids the distribution difficulty inherent in PoS.

Blockchains using PoS/PoW: Dash, Decred

Proof of History

Proof of History (PoH) aims to lighten the load of the network nodes in processing blocks by providing a means of encoding time itself into the blockchain. In a regular blockchain, reaching consensus over the time a particular block was mined is as much a requirement as reaching consensus over the existence of the transactions in that block. Timestamping is critical because it tells the network (and any observer) that transactions took place in a particular sequence. PoH solves the time challenge, and thus reduces the processing weight of the blockchain, making it lighter and faster. Solana combines PoH with a security protocol called Tower Byzantine Fault Tolerance (Tower BFT), which allows participants to stake tokens so they can vote on the validity of a PoH hash. This protocol penalizes bad actors if they vote in favor of a fork that doesn't match the PoH records (Demelza, 2018).

Blockchains using PoH: Solana

Private Consensus Mechanisms

Proof of Authority

Proof of Authority (PoA) is a reputation-based consensus algorithm that introduces a practical and efficient solution for blockchain networks (especially private ones). The PoA consensus algorithm leverages the value of identities, which means that block validators are not staking coins but their own reputation instead. Therefore, PoA blockchains are secured by the validating nodes that are arbitrarily selected as trustworthy entities. The Proof of Authority model relies on a limited number of block validators and this is what makes it a highly scalable system. Blocks and transactions are verified by pre-approved participants, who act as moderators of the system. The PoA consensus algorithm leverages the value of identities, which means that block validators are not staking coins but their own reputation instead. Therefore, PoA blockchains are secured by the validating nodes that are arbitrarily selected as trustworthy entities.

PoA consensus algorithm may be applied in a variety of scenarios and is deemed a high-value option for logistical applications. When it comes to supply chains, for example, PoA is considered an effective and reasonable solution. The Proof of Authority model enables companies to maintain their privacy while availing the benefits of blockchain technology. Microsoft Azure is another example where the PoA is being implemented. In a few words, the Azure platform provides solutions for private networks, with a system that does not require a native currency like the ether 'gas', since there is no need for mining (Thomas,J 2019).

Blockchains using PoA: VeChain, Stratis

Findings - Generations to come in Cryptocurrencies

With more than 18,000 cryptocurrencies in existence as of March 2022 (CoinMarketCap; Josh,H 2022), it is imperative to observe how the fundamentals of blockchain technologies have evolved. As ethereum set a landmark of adding a smart contract in this hyperledger system, classifications in distinctive trends in innovations of cryptocurrency use and applications can depict the agreeable roadmap of in this explosive creation and reproduction today. Until now, there have been four generations of cryptocurrencies: the worlds of decentralization, dapps, interoperability, and extreme TPS.

Table 1: Cryptocurrency Generations

Generations	Innovations	Trends	Example Cryptocurrencies
1st Generation	Proof of Work	World of Decentralization	Bitcoin, Litecoin, Dogecoin
2nd Generation	Smart Contracts	World of DApps	Ethereum
3rd Generation	Scalability	World of Interoperability	Cardano, IOTA, Polkadot
4th Generation	Metastable Consensus	World of Extreme TPS	Solana, Avalanche

First Generation - Proof of Work, the world of decentralization

Bitcoin is an example of a first-generation cryptocurrency which has the most market capitalization which counts about half of the whole cryptocurrency market. The peer-to-peer accounting system is represented by this generation. It is a currency with no borders. Peer-to-peer technology enables us to conduct transactions without the need for a centralized third party, such as a bank, indicating that first-generation technology is ***decentralized***. However, first-generation currencies have scaling issues. The bitcoin scalability issue stems from the fact that blocks in the blockchain can only be one megabyte in size (Cameron,D, David,E, June,M and Clare,N 2019).

Bitcoin. Bitcoin is the first successful decentralized digital currency, as the system operates without the use of a central bank or a single administrator. Bitcoin was created in 2009 by a person or group of people going by the name Satoshi Nakamoto and released as open-source software (Nathan, R 2021).

Second Generation - Smart Contracts, the world of dapps (decentralized apps)

The second generation of cryptocurrency is known to be more intelligent than bitcoin. Ethereum is an example of currency discovered in this generation. There are two major differences between this currency and others. The first benefit is that it enables the use of a programming language on the blockchain. ***Smart contracts*** and ***decentralized applications*** make use of the code (Herlihy, 2019). It reduces transaction sizes. It secures the transactions for both parties, allowing one to receive money after completing the task. The second generation also has a minor scalability issue. Second-generation coins include the sparkle coin, sky coin, and Ethereum.

Ethereum. Ethereum is an open-source, public blockchain-based distributed computing platform that supports smart contracts (scripting). The Ethereum Virtual Machine (EVM) is a decentralized Turing-complete virtual machine that can execute scripts via an international network of public nodes. Ethereum also has a cryptocurrency token known as "ether," which can be transferred between accounts and used to compensate participant nodes for computations performed (True, T 2021).

Third Generation - Scalability, the world of interoperability

There is no specific example of a third-generation cryptocurrency. All currencies are competing to be the next generation's currency, and some are already on the horizon. *The primary goals of this generation are the need for a governance system, reduced* ***scalability****, and* ***interoperability****.* Interoperability enables us to

communicate with other blockchains or cryptocurrencies. Cardano and IOTA are two third-generation coins on the horizon.

Cardano. Cardano is one of the most valuable cryptocurrencies in terms of market capitalization. It is intended to be a next-generation evolution of the Ethereum concept, with a blockchain that is a flexible, sustainable, and scalable platform. Cardano aims to enable smart contracts, which will enable developers to create a wide range of decentralized finance apps, new crypto tokens, games, and other applications. Cardano's main advantage is that, unlike Bitcoin, it is built with two layers. The Cardano blockchain is developed in two tiers. The first is the account value ledger, and the second is the rationale for value transfers from one account to another.

The Cardano Settlement Layer is the first layer of the Cardano blockchain (CSL)
The CSL serves as an account ledger or a balance ledger. This is a concept that was developed as a way to improve the Bitcoin blockchain. To generate new blocks and confirm transactions, it employs a proof-of-stake consensus algorithm.

The Cardano Computation Layer is the second layer of the Cardano protocol (CCL)
The data about how values are conveyed is stored in the CCL. Users of the CCL can define customized rules when analyzing transactions because the computation layer is not tied to the balance ledge (Rakesh,S 2021).

IOTA. IOTA is an open-source distributed ledger (cryptocurrency) aimed at enabling secure communications and payments among machines on the Internet of Things. IOTA's transactions are free regardless of transaction size, confirmation times are fast, the number of transactions the system can handle concurrently is unlimited, and the system is easily scalable because it uses directed acyclic graph (DAG) technology rather than traditional blockchain. David Snsteb, Sergey Ivancheglo, Dominik Schiener, and Dr. Serguei Popov founded IOTA in 2015. In order for an IOTA user to send a transaction, the user must first validate two other, randomly chosen transactions. To be accepted as "confirmed" by its recipient, a sent transaction must accumulate a sufficient level of verification. IOTA is managed by a single administrator known as the Coordinator, who confirms all transactions in accordance with a set of released milestones (Amir,H 2022).

Fourth Generation - Metastable Consensus, the world of extreme TPS (transactions per second)

While third-generation cryptos are still in the early stages of adoption, a new class of cryptocurrencies is redefining the state of the art. They are cryptocurrencies that use ***metastable*** consensus mechanisms like Avalanche. The network is never fully stable and hard set on a given consensus in this class of consensus mechanisms. Instead, it is adaptable to change as long as a sufficient number of nodes believe it should. Fourth-generation cryptocurrencies, in general, have ***extremely high transaction per second*** scalability, rivaling VISA or MasterCard.

Fourth Generation traits:

- Metastable high transaction per second consensus mechanism.
- NFTs - Non-Financial Transactions Support for Native Non Fungible Tokens. NFTs are possible from 2nd generation, however, it is a new trend that later generations blockchains often accommodate this feature.
- Subnets and network sharding - dividing the blockchain into segments that allow it to scale
- Native Asset Registry - Segmented architecture accommodates several cross-chain assets, each with its own infrastructure and resources, allowing for the creation of an asset registry.

- Atomic cross-chain operations entail freely moving assets from one subnet or subsystem to another in a single atomic operation that either succeeds or fails. There will be no centralized exchanges or custodial requirements in the future.

Solana. Solana is a crypto-computing platform with the goal of achieving high transaction speeds while maintaining decentralization. Solana is a cryptocurrency and a flexible framework for launching decentralized software (dapps) - ranging from Degenerate Apes to the Serum decentralized exchange — similar to Ethereum (or DEX). Its main novelty is speed, which is achieved through a combination of innovative technologies, including a consensus technique known as proof of history (PoH). Solana can execute around 50,000 transactions per second, whilst Ethereum can only handle 15 or less (the ETH2 upgrade, which is currently underway, is designed to make Ethereum much faster than it is now). Because Solana is so quick, traffic and fees are kept to a minimum. Solana's developers hope that its rapid speeds and low rates would someday allow it to compete with centralized payment processors like VISA. The native cryptocurrency of Solana is SOL, which is utilized for transaction fees and staking. It also entitles owners to vote on future upgrades. SOL can be purchased and sold on exchanges like Coinbase (Daniel, P 2021).

Avalanche. Avalanche consensus is surprisingly efficient, reaching finality in milliseconds. In random order, nodes query each other about transactions. Nobody knows which node is going to query which. As a result, it's extremely difficult to defraud the system because you can't predict who will be questioned about a specific TX (vertex). Nodes quickly form opinions about transactions, validating or rejecting them. There is no single chain tip consensus in Avalanche systems. Everyone comes to this conclusion on their own but at their own pace. It is the most decentralized cryptocurrency available; anyone can validate, stake, and participate by running a simple process Seq (2020).

Discussion - Classifications of Blockchain: A Pathway to the Moon

Blockchain technology has evolved since the dawn of the first successful cryptocurrency, Bitcoin. At the moment, blockchain concepts may be divided into four categories with two dimensions: participants' openness (public or private) and network's control scheme (decentralized or centralized).

	Centralized	**Decentralized**
Public	Cryptocurrency Stablecoins	Permissionless Blockchain
Private	Fiat Stablecoins	Permissioned Blockchain

Figure 1: Classifications of Blockchain

Permissionless blockchains **(public/decentralized)** such as Bitcoin, Ethereum, etc, are decentralized, institutionless, completely public peer-to-peer networks that anybody can join without the consent of other users. In the Permissionless model, which is also known as a public blockchain, there are no restrictions, and the participation is not controlled by an administrator. Anyone can participate in the consensus and validate the data. There are no administrators allowing the users to participate or giving them the permission and rights to make the changes. It is a completely decentralized blockchain platform across unknown parties.

Permissioned blockchains **(private/decentralized)** are analogous to the concept of a federation, in which a group of members allows new members to join only with the agreement of the existing members. Because there are hurdles to membership in the elite club, a node must be granted permission to join the network. We employ a permission ledger for security activities on a blockchain ledger, which can only be performed by a few people who are permitted to do so. Simply put, the distributed ledger in this system can only be viewed by a select few individuals who have been granted permission by the administrator. These users are given various levels of rights that allow them to do specific tasks. However, anyone who has not been granted permission by the administrator will not be able to access it publicly. The main advantage of this architecture is that because the number of persons who may access the ledger is limited, any modifications made to the ledger can be easily traced and the user recognized (Shobit, S 2021,Kathleen W,Eugenia,W 2021).

Cryptocurrency Stablecoins **(public/centralized)** are backed by another cryptocurrency as collateral, for example, DAI is the most known stablecoin using ether (ETH), the native token of the Ethereum network. This is also called on-chain crypto collateral stablecoin as it occurs on-chain and employs smart contracts instead of relying on a central user.

Fiat Stablecoins **(private/centralized)** are the most commonly used stablecoins which are backed one to one by fiat currency. Unlike cryptocurrency stablecoins, fiat stablecoins do not use any other cryptocurrencies as the underlying collaterals, also called as off-chain assets. As cryptocurrencies are growing fast as both currency and asset by disintermediating third parties in monetary exchange, like financial institutions, governments of countries are proposing fiat stablecoins such as digital dollars and digital yuan.

Conclusions

The original proposal of permissionless blockchain, such as Bitcoin, is very promising with the hope of disintermediating from the central banks or other financial institutions (Comprehensive Technological Research, 2022). This is a similar phenomenon when online bookstores disintermediate middlemen from a supply chain, resulting in lower prices with lower costs. In the current status of blockchain involvement, we do not picture the intermediation roadmap of cryptocurrencies because blockchain technologies are sharing the interests and interferences in fiat currencies of countries in the world (McFarland, 2021). One example is China's cryptocurrency ban in 2021 as the government has feared that currencies cannot be centrally controlled as citizens move out Yuan to decentralized assets such as untraceable cryptocurrencies due to blockchain's anonymity (Cai, 2021). Contrarily, China has created Digital Yuan which is the stablecoin of Chinese Yuan in crypto format. The United States of America also has started to discuss the possibility of the Digital Dollar.

It is still in a very early stage of cryptocurrencies. Contrarily to its original intention to be a payment method, cryptocurrencies have established themselves as investment assets like equities in the stock market (Caine, 2021). Recently, there are more merchants have started to accept cryptocurrencies as payment, substituting the use of credit cards. This duality of cryptocurrencies (payment/investment) makes blockchain technologies very attractive to the new era of world economy. It is very exciting to watch how blockchain will be adopted/innovated into our pathway (to the Moon?) in coming years.

References

Adria, C. (2021). These Will Be the Hottest Cryptocurrencies in 2022. https://www.fool.com/investing/2021/12/07/these-will-be-the-hottest-cryptocurrencies-in-2022/

Adam, B. (2019). The Future Of Cryptocurrency in 2019 and Beyond. https://www.investopedia.com/articles/forex/091013/future-cryptocurrency.asp

Amir, H. (2022). Why Third Generation Cryptocurrencies Are Game-Changers for Venezuela. https://medium.com/hackernoon/why-third-generation-cryptocurrencies-are-game-changers-for-venezuela-cb8c9b016f9d

Cai, L., Sun, Y., Zheng, Z., Xiao, J., and Qiu, W. (2021). Improving measurement of productivity in higher education. *Communications of the ACM*, 64(11), 88-93.

Caine, A. (2021). Myths vs. Facts of Cryptocurrency. Houston, TX, King of Kings Publishing.

Cameron, D., David, E., June, M. and Clare, N. (2019). Cryptocurrency: Ten Years On. https://www.rba.gov.au/publications/bulletin/2019/jun/cryptocurrency-ten-years-on.html

Cointelegraph. (2020). The history of Bitcoin: When did Bitcoin start? https://cointelegraph.com/bitcoin-for-beginners/the-history-of-bitcoin-when-did-bitcoin-start

Comprehensive Technological Research. (2022). The New Digital Revolution for Beginners. Las Vegas, NV.

Daniel, P. (2021). What is Solana? A Scalable, Decentralized Network for Dapps. https://decrypt.co/resources/what-is-solana-a-scalable-decentralized-network-for-dapps

Demelza, H. (2018). Consensus Mechanisms. https://cryptoresearch.report/crypto-research/consensus-mechanisms/

Don, T., and Alex, T. (2016). How Blockchain Will Change Organizations. https://sloanreview.mit.edu/article/how-blockchain-will-change-organizations/

Homan, F. (2018). Imagining the forest of World Wide Ledger from the Blockchain Trees. https://blogs.gartner.com/homan-farahmand/2018/09/24/imagining-the-forest-of-world-wide-ledger-from-the-blockchain-trees/

Herlihy, M. (2019). Blockchains from a Distributed Computing Perspective. *Communications of the ACM*, 62(2), 78-85.

Josh, H. (2022). How Many Cryptocurrencies Are There In 2022? https://explodingtopics.com/blog/number-of-cryptocurrencies

Jordon, T. (2022). 63+ Cryptocurrency Statistics, Facts & Trends. https://www.buybitcoinworldwide.com/cryptocurrency-statistics/

Kathleen W., and Eugenia W. (2021). Types of Blockchain: Public, Private, or Something in Between. https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between

McFarland, E. (2021). Blockchain Wars. Las Vegas, NV.

Nathan, R. (2021). Were There Cryptocurrencies Before Bitcoin? https://www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/

Powell, L., Hendon, M., Mangle, A. and Wimmer, H. (2021). Awareness of blockchain usage, structure, & generation of platform's energy consumption: Working towards a greener blockchain. *Issues in Information Systems*, 22(1), 114-123.

Ramaswamy, M. (2020). Leveraging Blockchain Technology for Small Businesses. *Issues in Information Systems*, 21(3), 207-216.

Ryan, C. (2021). Bit 2. The Global Spreadsheet, Information Theory, and Law. https://powping.com/posts/c982f51134cb23251616cc8fac0c8c7d570748005b81b38d90981c2e05ebb807

Rakesh, S. (2021). Cardano Aims to Create a Stable Cryptocurrency Ecosystem. https://www.investopedia.com/news/introduction-cardano/

Shobit, S. (2021). Public, Private, Permissioned Blockchains Compared. https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/

SEQ (2020). Avalanche Consensus, The Biggest Breakthrough since Nakamoto. https://medium.com/avalanche-hub/avalanche-consensus-the-biggest-breakthrough-since-nakamoto-66e9917fd656

Tate, J. and Knapp, A. (2019). Blockchain 2035: The Digital DNA of Internet 3.0. Las Vegas, NV, BlueShed LLC.

True, T. (2022). What Is Ethereum? https://learn.financestrategists.com/finance-terms/ethereum/

Thomas, A. (2019). Proof-of-Authority Algorithm Use Cases Grow: From Pharma to Games. https://www.bgp4.com/2019/11/17/proof-of-authority-algorithm-use-cases-grow-from-pharma-to-games/

Underwood, S. (2016). Improving measurement of productivity in higher education. *Communications of the ACM*, 59(11), 15-17.