Ilkogretim Online - Elementary Education Online, 2020; Vol 19 (Issue 4) : pp. 3462-3485
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2020.04.764734

C-BDE: A Comprehensive analysis to understand blockchain development environment

Mona Mulchandani, Phd Scholar, Computer Science and Engg., Medicaps University, Indore, India, mona.mulchandani@gmail.com
Dr. Dheeraj Rane, Asst. Professor, Computer Science and Engg., Medicaps University, Indore, India, dheeraj.rane@medicaps.ac.in

Abstract: In the digital world Smart contracts have become invincible. One of the applications of smart contracts is Blockchain has many advantages including decentralization, continuity, privacy, auditability and traceability. There is a broad variety of blockchain applications from cryptocurrencies, financial services, risk management, internet of things (IoT), and public and social services. Mining creates new blocks in the chain through secure and robust consensus. Mining also introduces rewards for the validation work. The blockchain taxonomy, introduces typical blockchain consensus algorithms. While a range of swotting concentrate on using blockchain technology in various applications, the unified blockchain does not have a systematic survey of mining techniques. Our motive is to observe and compare various blockchain mining techniques used by general blockchain applications including crypto currencies. The analysis will model a comprehensive new optimized blockchain mining architecture which would incorporate all common parameters as well as differences among the existing architectures. As the architecture gets designed it will be analyzed and then it will be implemented for validation.

Keyword: Blockchain, consensus algorithm, decentralize transaction, security, mining, digital, cryptocurrency.

I. INTRODUCTION TO BLOCKCHAIN

Computing power and breakthroughs in cryptography, along with the discovery and use of some new and interesting algorithms, have allowed the creation of distributed ledgers. In its simplest form, a distributed ledger is a database held and updated independently by each participant (or node) in a large network. The distribution is unique: records are not communicated to various nodes by a central authority, but are instead independently constructed and held by every node. That is, every single node on the network processes every transaction, coming to its own conclusions and then voting on those conclusions to make certain the majority agree with the conclusions.

A public ledger derives its name from the age-old record-keeping system that was used to record information like agriculture commodity prices, news and analysis. It was available for general public viewing as well as for verification. Public ledgers work the same way as bank records, though with a few differences. State of the art public blockchain protocols based on consensus algorithms are open source and not permission. Anyone can participate, without permission. (i) Anyone can download the code and start running a public node on their local device, validating transactions In the network, engaging in the process of consensus – the process to determine which blocks are added to the chain and what the current state is stated (ii) Anybody in the world can submit transactions over the network and demand them to be included in the blockchain if they are valid. (iii) Anyone can read transaction on the public block explorer. Transactions are transparent, but anonymous/pseudonymous.

The blockchain is like another application layer to run on the existing stack of Internet protocols, adding an entire new tier to the Internet to enable economic transactions, both immediate digital currency payments (in a universally usable cryptocurrency) and longer-term, more complicated financial contracts. Any currency, financial contract, or hard or soft asset may be transacted with a system like a blockchain. A blockchain is quite literally like a giant spreadsheet for registering all assets, and an accounting system for transacting them on a global scale that can include all forms of assets held by all parties worldwide.

SWOT Analysis of Blockchain
Strength: Cost-efficiency, Speedy access to medical data, Autonomous, Tamper proof information sharing.
Weakness: Less number of software and system vendors, not much scalable, lack of storage capacity.
Opportunities: Lower fraud risk, more control over data, potential of startup.
Threats: Hesitant social adaptation of technology, Non-standardization, interpretability issues.

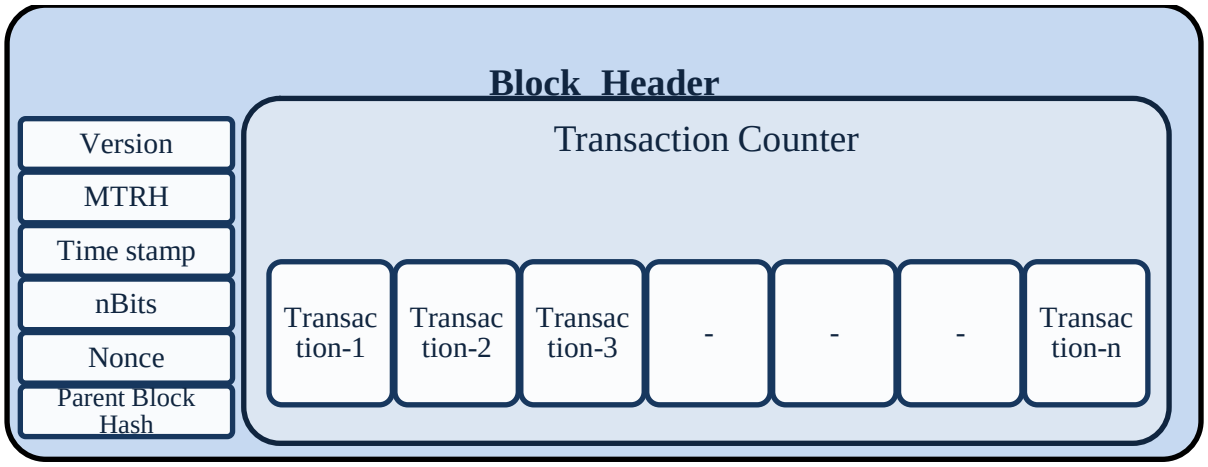

Figure-1: Block Structure in a Blockchain

Block is having a digital piece of information consist of –Transaction details, say the date, time, and dollar amount of your most recent Amazon purchase, Information about who is participating in transactions, Information which sets them apart from other blocks. Just like you and I have names that distinguish us from each other, every block stores a unique code called a "hash" that helps us to tell apart from any other block.

II. LITERATURE SURVEY

In his paper, Saqib Ali et.al. the essential storage room for data about exchanges is known as a block. Each block stores data about the network. In addition, each block contains information about any or all of the latest transactions which were not previously included in previous chains. Additionally, a block acts as a continuous general record or record book. Each block inside is a perpetual store of records of past transactions[1]. Once a square is finished, it offers path to the following block. These blocks are combined in a connected chain. This relationship prompted the name Blockchain.

As mentioned by Deepak Puthalet. al. [2], Blockchain is a distributed ledger that maintains an unceasingly evolving rundown of information records that are solidified against altering and modifying, even by information stores hubs administrators. One can see a Blockchain as a transparent director of all transactions that have ever been carried out. It grows continuously, as finished blocks are connected to past blocks, creating a chain. In a Blockchain, blocks are imperatively inserted in a direct, sequential order.

In his work Guy Zyskindet. al. has drawn the Blockchain worldview which can be reached out to give a summed up system to actualizing decentralized figure assets. Each process asset can be thought of as a singleton state-machine that can change between states by means of cryptographically-secured exchange [3]. While producing another state-machine, the nodes encode rationale which characterizes valid state transition and transfer it onto the blockchain. The blocks diary a progression of substantial transactions that, when incrementally executed with the state from the past block, transform the state-machine into its present block.

Zibin Zheng1 et. al. [4] describe the first block in the blockchain which is called the genesis block. It is the common ancestor of all the blocks in the blockchain, meaning that if you start at any block and follow the chain backward in time, you will eventually arrive at the genesis block. Every node always starts with a blockchain of at least one block because the genesis block is statically encoded within the bitcoin client software, such that it cannot be altered.

In his inspect Shuai Wang et. al., a block consists of the header block and the body row. It includes specifically- Block Version: set of criteria for block approval to be taken afterwards. Merkle tree root hash: Merkle hash estimation considerable number of exchanges in the block. Block Timestamp: current time since 1 January 1970 as seconds in widespread time; N Bits: Significant Block Hash goal limit. Nonce: A 4-byte sector, usually starting at 0 and increments with each hashed estimation. Parent hash square: a 256-

piece hash-estimate based on the past node. The block body consists of a counter and transaction to a transaction The greatest amount of transaction a block can contain depends on the size of the block and the duration of each transaction. A nonce is a number added to a hashed block which meets the restrictions of difficulty level when rehashed.
("quote">number only class="quote">used once")

Parent hash square: a 256-piece hash-estimate based on the past node. The block body consists of a counter and transaction to a transaction. The greatest amount of transaction a block can contain depends on the size of the block and the duration of each transaction.. The greatest number of transaction that a block can contain relies upon the block size and the span of every transaction. A nonce ("number only used once") is a number added to a hashed block which meets the restrictions of difficulty level when rehashed. The nonce is the number the miners of blockchain solve for. The nonce is the number that blockchain miners are solving for. Blockchain adds a variance called nonce in each block[5]. This nonce concept like salt applied to block contents.

S. Nakamoto et. al. [6] Bitcoin has written about Peer-to-Peer Electronic Cash System. This paper described a way of exchanging a currency Bitcoin that combines cryptography, computer science, and game theory in its design and implementation. Satoshi's creation enabled a participant to digitally transact directly with another participant without relying on a single, centralized intermediary, such as a bank, to validate the payments. When we say peer-to-peer, we are describing a transaction from one entity to another, directly. There is no intermediary the transaction has to pass through.

Trent McConaghy et. al. state that Bitcoin attracted attention for its ability to allow for peer-to-peer transactions without a centralized intermediary. Technologists were drawn to the blockchain, the underlying component technologies on which Bitcoin operates. To introduce the concept, a blockchain is a decentralized ledger that records transactions or activity between two participants permanently with verification. This verification comes in the form of reviewing cryptographic functions and timestamps. Transactions can be verified on multiple computers, which are referred to as nodes. This makes the blockchain decentralized and transparent. Blockchain technology can be uncoupled from the Bitcoin protocol and can be used for many other kinds of cryptocurrencies. It can also be applied across industries to a variety of use cases, specifically record of ownership tracking and management (often referred to as provenance), creative rights management, patient records, etc.

Deepak Puthal et. al. state that in the case of blockchains, they are politically decentralized because no one person has singular control over them. They are also architecturally decentralized because their infrastructure has no central point of failure, as each node keeps a copy of the blockchain[7]. But, blockchains are logically centralized because the system behaves like one computer despite being spread apart on all the participating nodes in the network.

In his cram Jun Zouet. al. has described for a block to be part of the blockchain, it needs to be given a valid hash. This contains the timestamp, the nonce and the difficulty. Mining is another crucial part of the blockchain technology, but it is outside the scope of this article. The third part is a merkle tree root[8]. This is a data structure to summarize the transactions in the block.

Omar Badreddinet. al. Describes various types of blockchains viz:
1. Public Blockchain: Public Blockchain protocols in light of Proof of Work (PoW) agreement calculations are open source and not consent. Anybody can take part, without consent. a. Anyone can download the code and begin running a public node on their local device, approving transactions in the network, accordingly taking an in the Agreement Procedure – the process for deciding which blocks are attached to the chain and the state in question.

2. Federated Blockchains or Consortium Blockchains: Federated Blockchains work under the authority of a group. Instead of public Blockchains, they don't enable any individual with access to the Internet to partake during the time spent confirming transactions. Federated Blockchains are speedier (higher adaptability) and give more transaction protection. Consortium blockchains are for the most part utilized as a part of the managing an account division. The agreement procedure is controlled by a pre-chosen set of nodes; for instance, one may envision a consortium of 15 money related organizations, every one of for which a node works and of which 10 each block must be signed in order to make the block valid.

1. Private Blockchains: Compose authorizations are centralized to one association. Read consents might be public or confined to an arbitrary extent [9].

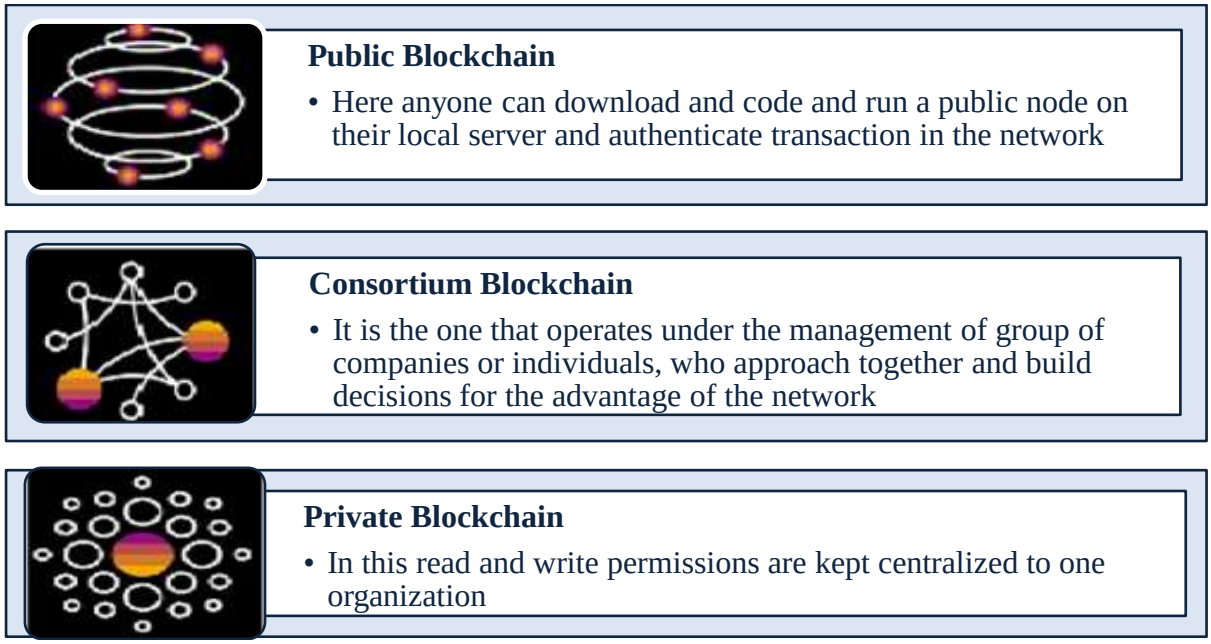

Figure 2: Types of Blockchain

HaraldVrankenet. al. have written about permissionless blockchain networks which power up most of the market's digital currencies. They allow every user to create a personal address and begin interacting with the network, by submitting transactions, and hence adding entries to the ledger. Additionally, all parties have the choice of running a node on the system, or employing the mining protocols to help verify transactions. In the case of Bitcoin, mining is done by solving complex mathematical equations which in return validate the transactions saved on the network – anyone is free to download the bitcoin blockchain and begin mining operations, in exchange for mining fees and block rewards.

Permissioned blockchains [10] maintain an access control layer to allow certain actions to be performed only by certain identifiable participants. These blockchains differ from public as well as private blockchains. A blockchain can be built and accessed in multiple ways. For instance, Bitcoin, the most popular cryptocurrency blockchain allows anyone to participate in the network in the capacity of a full node, or a contributing miner. Anyone can take a read-only role, or make legit changes to the blockchain like adding a new block or maintain a full copy of the entire blockchain. Such blockchains, which allow equal and open rights to all participants, are called open, public, or un-permissioned blockchains.

In his paper ZibinZhenget. al. has described the characteristics[11] of blockchain viz.

1. Decentralization: Any transaction should be approved by the trusted entity (e.g. the national bank) in conventional centralized transaction structures, certainly resulting in the cost and execution bottlenecks on the central servers. In contrast to the centralized mode brought in, outsider is never needed in blockchain again. Blockchain Agreement Calculations are used to preserve details distributed network.

2. Persistency: Transactions can be checked quickly and fair miners will not admit fraudulent transactions. It's also hard to erase or rollback transactions once they're used in the blockchain. You could instantly find blocks which contain invalid transactions.

3. Anonymity: May client can associate a generated address with the blockchain, which does not reveal the client's real identity. Be aware of the blockchain
.
4. Auditability: Bitcoin blockchain stores information about client adjusts in light of the Unused Transaction Performance (UTXO) shows: every transaction will apply to any previous unused exchanges.

When the present transaction is registered in the blockchain, the state of the unspent transactions referred will change from unspent to spent. And transactions may be effortlessly confirmed.

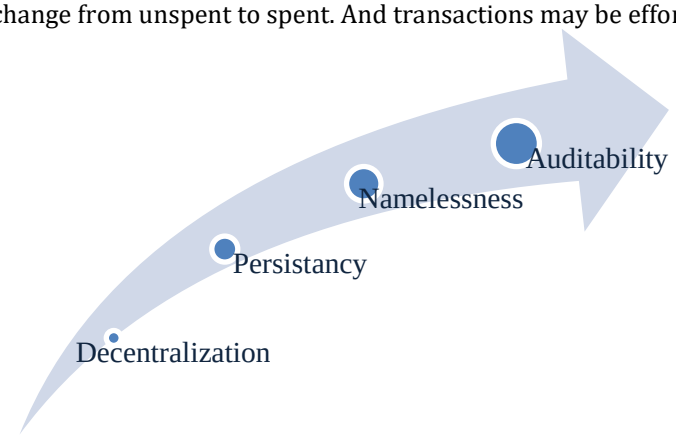

Figure 3: Characteristics of Blockchain

Florian Hawlitschekaet. al. [12] has explained the advantages of Blockchain First, it currently exists as a peer-to-peer network that has no single point of failure. If there is a failure in any node, the other nodes will continue to operate, maintaining the system's availability. Second, almost the entire documentation is digital and can be easily applied to many different applications. All transactions on the Blockchain are visible to all its participants, with the corresponding increase in auditability and trust. Changes to the Blockchain are extremely difficult and in the very rare case such a change occurred, it would be visible to the other users.

Distributed denial of service (DDoS) attack is hard to conduct in a blockchain network. Nevertheless, blockchain technology is vulnerable to DDoS attacks and these attacks on blockchain networks are in fact the most common form. Jo˜ao Sousa et. al. state that while attacking a blockchain network, hackers typically aim to break down a node by using multiple requests to absorb all its computing power. DDoS attackers are trying to isolate the network's mining pools, e-wallets, crypto exchanges and other financial services. A blockchain can also be hacked with DDoS. In its application layer, a blockchain can also be compromised with DDoS when hackers use DDoS botnets. Bitcoin takes steps in tandem with other blockchain networks to defend against DDoS attack [13].

In his paper Florian Wessling et. al. discuss Sybil attack [14] which is organized by assigning the same node to multiple identifiers. Blockchain networks do not have trusted nodes, so all requests are sent to a number of nodes. One hacker takes control of several nodes in the network during a Sybil attack. The victim is then surrounded by fake nodes which close all their transactions. The target ends up being vulnerable to double-spending assaults. A Sybil assault is very hard to detect and avoid,, but the following measures can be effective: increasing the cost of creating a new identity, requiring some type of trust for joining the network, or considering user power based on reputation.

Zibin Zheng1 et. al. A majority attack [11] is possible when 51 percent of the network hash rate is dominated by a hacker and an alternate fork is created that eventually takes precedence over current. This attack was initially the only known weakness in blockchain and in the near past seemed unlikely. At least five cryptocurrencies, however, — Verge, ZenCash, Monacoin, BitcoinGold, and Litecoin Cash — have already suffered from attacks of 51 per cent. In each case, cyber criminals gathered ample hashing power to hack the network and pocket millions of dollars

In his paper Mauro Contiet. al., eclipse attack [15] allows a hacker to monitor a large number of IP addresses, or to have a botnet distributed. The attacker then overwrites the addresses on the victim node's tried list, and waits until the victim node restarts. After restarting, all outgoing victim node connections will be routed back to the attacker-controlled IP addresses. This leaves the victim unable to receive transactions that are interested.

Selfish mining refers to a malicious miner's attempts to increase his share of the reward by not transmitting mined blocks to the network for a while and instead releasing many blocks at once, causing other miners to lose their blocks, possible steps to avoid this form of attack may be random assignment of

miners to different branches of pools, choosing the block with a more recent timestamp, or creating blocks within a limited appropriate time frame. This type of attack is also called withholding block.

In his learning Zibin Zheng1 et. al. discuss applications of blockchain[4]. A. Financial Service Blockchain has been widely applied for financial transaction which is so-called cryptocurrency. Nowadays, cryptocurrencies have appeared as prominent software systems. The first block or genesis block contains the first transaction. The hash of the first block is forwarded to the miner, who employs it and generates a hash for the second block. In similar fashion, the third block creates a hash that comprises of the first two blocks, and etc. All blocks in the blockchain can be traced back to the genesis block.

Pinyaphat Tasatanattakool et. al. B. Healthcare Blockchain has a tremendous potential in addressing the interoperability issues exist in the current healthcare systems. It can be used as a standard which allows the stakeholders, i.e. healthcare entities, medical researcher, etc to share electronic health record (EHR) in a secure manner. The system enables users to process the patient data without exposing patient privacy 16. C. Business and Industry - In his paper, Karl Wustet.al. Emergence of Internet of Things (IOT) has brought many advantages such as delivering an inter-connection between objects and humans. This motivates authors in to propose an e-business architecture which is particularly developed for IOT environment [17]. For this purpose, distributed autonomous corporation (DAC) is adopted as an entity that gives transaction services in the absence of human intervention.

In his paper, XiweiXu proposes Blockchain taxonomy[18], and blockchain-based structures. Using blockchain technology, taxonomy can be used when analyzing blockchains and assist in designing and testing software architectures. Their taxonomy encompasses the main architectural features of blockchains, and the effect of various decisions. This taxonomy is intended to assist with significant architectural considerations about the performance and quality attributes of blockchain based systems.

III. DOMINANT CRYPTOCURRENCIES

A cryptocurrency is a digital record-keeping device that uses balances to keep track of the obligations from trading and that is publicly known to all traders. In the absence of a central authority, the cryptocurrency relies on a distributed verification of transactions, updating and storage of the record of transaction histories. This necessitates that consensus between the users is maintained about the correct record of transactions. This trust in the currency is established by having a competition for the right to update record. The possibility of double-spending can undermine the usage of the cryptocurrency. This problem is mitigated by the usage of the blockchain and by introducing confirmation lags.

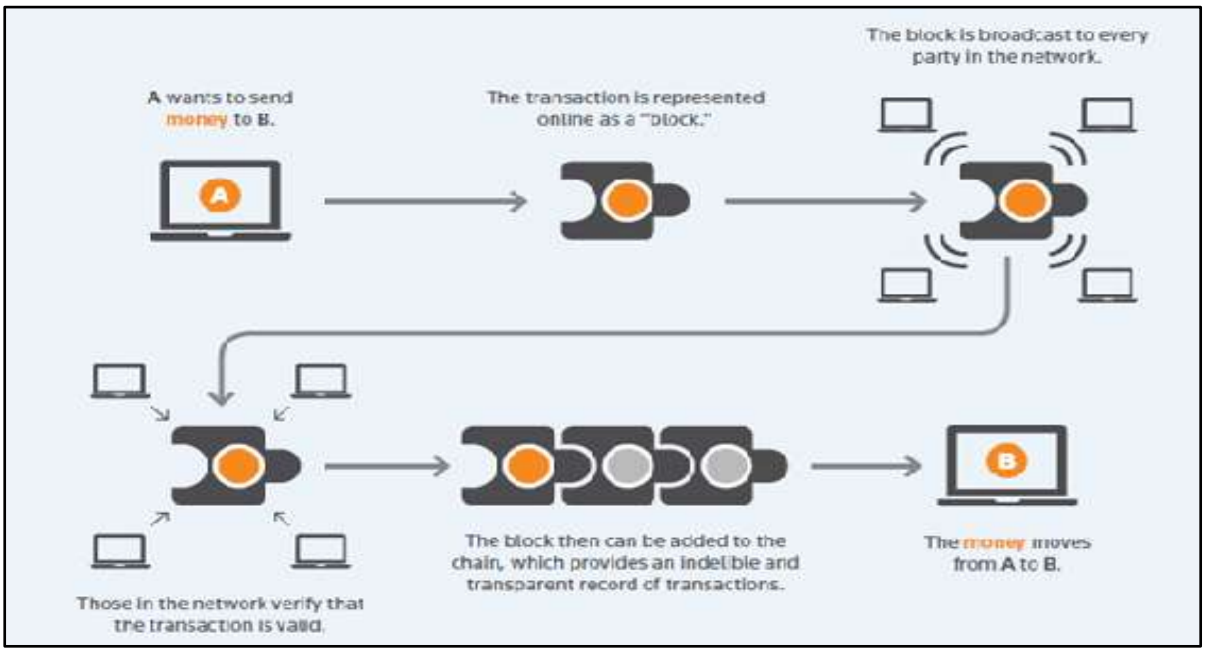

Figure 4: Visual Representation of Blockchain as Crypto currency [37]

3.1 Dominant Global Cryptocurrencies

Bitcoin(BTC)

Its security robustness, two main properties have probably been its key to success: anonymity and decentralization. Bitcoin is an online virtual currency based on public key cryptography, proposed in 2008. Bitcoin is a cryptocurrency based on accounting entries. For that reason, it is not correct to look at bitcoins as digital tokens since bitcoins are represented as a balance in a bitcoin account. A bitcoin account is defined by an Elliptic Curve Cryptography key pair. The bitcoin account is publicly identified by its bitcoin address, obtained from its public key using a unidirectional function. Using these public information users can send bitcoins to that address. Then, the corresponding private key is needed to spend the bitcoins of the account. Regarding this definition, it is easy to understand that any user can create any number of bitcoin addresses (generating the key pair) either using any standard crypto-software or self purpose created programs, like bitcoin wallets.

Being the oldest cryptocurrency, it has the largest developer and investor group to back it up for further development. Bitcoin is easy to buy, even for beginners, as the top exchanges and wallets support it all. Bitcoin is accepted in the mainstream economy. Bloomberg, Microsoft, Overstock.com, Expedia.com and several others have also started accepting BTC payments.

Ethereum (ETH)

Ethereum is a framework built on blockchain designed to build decentralized applications and smart contracts. Ethereum is Vitalik Buterin's second most popular crypto-currency after Bitcoin was founded in 2015. Ethereum is more than just a digital currency, practically. Ether is the native crypto-currency used by all the Ethereum blockchain transactions.Ethereum is a decentralized software platform that enables Smart Contracts and Distributed Applications (ĐApps) to be built and run without any downtime, fraud, control or interference from a third party. During 2014, Ethereum had launched a pre-sale for ether which had received an overwhelming response.

It's the most common platform to create smart contracts, what the next big thing in the cryptocurrency universe is considered to be. The Ethereum offers a fantastic forum for other blockchain projects to launch the Initial Coin Offerings (ICOs).

Ripple (XRP)

Ripple is a real-time global settlement network that offers instant, certain and low-cost international payments. Ripple “enables banks to settle cross-border payments in real time, with end-to-end transparency, and at lower costs. Ripple’s structure doesn't require mining; it reduces the usage of computing power, and minimizes network latency. Ripple believes that ‘distributing value is a powerful way to incentivize certain behaviors’ and thus currently plans to distribute XRP primarily “through business development deals, incentives to liquidity providers who offer tighter spreads for payments, and selling XRP to institutional buyers interested in investing in XRP.”

It takes about a week to transfere international capital. Ripple, on the other hand, will make that happen in seconds. Also, the fees are considerably smaller as compared to what financial institutions and other cryptocurrencies are paying.Ripple has a very clear use case international payment.

Bitcoin Cash (BCH)

In 2016 Bitcoin Cash was forced out of Bitcoin itself. When Bitcoin's developer group couldn't agree on the improvements needed in Bitcoin's code, they were forced into BCH. The aim of creating BCH was to solve some of Bitcoin's existing problems, in particular with respect to scalability and transaction fees.

Bitcoin Cash is supposed to be fully decentralized, close to Bitcoin. But now it has a CEO; something that has been widely criticized in the field of cryptography. BCH mining is as lucrative as Bitcoin mining, but it does produce fewer returns, so it's not a favorite among the miners.

EOS

EOS is one such cryptocurrency which is among the top 10 cryptocurrencies even before the launch of its platform. In June 2017 EOS token was launched via an ICO. EOS 'network, which is scheduled to launch in June 2018, is intended to be a direct competitor to Ethereum and NEO.EOS was founded by Dan Larimer, who is also the creator of the Bitshares cryptocurrency exchange and blockchain-based blogging site Steemit. EOS is developing a network for developers to construct decentralized apps and smart contracts. In fact, it is one of the few cryptocurrencies which was least affected by the market crash which happened in 2018.

EOS will be much more robust than Ethereum, as it uses an advanced transaction verification method. It is currently able to execute 10,000-100,000 transactions per second. EOS has an incredibly experienced team with proven track record.

Cardano (ADA)

Cardano was founded in September 2017 by Charles Hoskinson, co-founder of the Ethereum. Cardano was also developed as a forum for decentralized apps and smart contracts, much like Ethereum. Like EOS, the distinction between Cardano and Ethereum lies in the technical advancements it has made over the technology of Ethereum. Cardano is considered to be the 3rd and most advanced blockchain technology generation yet, making it one of the top 10 cryptocurrencies of 2018.
Cardano is sponsored by an international group of global researchers and scientists who contribute to the growth of his blockchain. Cardano is much more robust, with a total capacity of 257 transactions per second, than Ethereum. Cardano aims to bring about interoperability which means it can communicate seamlessly with various cryptocurrencies and their infrastructures.

Litecoin (LTC)

Litecoin is based on an open source global payment network that is not controlled by any central authority and uses "scrypt" as a proof of work, which can be decoded with the help of CPUs of consumer grade. Although Litecoin is like Bitcoin in many ways, it has a faster block generation rate and hence offers a faster transaction confirmation. Other than developers, there are a growing number of merchants who accept Litecoin. As of June 2018, Litecoin has a market cap of $4.89 billion and on June 21, 2018, it closed at $96.7. Litecoin was created way back in 2011 by Charlie Lee, an ex-Google employee. It was built on the blockchain of Bitcoin itself, with the purpose of improving it.So, like Bitcoin, Litecoin is also just a digital currency and does not provide a platform for smart contracts.

Litecoin transactions take about 2.5 minutes, while a Bitcoin transaction takes about 10 minutes to complete. This is why it is called "Lite"coin. Average transaction fees for Litecoin are about $0.179 versus Bitcoin's $1.8.

Except for speed of transaction, there is no other offer from Litecoin that could significantly differentiate it from others. It is faced with rigid coin competition providing anonymity, smart contracts, and foreign payments, etc.

Stellar (XLM)

Jed McCaleb who is also the founder of Ripple founded Stellar in 2014. In reality, Ripple was hard forked into Stellar, and the Foundation for Stellar Creation was born. Like Ripple, Stellar also aims to make cross-border payments more successful. Stellar has been around since 2014 but it did not see much traction ‘til the end of Q1 2017. Its price grew from $0.0039 in April 2017 to $0.85 in January 2018. That’s a return of 21,694% in less than 9 months.

Contrast with its closest rival, Ripple, Stellar is more decentralized. Being also a non-profit, it inspires more faith than others. Stellar established strategic alliances with more than 30 banks as well as with organizations such as Deloitte and IBM.

IOTA

Founded in 2015, IOTA is among the top 10 cryptocurrencies the most unique coin. It is the only one to use a modern protocol innovation called 'Tangle' instead of blockchain Although IOTA was founded in 2015; it only launched its token on exchanges in 2017. It was an instant success as its price rose from $0.44 in June 2017 to $5.34 in December 2017, giving it a return of around 1.200 trillion. Like most other top 10 cryptocurrencies, IOTA also suffered a price drop earlier this year. It is currently going strong with a growth of about 150% in last one month with the market cap touching $6.61 billion.

The biggest advantage IOTA provides is zero transaction fees over all other cryptocurrencies. When all other cryptocurrencies struggle with the problems of scalability, IOTA's technology promises infinite scalability.

NEO

NEO is also referred to as the "Chinese Ethereum" due to the similarities in its deal to Ethereum's. It also provides a blockchain-based platform for Smart contract creation and ICO launch. NEO is able to complete 10,000 transactions per second as compared with Ethereum's 15 transactions. Although Ethereum only supports one programming language, NEO supports multiple languages such as C++, C#, Go, Java, making it one of programmers' favorites. It seems to enjoy the Chinese government's support which gives it a clear advantage in the Chinese and Asian masses market.

Zcash (ZEC)

Zcash, a decentralized and open-source cryptocurrency launched in the latter part of 2016, looks promising. “If Bitcoin is like http for money, Zcash is https," is how Zcash defines itself. Zcash offers privacy and selective transparency of transactions. Thus, like https, Zcash claims to provide extra security or privacy where all transactions are recorded and published on a blockchain, but details such as the sender, recipient, and amount remain private.

Dash (DASH)

Dash operates “Decentralized Governance by Blockchain” (The Dash Network 2017) which allows owners of Masternodes to make decisions, and provides a method for the platform to fund its own development. Dash is a more secretive version of Bitcoin. Dash offers more anonymity as it works on a decentralized master code network that makes transactions almost untraceably. Dash is overseen by a decentralized network of servers—known as “Masternodes” which alleviates the need for a third party governing body, and allows forfunctions such as financial privacy and instant transactions. On the other hand, users or “miners” in the network provide the computing power for basic functions such as sending and receiving currency, and the prevention of double spending. The advantage of utilizing Masternodes is that transactions can be confirmed almost in real time because Masternodes are separate from miners, and the two have non-overlapping functions.

Monero (XMR)

Monero (XMR) is a “secure, private, untraceable currency” centered around decentralization and scalability that was launched in April 2014. The currency itself is completely donation-based, community driven and based entirely on proof-of-work. Whilst transactions in the network are private by default, users can set their level of privacy allowing as much or as little access to their transactions as they wish [6]. Monero has been launched with a strong focus on decentralization and scalability, and enables complete privacy by using a special technique called ‘ring signatures.’ With this technique, there appears a group of cryptographic signatures including at least one real participant – but since they all appear valid, the real one cannot be isolated. It arguably holds some advantages over other Bitcoin-based cryptocurrencies such as having a dynamic block size, overcoming the problem of scalability, and being a disinflationary currency meaning that there will always exists an incentive to produce the Monero currency.

MaidSafeCoin

MaidSafeCoin is a digital currency which powers the peer-to-peer Secure Access For Everyone (SAFE) network, which combines the computing power of all its users, and can be thought of as a "crowd-sourced internet" calling themselves a 'crowd-sourced internet', you can provide space in your computer in exchange for coins. A number of decentralized apps now use the SAFE network to store data securely. As the currency is used to pay for services on the SAFE network, the currency will be recycled meaning that in theory the amount of MaidSafe coins will never be exhausted. The process of generating new currency is similar to other cryptocurrencies and in the case of the SAFE network it is known as "farming". Users contribute their computing power and storage space to the network and are rewarded with coins when the network accesses data from their store. The market cap for MaidSafeCoin is about $39 million. It is known for: being a security-centric data platform.

Lisk

Lisk is a crowd funded cryptocurrency, and a unique one – it brands itself as "the first modular cryptocurrency utilizing sidechains". Unlike other systems on this list, the Lisk system can be used by anyone to make their own decentralized apps in the programming language Javascript. As such, this currency has practical application value and can be used to create many types of 'dapps', including social media platform, e-commerce store, and many others. It currently has a market cap of around $25 million. It is known for: useful for programmers to make own 'dapps', the first to utilize sidechains.

Storjcoin X

Storj released Storjcoin X in July 2014. At its core, Storj a decentralized, open-sourced and encrypted cloud data storage which uses Storjcoin tokens to gain access and usage in the Storj network. The market cap as of mid-September is $8 million.

Dogecoin

Dogecoin (Dogecoin 2017) originated from a popular internet meme in December 2013. Created by an Australian brand and marketing specialist, and a programmer in Portland, Oregon, it initially started off as a joke currency but quickly gained traction. It is a variation on Litecoin, running on the cryptographic scrypt enabling similar advantages over Bitcoin such as faster transaction processing times. Part of the attraction of Dogecoin is its light-hearted culture and lower barriers to entry to investing in or acquiring cryptocurrencies. One of the most popular uses for Dogecoin is the tipping of others on the internet that create or share interesting content, and can be thought of as the next level up from a "like" on social media or an "upvote" on internet forums. This in part has arisen from the fact that it has now become too expensive to tip using Bitcoin.

Ether

Ether is the cryptocurrency for Ethereum, a decentralized platform that can execute peer-to-peer 'smart contacts'. As of September 2016 and as a result of an attack to The DAO, Ethereum was split into 2: Ethereum (ETH) and Ethereum Classic (ETC). Ethereum created by Vitalik Buterin and launched in mid-2015 after a successful crowdsale, this platform was marketed as the "next generation cryptocurrency and decentralized application platform" and has a market cap of $1.1 billion. Peer-to-peer smart contracts are what Ethereum is known for, aside from the cryptocurrency. It enables people to code and enact contracts without third parties. For example, this guide explains how you can set up a smart contract for a conference, where organizers can sell tickets, set a maximum number of attendees, and provide refunds automatically.

Tether

Tether is a virtual currency that is supposed to be tied — or tethered to the value of a dollar. Customers can buy Tether coins on Bitfinex and then transfer them to other virtual currency exchanges, providing a way to move dollars between countries without going through banks. Tether has also become a very popular way to buy Bitcoin.

Inorder to maintain accountability and to ensure stability in exchange price, we propose a method to maintain a one to one reserve ratio between a cryptocurrency token, called tethers, and its associated real world asset, fiat currency. This method uses the Bitcoin blockchain, Proof of Reserves, and other audit methods to prove that issued tokens are fully backed and reserved at all times.

Bitcoin Private (BTCP)

Bitcoin Private, a supposed “fork-merge” of Bitcoin and Zclassic, is intended to add privacy and spend ability to the Bitcoin blockchain while remaining cognizant of the challenges, choices, and failures of prior forks. To accomplish this, Bitcoin Private will use a larger block size (2 MB), a shorter block time (2.5 min), and an ASIC-resistant (GPU-friendly) proof-of-work (POW) algorithm for mining — Equihash.

The Bitcoin Private clients will support blockchain pruning and SPV techniques like Electrum in order to reduce the burden of the blockchain on user devices. To safeguard against replay attacks from Bitcoin and Zclassic, Bitcoin Private will feature two-way replay protection. Bitcoin Private is an amalgamation of two transaction systems transparent and shielded transactions.

Bitcoin Cash (BCH)

The creation of Bitcoin Cash is what is called a "hard fork." The creators are releasing completely new software that allows for eight times the number of transactions per block. This means Bitcoin Cash could process transactions faster. Bitcoin Cash is not worth the same as bitcoin. As of this writing, a unit of Bitcoin Cash is valued around $240, but one Bitcoin is worth more than $2,700.

Bitcoin Cash remodeled to allow for larger block sizes (≥8 MB vs 1 MB) to which reduce fees and increases transaction throughput. However, this did not come without tradeoffs — its price potential was damaged because of its lack of a fixed block-size and “fee market”.Its purpose was to solve the two main issues that had arisen with bitcoin as its popularity grew: slow transaction times and high fees.

Bitcoin Gold

Bitcoin Gold took another route, instead reducing the block time (2.5 min), switching the PoW algorithm to Equihash (ASIC resistant), and introducing an enhanced difficulty adjustment algorithm, which occurs every block.

The summary statistics for the raw exchange rates of the cryptocurrencies, shows simple reflection of the “worth” or value of each currency. It can clearly be seen that the exchange rate of Dogecoin is the least significant; the exchange rate is approximately $0.0002 USD to one Dogecoin. In contrast, being the most popular cryptocurrency, Bitcoin has the largest minimum, first quartile, median, mean, third quartile, and maximum values, which show its greater significance and higher “value” to those with a vested interest in cryptocurrencies. The exchange rates of all seven currencies are positively skewed, with Litecoin, Monero, and Ripple being the most skewed. In terms of kurtosis, MaidSafeCoin shows less peakedness than that of the normal distribution; Bitcoin, Dash, and Dogecoin show levels similar to the normal distribution; Litecoin, Monero, and Ripple have significantly greater peakedness than the normal distribution.

The exchange rates of Dogecoin, MaidSafeCoin, and Ripple have the smallest variances and standard deviations, indicating that their low volatility can perhaps be explained by the low values of the exchange rates coupled with the fact that their range and inter quartile ranges are very limited. On the other hand, Bitcoin, Dash, and Litecoin’s exchange rates show the greatest variance and standard deviation.

Figure 5: Dominant Cryptocurrencies

IV. CONSENSUS

Consensus Problem is a fundamental problem in fault-tolerant distributed systems. Consensus involves multiple servers agreeing on values. Once they reach a decision on a value, that decision is final. Consensus algorithm may refer to one of several proposed protocols for solving the consensus problem. Typical consensus algorithms, decision-making process, make progress when any majority of their servers is available. Blockchain consensus models are methods to create equality and fairness in the online world.

Traditional consensus approaches in distributed systems have focused on building fault tolerance in the face of unreliable systems provisioning mainly for fail-stop faults. Paxos, Raft and variants, view-stamped replication can be used for ordering transactions in distributed databases or to order client generated requests and respective state change in distributed applications using replicated state machines.

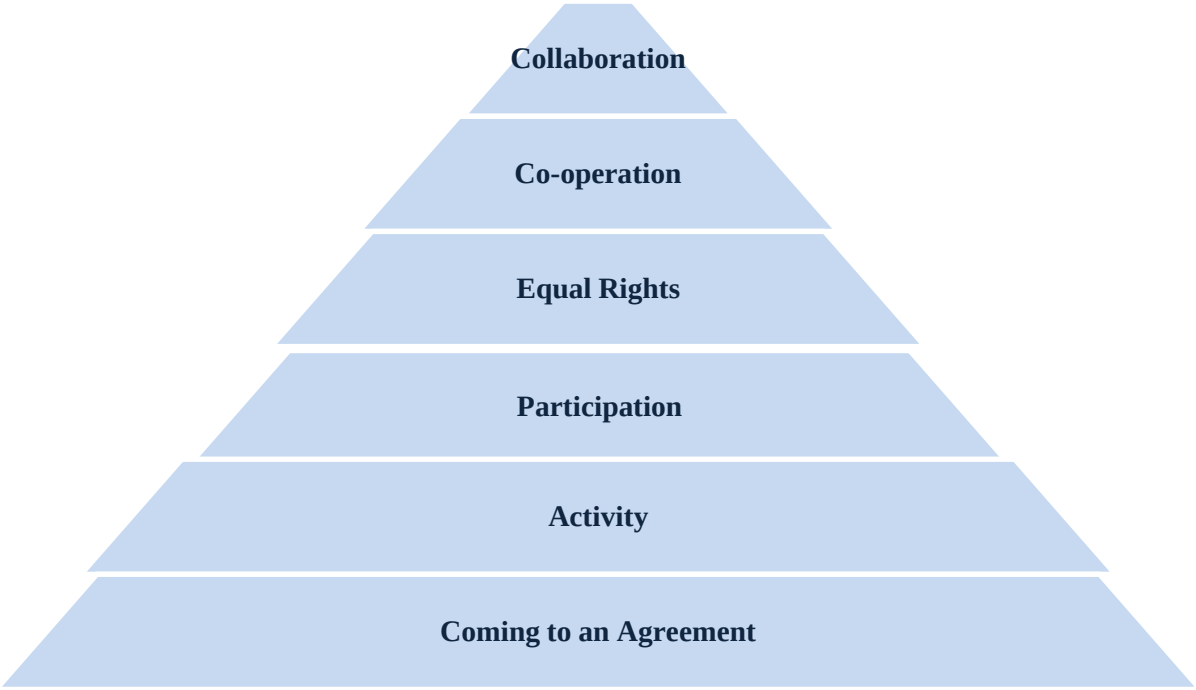

Figure 6: Objectives of Blockchain consensus models

Double spending problem means reusing the currency in two transactions at the same time. The traditional currency is the entity, so we will not face the problem of double spending while using traditional currency. We can also solve the double spending problem in the Internet transactions with the centralized trusted institutions. Blockchain solves this problem with the method of verifying the transactions by many distributed nodes together. Byzantine Generals Problem is the problem in the distributed system. The data can be delivered between different nodes through peer-to-peer communications. However, some nodes may be maliciously attacked, which will lead to the changes of communication contents. Normal nodes need to distinguish the information that has been tampered and obtain the consistent results with other normal nodes. This also needs the design of the corresponding consensus algorithm.

Byzantine Generals Problem is the problem in the distributed system. The data can be delivered between different nodes through peer-to-peer communication. However, some nodes may be maliciously attacked, which will add to the changes of communication contents. Normal nodes need to distinguish the information that has been tampered and obtain the consistent results with other normal nodes. This also needs the design of the corresponding consensus algorithm.

The principal issue with Byzantine is finding an agreement. If even a there is one mistake, nodes can't come to an understanding. On the other hand, Consensus algorithms don't really face this type of problem. Their primary target is to reach a specific goal by any means. The Blockchain consensus models are much more reliable and fault tolerant than Byzantine.

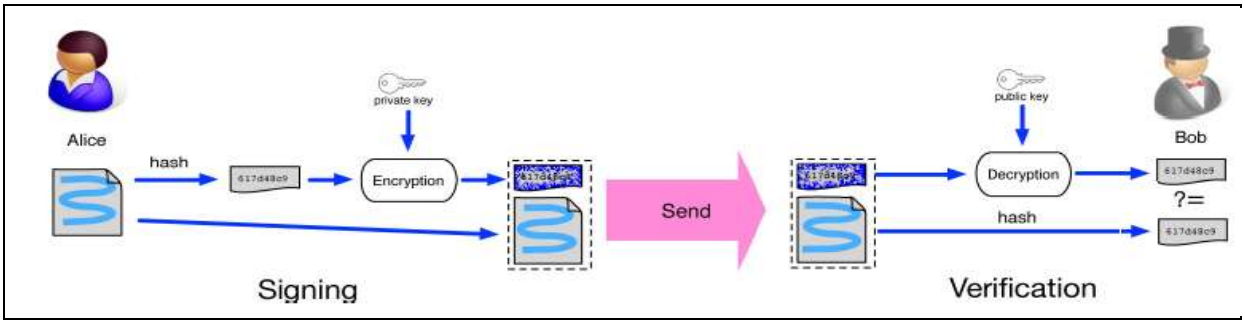

Figure 7: Digital Signature used in Blockchain [33]

Every user possesses a pair of private and public key. The transactions are signed using the private key. Digital signed transactions are distributed across the entire network and are then accessible by public keys, which are available to all on the network. An example of digital signature used in blockchain is shown in Figure 3.1. A user Alice then has to sign a contract, producing a hash value extracted from the contract. She then encrypts the hash value using her private key and sends the authenticated hash with the original data to another user Bob. Bob verifies the transaction obtained by comparing the decrypted hash (using Alice's (public key) to the hash value derived from the data provided by the same hash function as Alice's. Typical digital signature algorithms used in blockchains include digital signature algorithm.

Consensus Algorithms

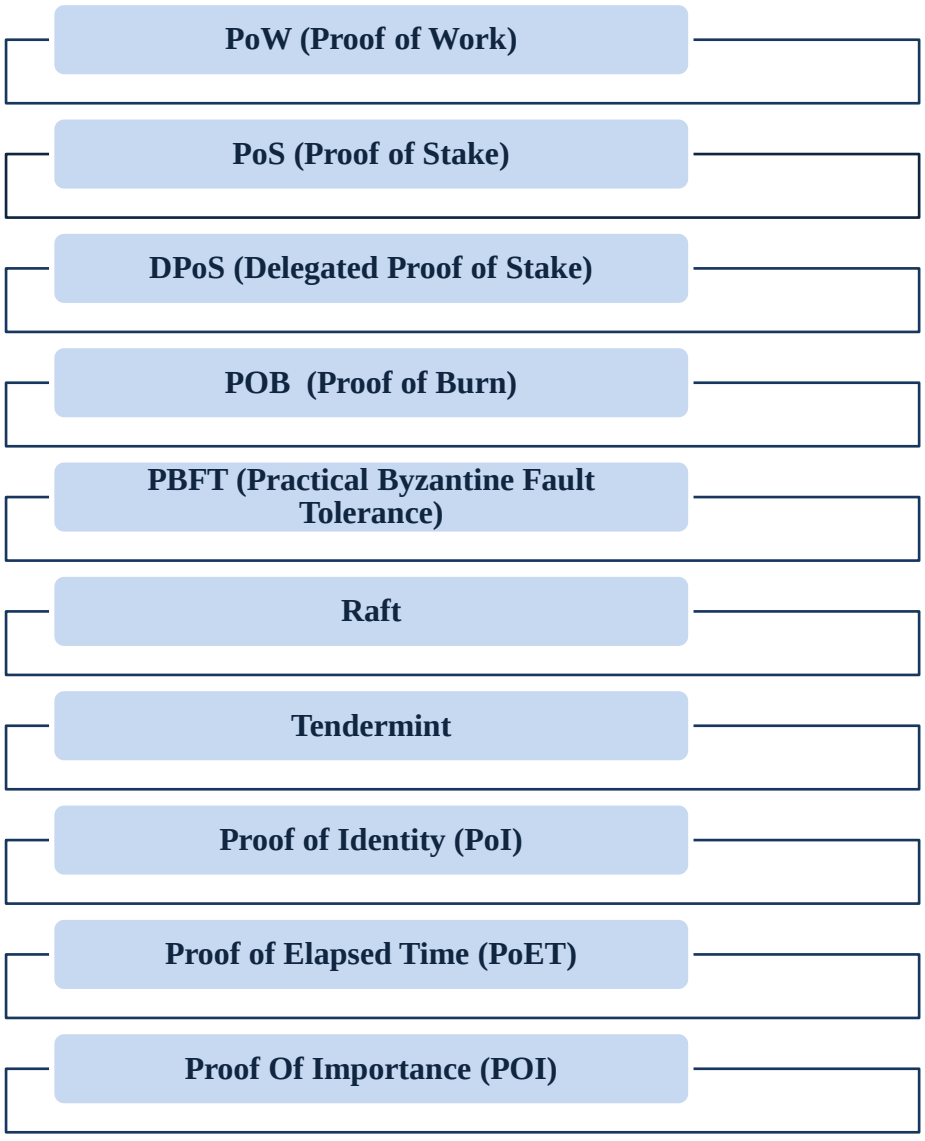

Figure 8: Consensus Algorithms

PoW (Proof of Work)

In a decentralized network, somebody has to be chosen in a decentralized network to monitor the transactions. The best way is by random picking. Random selection, however, is vulnerable to attacks. So if a node decides to publish a block of transactions, it has to do a lot of computing to show that the node is not going to attack the network.

A distributed system broadcast transactions to all the nodes in the network. Its core idea is to allocate the accounting rights and rewards through the hashing power competition among the nodes. Each node collect the new transactions into a block, and then works on finding a difficult "Proof-of-Work" for its block, which is called the "mining" process i.e., execute a CPU intensive computation that takes time to solve, but can be verified quickly. Based on the information of the previous block, the different nodes calculate the specific solution of a mathematical problem. It's difficult to solve the math problem. Basically, each network node calculates the Block Header hash value. The block header contains a nonce, and the miners will often change the nonce to get different hash values. The agreement requires the estimated value to be equal to, or less than, a given value. The consensus requires that the calculated value must be equal to or smaller than a certain given value. The mining process involves scanning for a value when it is hashed with SHA-256, and the result begins with a number of zero bits.

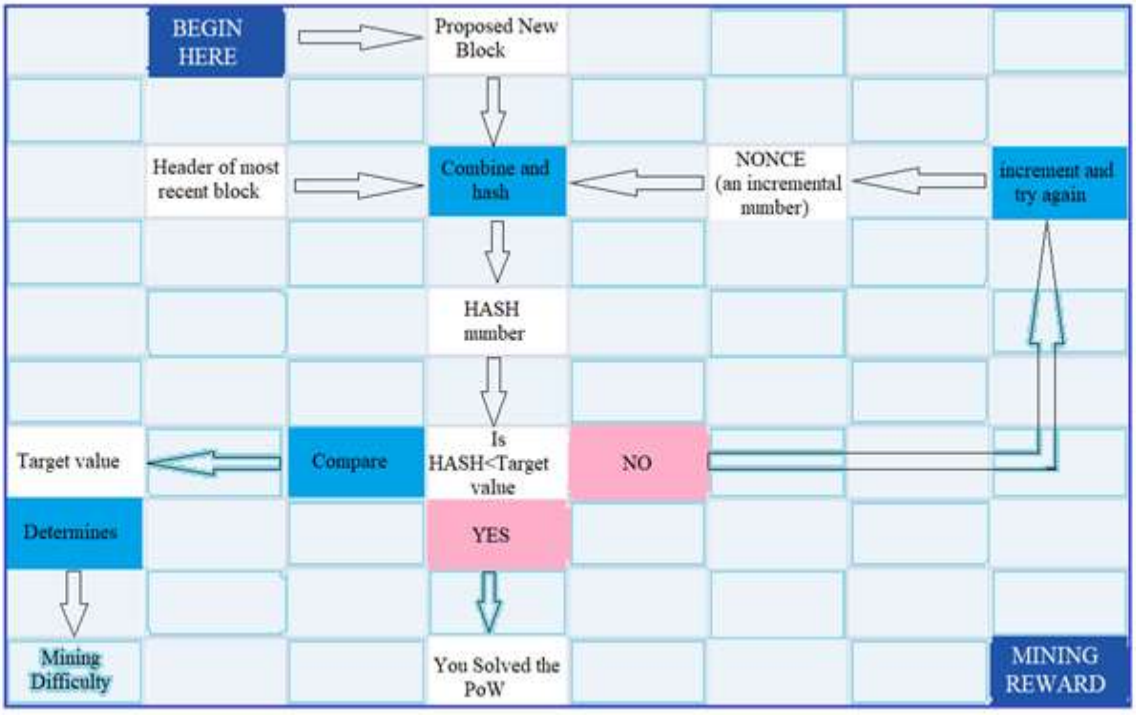

Figure 9: Proof of Work

PoS(Proof of Stake)

The earliest application of PoS is PPCoin. In PoS, the digital currency has the concept of coin age. Coin age of a coin is its value multiplied by the time period after it was created. The longer one node holds the coins, the more rights it can get in the network. Holders of the coins will also receive a certain reward according to the coin age. The proof hash is a composed hash value of the weight factor, the unspent output value and the fuzzy sum of current time. PoS limit the hashing power of each node. The difficulty of mining is inversely proportional to coin age.

PoS encourage the coins holders to increase the holding time. With the concept of coin age, the blockchain is no longer entirely relying on the proof of work. That effectively solves the resource wasting problem in PoW. The security of the blockchain using PoS improves with the increasing value in the blockchain. The attackers need to accumulate a large number of coins and hold them long enough to attack the blockchain. This also greatly increases the difficulty of attack.

DPoS(Delegated Proof of Stake)

In the initial design stage of bitcoin, Satoshi Nakamoto hoped that all the participants can use the CPU to mine. So the hashing power can match the nodes and each node has the opportunity to participate in the decision-making of the blockchain. With the development of technology and the appreciation of bitcoin, the machines that are specially designed for mining are invented. The hashing power is grouped in the

participants that have large numbers of mining machines. The ordinary miners rarely have the opportunity to create a block.

POB – (Proof of Burn)

Value of one digital currency can then be exchanged through the Proof of Burn (PoB) mechanism into the next. This implies that a node takes part in a lottery to determine the status of the blockchain by burning value that they hold as of now, as another cryptographic currency, such as bitcoin or ether. The node transfers bitcoin, ether or some other digital currency to an unspent address, in order to locate the following block. In addition, in the local coins the node gets a credit for the Blockchain that it helps to maintain. The key Blockchain to implement the PoB system for mining effectively was Slimcoin. Its system consolidates Proof of Burn with PoW and PoS, making it the first cryptocurrency to join three consensus mechanisms. The Blockchain is the primary database of cryptocurrency that holds all transaction-related information efficiently, verifiably and permanently. It is digitized and decentralized. Once registered, the data in any given block cannot be modified retroactively unless all subsequent blocks are altered which requires the cooperation of the network majority.

PBFT(Practical Byzantine Fault Tolerance)

One of the most well-established BFT algorithms is The Functional Byzantine Fault Tolerance (PBFT). Specially, it rests on three rounds of message exchange until consensus is reached. This ensures that 3f+1 node are always able to achieve consensus in the presence of f Byzantine nodes; this is proved to be optimal. PBFT (Practical Byzantine Fault Tolerance) is an algorithm for the replication of Byzantine Faults. As PBFT could accommodate up to 1/3 of malicious byzantine replicas, Hyperledger Fabric uses the PBFT as its consensus algorithm. In a round a new block is found. According to certain rules a primary will be selected in every round.

Raft

After the Byzantine Generals Problem was raised, Lamport proposed Paxos algorithm
to solve the consistency problem in certain conditions in 1990. But because the content of the paper is difficult to understand, it was not accepted. The Paxos was briefly reintroduced in 2001. Then Paxos occupies the dominant position in the field of consistency algorithm. Many other algorithms are derived from it. But Paxos algorithm is too theoretical. The people have great difficulty in understanding it and engineering implementation. In 2013, Standford's Ongaro and others published the paper and proposed Raft algorithm. Raft achieves the same effect as Paxos and is more convenient in engineering implementation and understanding.

Tendermint

Tendermint is a consensus algorithm of Byzantine origin. In a round a new block is found. In this round, a proposer will be selected to broadcast a non-confirmed block. It Can be divided into three steps: 1) Predict phase. Validators tend to show a prediction for the block being proposed. 2) Phase by precommit. If the node on the proposed block has earned more than 2/3 of the prevotes, it will broadcast a precommit for that block. If the node received in excess of 2/3 of precommits, it will enter the commit stage. 3) Move on the commit.. The node validates the block and a commit for that block is transmitted. When the node has received 2/3 of the commits, the block is acknowledged. Unlike PBFT, nodes are expected to lock their coins to become validator. If a validator is found to be deceptive, penalty will apply.

Proof of Identity (PoI)

It's a cryptographic proof (data piece) that says every user knows a private key that correlates with an accepted identity and is cryptographically attached to a specific transaction. Any person in any community may construct a PoF (only a data block) and present it to everyone in the processing node for example.

With POI, the dependency is neither on the amount of 'work' nor the amount of 'stake' you hold. POI, as an algorithm, takes a more holistic approach to considering the overall productivity of a user in the network. The reward, as per POI approach, should be based on the contribution of a user to the network in all

capacities. The staking of the block, therefore, is based on multiple factors including reputation, overall balance, and the number of transactions done through or from a particular address. Through these factors, the network determines how 'useful' the member is to the network.

Proof of Elapsed Time (PoET)

Endeavor to guide the issue of PoS through arbitrary determination of members proposing blocks is required to ensure that each member has a fair opportunity to propose a block and thus to yield prevailing benefits. With that, each member asks for a hold-up time from their reliable local enclave. The member with the briefest hold-up period is next to deliver a block for the allotted waiting time after it has held-up. Will privately trusted enclave signs the potential and the outcome so that other members can confirm the waiting period has not been misled by any. All things considered, the people broadcasting PoET have asserted that it fits the PoS qualities.

The POET network consensus mechanism needs to ensure two important factors. First, that the participating nodes honestly choose a time which is indeed random and not a shorter period selected by the participants to win, and two, the winner has indeed completed the waiting time.

Proof of Importance (POI)

The last deviation from the consensus mechanisms is the Proof of Importance (PoI). The primary forum for executing this cryptographic money was NEM. With PoI it is not just the worth of the coin balance. NEM's consensus network relies not only on the number of coins but also on the prospect of remuneration for successful system action. The chances of staking a block are a component of different variables, including popularity, balance and the amount of transactions made to and from that position. This offers a more all-embracing picture of a member of the 'helpful' network. These are selected using a complex algorithm, not simply by the probability and size of their shares. Likewise, they stream into the process their importance for the system and the value the system obviously has for them. Recognition of false usage and deceptive models is obviously included in this concept to stop Sammy members having a higher score.

Attributes of Consensus Algorithm

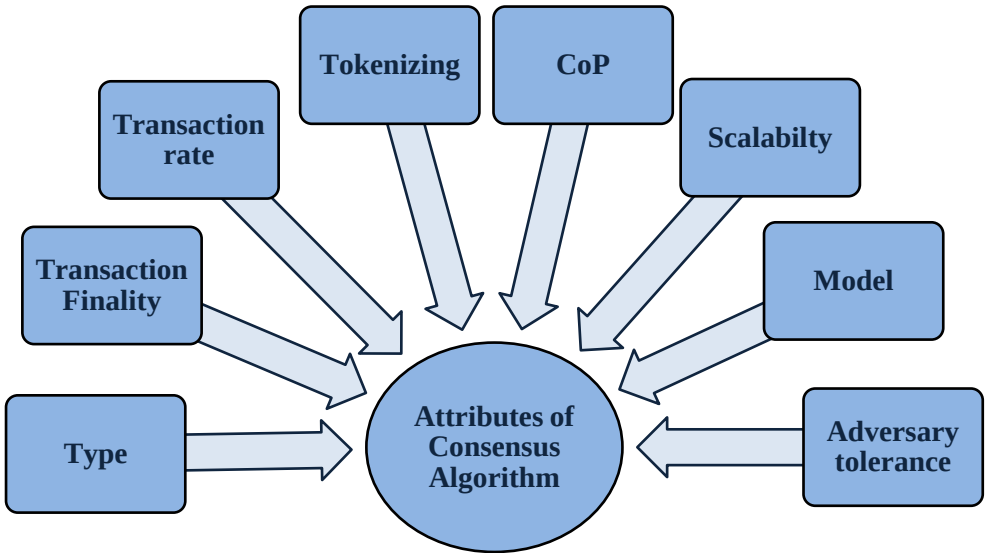

Figure 10: Attributes of Consensus Algorithm

Consensus Properties

The research on consensus has extensively been studied in distributed systems to be resilient to node failures, partitioning of the network, message delays, messages out-of-order or missing, and compromised messages. Consensus mechanisms need to deal with selfish, unreliable, or malicious nodes in the

Blockchain sense, and ensure that all nodes in the network agree on a clear global state. Any agreement on Blockchain seeks to answer three main properties on which its applicability and effectiveness can be calculated.

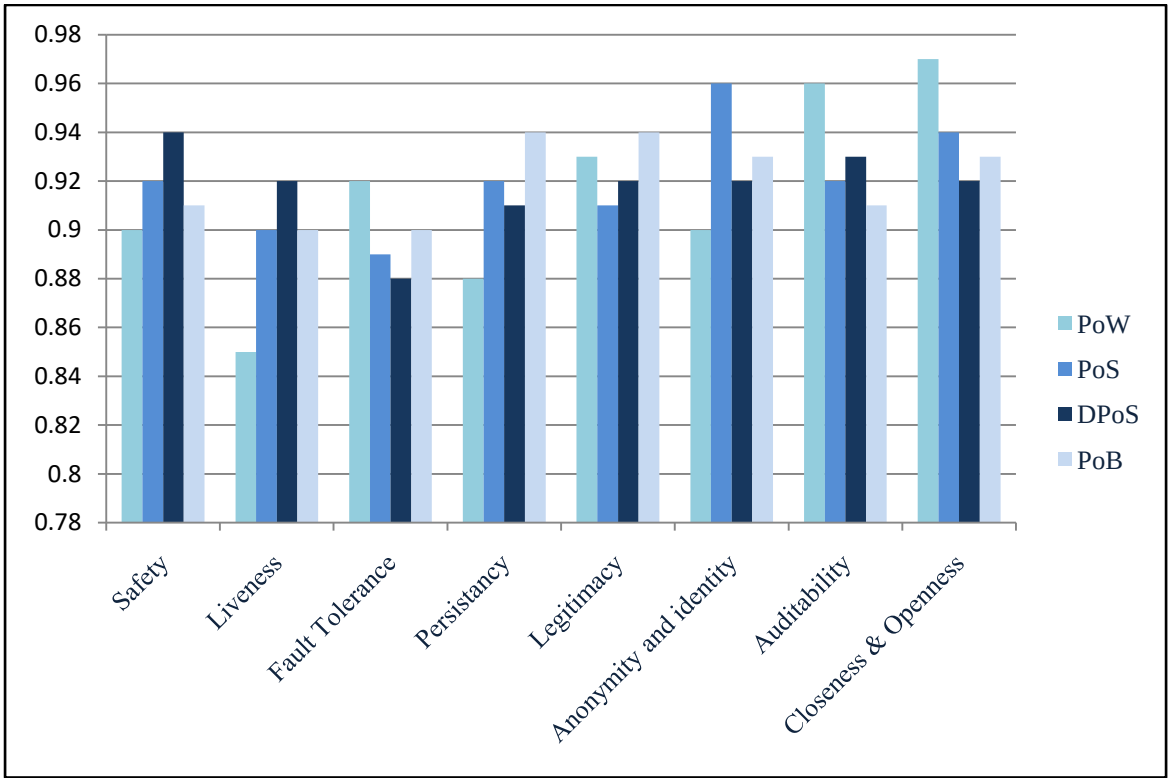

Figure 11: Consensus Properties

1. Safety: Safety property guarantees that something bad will never happen. It corresponds to validity and agreement properties in the traditional consensuses appeared in distributed systems. Validity is defined as if some correct processes propose the same value v, then any correct process that decides, decides v. Agreement ensures that no two correct processes decide differently. Generally, a consensus mechanism is safe if at least one honest node produces a valid output then all other nodes produce or receive the same output. The results are valid and identical to all nodes, referring as consistency of the share state.

2. Liveness: Liveness guarantees that something good will happen eventually. This is also known as termination in the traditional consensus in distributed systems stating that every correct process eventually decides on a value. A consensus mechanism ensures liveness if all benign nodes participating in a consensus eventually produce a value and all correct requests will be eventually processed. There is no bound on the time it takes to decide on a value, such that this property does not require every node to have an identical state at a given point of time.

3. Fault Tolerance: A consensus mechanism provides fault tolerance if it is resilient (operate correctly) from failures of some nodes participating in a consensus at any point. As long as faulty nodes are limited, the correct consensus is still being reached. The failure of nodes exhibits in two categories. Fail-stop or crash-failure deals with nodes that stop to process temporarily or permanently in emitting or receiving messages, or participating in the consensus protocol. Byzantine failures on the other hand deal with malicious nodes that are specially crafted to defeat properties of a consensus protocol.

4. Persistency: Transactions recorded in a Blockchain ledger is considered persistent as they spread across the network, where each node maintains and controls its records. As long as the majority of nodes are benign, persistency is persistently retained. Several properties are derived from this characteristic including transparency, and immutability (temper resistance). This transparency and immutability mean that Blockchains are auditable.

5. Validity: Unlike some distributed systems, Blockchains do not require executions from each node. Transactions, or blocks, broadcasted in a Blockchain should make other nodes checked. And it could quickly detect some falsification. This system consists of three major roles: (1) proposers who propose a value, (2) acceptors who validate and decide which value to be taken and (2) learners who accept on the chose value.

6. Anonymity and Identity: Anonymity is the main characteristic of public Blockchains. Identity in this system can be untied to a user real-world identity. One user can obtain multiple identities to avoid identity exposure. There is no need for any central entity to maintain private information. As a result, according to the transaction information, the real-world identity cannot be obtained, preserving a certain amount of privacy. On the other hand, identity is usually required in the systems that are operated and governed by known entities in the settings like private and permissioned Blockchains.

7. Auditability. Record timestamp and persistent information allow ones to easily verify and trace previous records through nodes in a Blockchain network. The degree of auditability depends on types of Blockchain systems and their implementations. Private Blockchains are the least auditable as nodes are administrated by one entity; permissioned Blockchains come second in which some agreements, such as encrypted data, may prevent information to be fully auditable, and public Blockchains are the highest as nodes are truly decentralized.

8. Closedness and Openness: Opened Blockchains rely on public nodes to maintain records of transactions. Therefore, anyone can publish a transaction and join the system by following a set of rules and information inside this Blockchain is public. Permissioned Blockchains are considered semi-opened as nodes are pre-specified or validated before joining.

V. BLOCKCHAIN ECO-SYSTEM

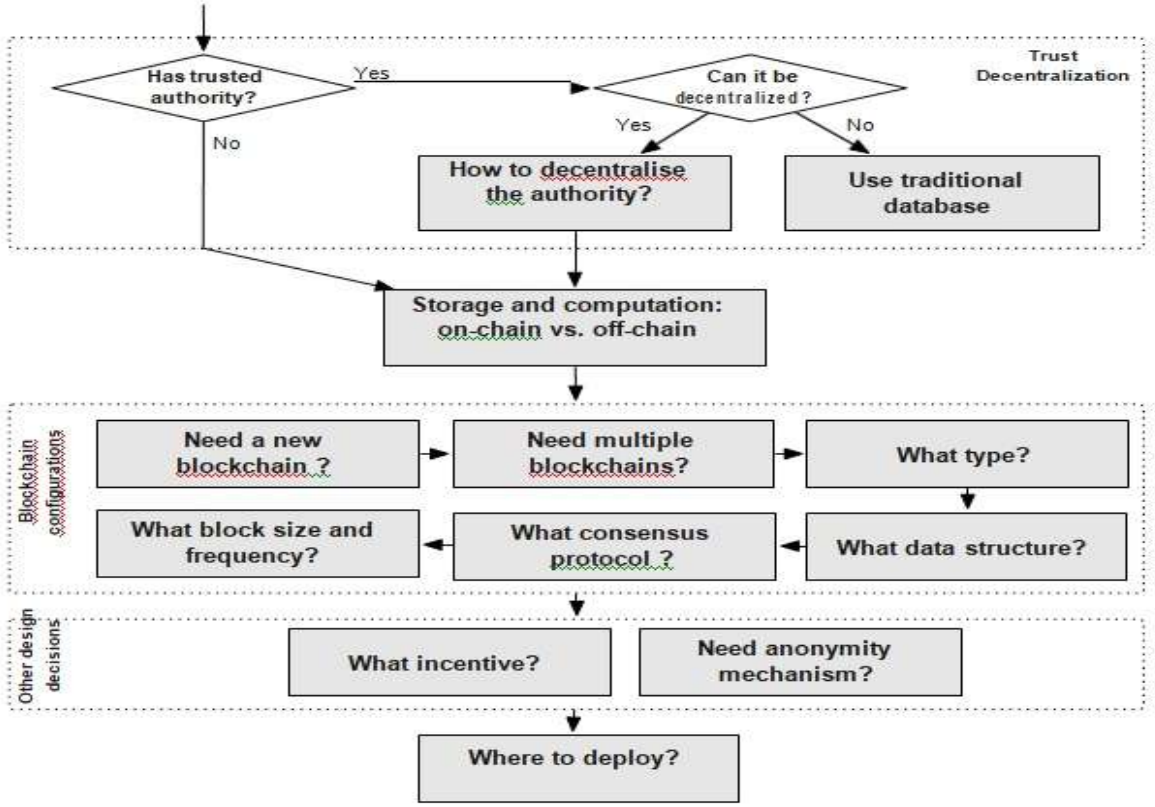

Figure12: The Blockchain eco-system [21]

The Design Process for Blockchain eco-framework Taxonomy can be utilized amid the procedure of architecting programming frameworks to manage the framework structure. In this segment, we talked about a demonstrative calculated model of architecting a framework that possibly utilizes blockchain

innovation. The procedure is utilized to outline how a blockchain system structure can be regulated at different phases of the planned procedure.

A blockchain is used in situations where no single professional is needed and the expert believed could be decentralized. Structure choices with respect to believe decentralization are talked about. From that point forward, a gathering of plan choices around blockchain configuration should be made, similar to the sort of blockchain, agreement convention, square size and recurrence. The structure choices on blockchain configuration are examined.

A few choices fundamentally affect adaptability (like square size and recurrence), security (like accord convention), cost efficiency (like kind of blockchain) and execution (like information structure). There are additionally exchange offs between the key properties of blockchain. At last, where to convey the modules of the blockchain-based framework is additionally vital. This plan procedure, our scientific classification can help the basic leadership through empowering an orderly correlation among the capacities of different structure choices. The scientific classification additionally demonstrates the effect of different plan alternatives on the quality characteristics. The exchange off examination of value characteristics gives an establishment to the correlation.

Architectural Design Challenges

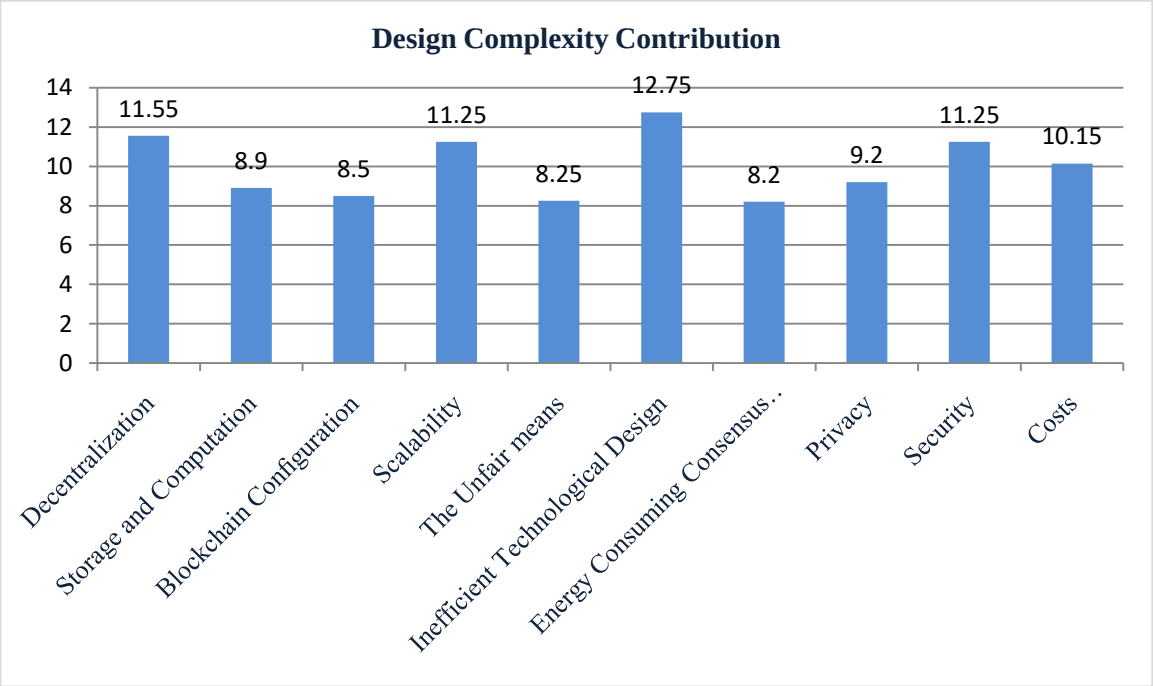

Figure 13: Design Complexity Contribution

1. **Decentralization:** Decentralization declines duty and ability from a focal area or specialist. In a brought together framework, all clients depend on a focal expert to intervene exchanges. For instance in a bank, clients depend on the bank's frameworks to accurately change their record adjusts after a bank exchange. A focal expert can control the entire framework, including by straightforwardly refreshing backend databases, or by redesigning the product that actualizes the framework. In this manner, a focal expert is a solitary purpose of disappointment for a brought together framework. Interestingly, a completely decentralized money framework like Bitcoin enables individuals to achieve concurrence on who claims what without confiding in one another or a different outsider. Such a framework is exceptionally accessible since each full hub in Bitcoin organize downloads each square and exchange, checks them against Bitcoin's center agreement governs and gives the expected usefulness to process exchanges. There are right now 5000+ hubs in the Bitcoin arrange, in spite of the fact that not all are full hubs that structure the foundation of Bitcoin.

2. **Storage and Computation:** While blockchains give some one of kind properties, the measure of computational power and information storage room accessible on a blockchain arrange stays restricted.

Likewise, utilizing open blockchains costs genuine cash, with an unexpected sort of cost model in comparison to traditional programming frameworks. Concerning cost proficiency, execution, and flexibility, real structure choices in utilizing a blockchain incorporate picking what information and calculation ought to be set on-chain and what ought to be

3. **Blockchain Configuration**: When utilizing a blockchain, one structure choice is the extension, for example regardless of whether to utilize an open blockchain, consortium/network blockchain or private blockchain. Most advanced monetary forms utilize open blockchains, which can be gotten to by anybody on the Internet. Utilizing an open blockchain results in better data straight forwardness and audit ability. In an open blockchain, information security depends on encryption or cryptographic hashes. A consortium blockchain is utilized over various associations. The accord procedure in a consortium blockchain is constrained by pre-approved hubs. The directly to peruse the blockchain might be open or might be confined to specific members. In a private blockchain arrange, compose consent is kept inside one association, in spite of the fact that this may incorporate different divisions of a solitary association. In the case of utilizing a consortium blockchain, private blockchain or permissioned open blockchain, an authorization the board segment will be required to authorize members inside the system. Private blockchains are the most pliable for ordering in light of the fact that the system is administered and facilitated by a solitary association. Numerous blockchain stages bolster arrangement as consortium blockchains or private blockchains,

4. **Scalability:** Blockchains are experiencing difficulty viably supporting countless on that machine. Both Bitcoin and Ethereum, the major blockchain systems, experienced modest rates of exchange and higher charges per exchange due to a large rise in clients. While this reality has prompted top to bottom research about how to help both these systems, and blockchains all in all, proportional, the discussions around the recommendations are exceptionally changed and are probably going to take a lot of time. Also, scaling techniques should be confirmed and altogether screened before execution into the records. Versatility concerns must be successfully tended to before the blockchain can be embraced on a wide scale.

5. **The Unfair methods:** Since its dispatch, bitcoin has for some time been related with the shadowy dealings of the underground market and the dim web. Since this is the main communication of the general population with blockchain innovation, this association has persevered with bitcoin, altcoins, and the tech basic it also. A portion of the scientists have found that digital currencies are being used by crooks to facilitate purchases of restricted products at online shopping centres, as an apparatus for illegal tax avoidance, just as installment techniques for ransomware. While these exercises are illicit, they are an aftereffect of individuals' uses of computerized monetary standards and can be done with fiat money as well. In any case, for blockchain innovation to be acknowledged by the general population, it must shake this shadowy affiliation.

6. **Inefficient Technological Design:** The Ethereum shrewd contract stage enables engineers to send their own decentralized applications (DApps) for a changed exhibit of employments. Although bitcoin is the main digital currency, organization of the Ethereum enables clients to trade the blockchain's ability for genuine applications. In any case,, look into has demonstrated that a considerable number of brilliant contracts conveyed on the stage have vulnerabilities because of their coding. In addition, the Bitcoin arrange is intended to incorporate a lot of information with every exchange. While a portion of this data is critical, not every last bit of it is fundamental. This makes the Bitcoin blockchain substantial and rather moderate. The architecture of blockchains needs to be simplified and enhanced to reduce these unnecessary aspects

7. **Energy Consuming Consensus Mechanisms:** Most blockchains use proof of work (PoW) to achieve agreement. PoW involves making use of a machine's computational power to unravel complex scientific conditions in order to validate an exchange and add it to a square. While this device, as shown in the Bitcoin structure, works admirably, it absorbs a lot of vitality. It has been accounted for that the excavators working to allow transactions in the Bitcoin network have been credited for investing about 0.2 percent of the world's power all year round. This is the equivalent to what the Bulgarian nation is devours. Additionally, going on the flow pattern it is being estimated that, by 2020, the Bitcoin network will need more power than is currently needed by the entire world. And latest worldwide concerns vitality creation and utilization, blockchains should utilize different techniques to accomplish agreement,

for example, the evidence of-stake calculation which requires substantially less vitality. This will enable the innovation to be coordinated into a future, which is progressively aware of vitality matters.

8. **Privacy:** The Bitcoin blockchain is intended to be self-evident. All information relating to an exchange is available for anybody to see. Except for security driven coins, this is the equivalent with a significant number of the blockchains as of now in presence. While this element might be critical in a few settings, it turns into an obligation whenever disseminated records are to be utilized in delicate situations. For example, private patient information ought to be accessible for all just like the case with exclusive business information. This is likewise appropriate to government information or money related information. For blockchain innovation to be received on a wide scale, the records should be modified so as to restrict access to the information contained in that to just the individuals who have the vital freedom.

9. **Security:** While massive blockchain networks are very unlikely to happen, blockchains are defenseless against an attack of 51 per cent. This alludes to a situation in which a mine worker or a group of diggers inappropriately regulates of 50 percent mining control. In such a situation, the diggers would most likely control the claims of new exchanges, particularly those made by various mineworkers. These will also almost definitely revolve around the exchanges these supported and in these way twofold spoken tokens to invest. Although the controlling excavators would not be able to alter old obstacles, this would significantly affect the token's respectability with the affected blockchain and it would need to recuperate in the open eye. Luckily, the likelihood of this assault is diminished as more individuals partake in the system as diggers.

10. **Costs:** Blockchain innovation is a powerful device for decreasing expenses. It diminishes the charges related with exchanging esteem and can streamline operational procedures. Be that as it may, in light of the fact that it is a generally new advancement, it is hard to incorporate it with heritage frameworks. Such a procedure would definitely be a expensive topic that many businesses and governments are hesitant to accept.

VI. CONCLUSION AND FUTURE SCOPE

Blockchain has shown its promise in academia and industry. This paper gives a brief investigation of blockchain mining techniques used by general blockchain applications including different crypto currencies. This swotting will help us to model a new optimized blockchain mining architecture which would incorporate all common parameters as well as differences among the existing architectures. The newly designed architecture can be analyzed and implemented be implemented for validation.

With regard to four fields, we are addressing potential future directions: blockchain research, halt the trend toward centralization, big data analytics and blockchain implementation.

A. Blockchain testing

Recently different forms of blockchains are emerging and up to now more than 700 cryptocurrencies are listed in. Some developers, however, could falsify their output on blockchain to draw investors motivated by the huge benefit. In addition, when users want to integrate blockchain into business they need to know which blockchain suits their needs.

Blockchain testing may be split into two phases: Phase of standardization and Phase of testing. All requirements must be made and accepted in the standardization process. When a blockchain is born, it could be checked if the blockchain works fine as developers says, with the agreed criteria. As for the process of testing, blockchain testing must be carried out with specific requirements.

B. Stop the tendency to centralization

Blockchain is developed as a framework of decentralization. However, there is a pattern that the miners in the mining pool are concentrated. Up to now, the top 5 mining pools together hold more than 51 per cent of the Bitcoin network's total hash capacity. In addition, egotistical mining strategy showed that pools with more than 25 percent of total computing power could produce more revenue than fair share it would draw moral miners into the selfish pool and finally the pool could easily reach 51 percent of the total capacity. Since the blockchain is not meant to support a few organizations, some methods of solving this problem should be proposed.

C. Big Data Analytics Blockchain could combine well with big data. We have classified the mix here approximately into two types: data management and data analytics. As for data storage, blockchain may

be used as it is distributed and safe to store important data. Blockchain would also be able to ensure the data is original.

D. Blockchain applications

Many blockchains are currently being used in the financial domain, and there are more and more applications emerging for various fields. Traditional industries may consider blockchain and apply blockchain to their fields to enhance their systems. A smart contract is a computerized transaction protocol enforcing contract terms. It's been long suggested, and now this concept can be implemented with blockchain. In blockchain, smart contract is a code fragment that could be executed by miners automatically. Smart contract has transformative potential in various fields like financial services and IOT.

REFERENCES

[1] Guojun Wang, Bebo White,Roger Leslie Cottrell SaqibAli, ""A Blockchain-based Decentralized Data Storage and Access Framework for PingER"," in *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications*, New York, NY, 1-3 Aug. 2018 2018, pp. 1303-1308.

[2] N. Malik, S. P. Mohanty, E. Kougianos and G. Das D. Puthal, ""Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems,""*IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 6-14, July 2018.

[3] O. Nathan and A. '. Pentland G. Zyskind, ""Decentralizing Privacy: Using Blockchain to Protect Personal Data,""*IEEE Security and Privacy Workshops,* pp. 180-184, 20 July 2015.

[4] Hong-Ning Dai,Xiangping Chen Zibin Zheng and Shaoan Xie, "Blockchain challenges and opportunities: a survey,"*Int. J. Web and Grid Services*, vol. 14, no. 4, pp. 352-372, 2018.

[5] Shuai Wang et al., "An Overview of Smart Contract: Architecture, Applications, and Future Trends,"*2018 IEEE Intelligent Vehicles Symposium (IV)*, pp. 108-113, October 2018.

[6] Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system,"*PDF* , October 31 2008, http://bitcoin.org/bitcoin.pdf.

[7] N. Malik, S. P. Mohanty, E. Kougianos and C. Yang D. Puthal, ""The Blockchain as a Decentralized Security Framework [Future Directions],""*IEEE Consumer Electronics Magazine*, vol. 7, no. 2, pp. 18-21, March 2018.

[8] B. Ye, L. Qu, Y. Wang, M. A. Orgun and L. Li, J. Zou, ""A Proof-of-Trust Consensus Protocol for Enhancing Accountability in Crowdsourcing Services,""*IEEE Transactions on Services Computing*, April 2018.

[9] Omar University of Texas Badreddin, "Powering Software Sustainability with Blockchain,"*Proceeding CASCON '18 Proceedings of the 28th Annual International Conference on Computer Science and Software Engineering*, pp. 315-322, October 2018.

[10] HaraldVranken, "Sustainability of bitcoin and blockchains,"*Current Opinion in Environmental Sustainability*, vol. 28, pp. 1-9, October 2017.

[11] S. Xie, H. Dai, X. Chen and H. Wang Z. Zheng, ""An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,""*IEEE International Congress on Big Data (BigData Congress)*, pp. 557-564, 11 Spetember 2017.

[12] BenediktNotheisena, TimmTeubner Florian Hawlitscheka, "The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy,"*Electronic Commerce Research and Applications (ELSEVIER)*, vol. 29, pp. 50-63, May-June 2018.

[13] MarkoVukoli´c Jo˜ao Sousa and AlyssonBessani, "A Byzantine Fault-Tolerant Ordering Service for the,"*2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 51-58, July 2018.

[14] F. Wessling and V Gruhn, ""Engineering Software Architectures of Blockchain-Oriented Applications,""*IEEE International Conference on Software Architecture Companion (ICSA-C)*, pp. 45-46, 2018.

[15] SandeepKumar E,ChhaganLal, SushmitaRuj Mauro Conti, "A Survey on Security and Privacy Issues of Bitcoin,"*IEEE Communications Surveys and Tutorials*, vol. 20, no. 4, pp. 3416 - 3452, 2018.

[16] ChianTechapanupreeda Pinyaphat asatanattakool, ""Blockchain: Challenges and Applications"*Open Science Journal of Electrical and Electronic Engineering*, vol. 5, no. 4, pp. 30-43, 2018.

[17] ArthurGervais Karl Wust, "" Do you need a Blockchain?","*2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pp. 45-54, November 2018.

[18] Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen Xiaoqi Li, "A Survey on the Security of Blockchain Systems,"*Future Generation Computer Systems*, Feb 2018.

[19] Y. Yuan and F. Wang, ""Blockchain and Cryptocurrencies: Model, Techniques, and Applications,""*IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1421-1428, Spetember 2018.

[20] Steven R. Weller, FengjiLuo, Junhua Zhao, and Zhao Yang Dong Gaoqi Liang, "Distributed Blockchain-Based Data Protection Framework for Modern Power Systems against Cyber Attacks,"*IEEE Transactions on Smart Grid (Early Access)*, pp. 1-1, March 2018.

[21] Xiwei Xu et al., "A Taxonomy of Blockchain-Based Systems for Architecture Design,"*2017 IEEE International Conference on Software Architecture (ICSA)*, pp. 243-252, May 2017.

[22] Wenchao Liu1, Qian Wang2, Gang Qu2, and Zhenglin Liu1 Zhaojun Lu1, "A Privacy-preserving Trust Model based on Blockchain for VANETs,"*IEEE Access*, vol. 4, 2018.

[23] Antonopoulos Andreas M, ""Mastering Bitcoin","*BOOK*, vol. ISBN: 978-1-449-37404-4, 2014 December.

[24] Pagnotta and Andrea Buraschiy EmilianoS, "An Equilibrium Valuation of Bitcoin and Decentralized Network Assets,"*SSRN´s eLibrary*, March 2018.

[25] Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts,"*2016 IEEE Symposium on Security and Privacy (SP)*, pp. 839-858, August 2016.

[26] JesperBuus Nielsen (Eds.) Jean-SébastienCoron, "Advances in Cryptology – EUROCRYPT 2017,"*Book(Springer)*, vol. ISSN 0302-9743,ISSN 1611-3349,ISBN 978-3-319-56613-9, ISBN 978-3-319-56614-6, April 30 – May 4 2017.

[27] Rodolphe Marques, Andreas M¨uller,Dimitri De Jonghe, Troy McConaghy, Greg McMullen,Ryan Henderson, Sylvain Bellemare,and Alberto Granzotto Trent McConaghy, "BigchainDB: A Scalable Blockchain Database,"*bigchaindb-whitepaper.pdf*, June 2016.

[28] JamesT.Wilson2 andKevin A. Clauson2 MagedN.KamelBoulos1*, "Geospatial blockchain: promises, challenges, and scenarios in health and healthcare,"*International Journal of Health Geographics*, 5 july 2018.

[29] Arthi Manohar1, Jo Briggs1, Mike Harding2, Chris Speed3, John Chris Elsden1, "Making Sense of Blockchain Applications: A Typology for HCI,"*CHI '18 Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, no. ISBN: 978-1-4503-5620-6, p. 458, April 2016.

[30] AjinkyaNighot2, Rahul Wantmure3 VipulH. Navadkar1, ""Overview of Blockchain Technology in Government/Public Sectors" ,"*International Research Journal of Engineering and Technology (IRJET)*, vol. 5, no. 6, June 2018.

[31] Rifat Shahriyar1, Anindya Iqbal1, and Amiangshu Bosu2 Partha Chakraborty1, ""Understanding the Software Development Practices of BlockchainProjects: A Survey","*ESEM 18, Proceedings of the 12th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement*, 2018.

[32] ZehuiXiong, DusitNiyato, Ping Wang, Dongdong Ye, Dong In JiawenKang, "Incentivizing Consensus Propagation in Proof-of-Stake Based Consortium Blockchain Networks,"*IEEE Wireless Communications Letters* , vol. 8, no. 9, August 2018.

[33] RakeshAgrawal PrathimaAgrawal, ""Software Implementation Of A Recursive FaultTolerance Algorithm On A Network Of Computers","*ACM SIGARCH Computer Architecture News - Special Issue: Proceedings of the 13th annual international symposium on Computer architecture (ISCA '86)*, vol. 14, no. 6, May 1986.

[34] Alan Cohen and Jared Butcher Michael Ronnok, ""Blockchain Technology and RegulatoryInvestigations","*Thomas Reuters*, March 2018.

[35] Lakshmi Siva Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications,"*2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, pp. 1-5, August 2017.

[36] Trent McConaghy, "Blockchain, Throughput,"*Medical and Integrated Circuits and Sensors (MICAS)*, October 2014, PDF.

[37] Ittay Eyal, and Robert Escriva, Cornell University Fan Zhang, Cornell Tech Ari Juels, and Robbert van Renesse, "REM: Resource-Efficient Mining for Blockchains,"*Cornell University 26th USENIX Security Symposium*, no. ISBN 978-1-931971-40-9, August 16–18 2017.

[38] ShaokunFan2 and JiaqiYan3 J. Leon Zhao1*, "Overview of business innovations and research opportunities in blockchain and introduction to the special issue,"*SpringerOpen*, December 2016.