A Survey of Breakthrough in Blockchain Technology: Adoptions, Applications, Challenges and Future Research

Abdurrashid Ibrahim Sanka[a,*], Muhammad Irfan[a], Ian Huang[b], Ray C.C. Cheung[a]

[a]*Department of Electrical Engineering, City University of Hong Kong, Hong Kong*
[b]*Digital Transaction Limited*

Abstract

Blockchain technology gets more attentions and more adoptions in various countries and companies all over the world. Currently blockchain is bringing revolution in many enterprises like finance, healthcare, supply chain, insurance, registry and internet of things. Many enterprises integrate blockchain with their systems for its benefits. Despite its strength, blockchain has some challenges in security, privacy, scalability and other few. This paper surveys the breakthrough in the blockchain technology, its applications and challenges. As many blockchain papers focus on cryptocurrencies, IoT and security, this paper focuses on the overall state of the art of blockchain technology, its recent developments and adoptions especially in areas beside cryptocurrencies. We give a comprehensive review of the cryptography behind the blockchain for better understanding of the technology. We also review quantitative surveys and analysis on both the public and the enterprise blockchains. Future research opportunities and directions on blockchain were also reviewed.

Keywords: Blockchain, Cryptography, Consensus, Breakthrough and adoptions.

1. Introduction

Blockchain technology is an inspiring emerging technology capable of disrupting many industries and our way of life. Beside its application and strength in cryptocurrencies, blockchain can help many industries to improve their inefficiencies and overcome many bottlenecks. For example, using blockchain can speed up transaction settlements, reduce costs, bring transparency and auditability as well as increase efficiency, revenue and security [1, 2, 3, 4]. R3 as a consortium of more than 200 financial institutions in the world has been harnessing the benefits of blockchain. Corda is the R3's blockchain platform for enhancing business networks and transactions [5, 6].

There are several adoptions of blockchain in various countries like Georgia, Estonia, Russia and companies like IBM. Gartner [7] forecasted the blockchain business value to be more than $176 billion and $3.1 trillion by 2025 and 2030 respectively. Cisco also predicted that blockchain market will be 9.7 billion USD by 2021 and 10% of the world GDP will be on blockchain by 2027 [8]. More than 40 central banks are experimenting with central bank digital currency (CBDC) while the Facebook's digital currency (Libra) was targeted to be launched in 2020 after getting the US regulatory approval [9, 10]. China's president October 2019, advocated for research, investment and adoption of blockchain technology for China's national and industrial development [11].

Most of the enterprise blockchain projects started earlier are now in production stage with many already deployed in 2019. Cambridge centre for alternative finance [12] surveyed 67 live networks that are already deployed and in production. According to the Deloitte's 2019 global blockchain survey [13], 86% of 1386 high revenue companies believed that blockchain will get the mainstream adoption. Many of the respondents (53%) opined that blockchain is one their top five critical strategic priorities.

Many applications of blockchain transformed from hype to reality with more being explored. Currently about 1200 cryptocurrencies exist [14] and many use cases have been developed in many areas such as insurance, healthcare, supply chain, registry, identity management and more. Despite its benefits, blockchain suffers some challenges of scalability, security, legal regulation privacy and few more. Hence, there is need to review or survey the state of the art of blockchain to quantify its progress, brace up for the future and explore future directions for further research.

There are many survey papers on blockchain many of which concentrated on Bitcoin, security and IoT [15]. Conti [16] presented a detailed survey of the privacy and security issues in Bitcoin. Tschorsch [17] gave a comprehensive survey on Bitcoin. Romano and Schmid [18] investigated the wider outlook of blockchain technology discussing its applications and known issues. Nofer [19] discussed the applications of blockchain and highlighted how the blockchain can disrupt other industries. Zheng et al [20] presented a survey of the challenges and opportunities of blockchain technology. Monrat also [21] surveyed blockchain applications, challenges

[*] Corresponding author

Email addresses: iasanka2-c@my.cityu.edu.hk (Abdurrashid Ibrahim Sanka), m.irfan@my.cityu.edu.hk (Muhammad Irfan), ian.yy.huang@gmail.com (Ian Huang), r.cheung@cityu.edu.hk (Ray C.C. Cheung)

and applications. Firica [22] presented the progress achieved by blockchain in Romans. Vranken [23] looked into the possibility of sustaining bitcoin system. Yang [24] surveyed the blockchain state of the art and research challenges. Wang [3] presented a blockchain survey for IoT. Major challenges, limitations and benefits of adopting blockchain in IoT were explored. Farouk [1] surveyed blockchain for industrial healthcare, Miglani [25] studied the applicability of blockchain in the internet of energy management while Frizzo-Barker [2] is a systematic review of blockchain for businesses. Kus [26] surveyed the Anonymity and Privacy in Bitcoin-Like Digital Cash Systems. Sankar [27] Surveyed the consensus protocols on blockchain applications. Wang [28] Surveyed blockchain consensus mechanisms. Other blockchain surveys include [29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39].

Review of quantitative analysis and surveys of the blockchain is missing in the existing academic blockchain survey papers. The existing survey papers also lack in depth discussion and review of the cryptography behind the blockchain. In this paper, we survey the breakthrough and state of the art of blockchain technology covering recent developments in its adoptions, applications and challenges. We provide a comprehensive review of the cryptography behind the blockchain technology. We also review the recent quantitative analysis and surveys of blockchain as it is missing in the existing blockchain surveys. Finally, we studied the challenges and future research directions on blockchain. The contributions of this paper are summarized as follows:

- We give detail background of blockchain technology citing its benefits and importance.
- We review the blockchain applications and challenges.
- We give a comprehensive review of the cryptography behind blockchain technology.
- We survey the breakthrough of blockchain technology covering its recent developments, adoptions and use cases.
- We review the recent quantitative analysis and surveys on blockchain technology.
- We review the future research opportunities and directions on blockchain.

The rest of the paper is organized as follows: Section II gives the background of blockchain technology. Section III gives the details of the cryptography behind blockchain. Section IV reviews the applications of blockchain while section V discusses the breakthrough and the state of the art of blockchain. Section VI is the review of the quantitative analysis and surveys of blockchain while the challenges and future research directions on blockchain is covered in section VII. Conclusion is finally made in section VIII.

2. BACKGROUND

Blockchain was initially proposed by Satoshi Nakamoto in 2008 [40] in his quest to solve the economic crisis in Europe at that time. The technology underpins cryptocurrencies like Bitcoin and many other applications. Satoshi suggested Bitcoin as a new payment method that dispenses with central authorities (central banks). Satoshi proposed the use of cryptographically protected chain of data blocks later called blockchain for keeping the transaction records. The record continuously grows as new blocks are added (Bitcoin is now over 261GB in size). The strength and promising features of blockchain were first observed from the success of Bitcoin cryptocurrency whose capital market now reaches 167 billion USD [41].

*2.1. **What is Blockchain?***

Blockchain is a distributed database (ledger) consisting of interconnected blocks of data that are protected by cryptographic concepts against tampering. Consensus of the participants (nodes) in a blockchain network manages the rules for using and updating the blockchain. This is an agreement between the participants in the same blockchain network for example Bitcoin or Ethereum. Each node may have a copy of the blockchain (Full node) or depend on another node for the blockchain information (lightweight node).

Each block in a blockchain contains information (hash) of the previous block stored before it to ensure tamper proof protection and data integrity. Whenever a data is changed in a block, the hash of the block will change and can easily be detected. The major attractive features of blockchain technology are its ability to dispense with the central authority, anonymous nature, data protection and security. The distributed nature of blockchain and its consensus enable Bitcoin to solve the double spending problem making it the most successful cryptocurrency.

Figure 1 shows the structure of blockchain. It consists of block header and the transaction data. The header consists of several items (depending on the network) such as hash of the previous block, time stamp, Merkle tree of transactions, nBits and the nonce. The transaction data contains the hashes of the all the transactions in the block. Genesis block is the first block in a blockchain and has no previous hash. All blocks can be traced to the genesis block for verification.

Full blockchain node can be run as a HTTP JavaScript Object Notation (JSON) server for communicating with external applications. Figure 2 is a snapshot of block 100,000 queried from Bitcoin blockchain using remote procedure call (RPC) on Bitcoin-server (bitcoind) in our computer. The block contains block header and four transactions (tx) represented in JavaScript Object Notation (JSON) format.

*2.2. **Why Blockchain Is Important?***

Blockchain possesses good features that make it beneficial. Report from the UK government office of science showed that use of blockchain secures data records, reduces operational costs and provides transparency in transactions [42]. Estonian

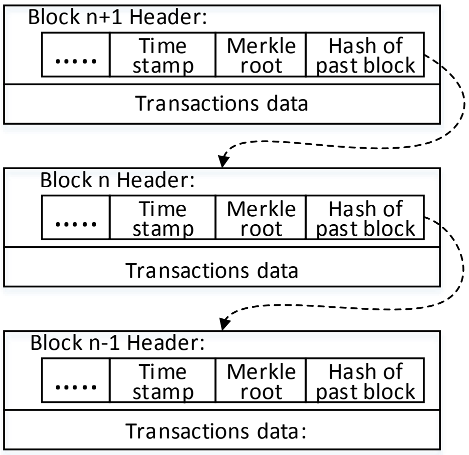
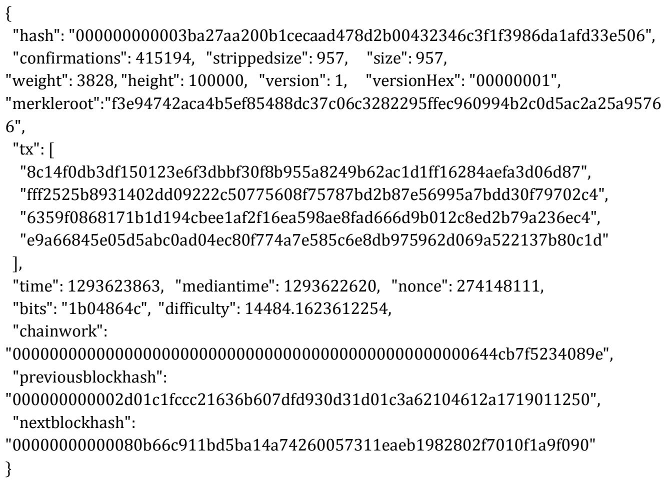


Figure 1: blockchain structure



```
{
  "hash": "000000000003ba27aa200b1cecaad478d2b00432346c3f1f3986da1afd33e506",
  "confirmations": 415194,  "strippedsize": 957,    "size": 957,
"weight": 3828, "height": 100000,  "version": 1,    "versionHex": "00000001",
"merkleroot":"f3e94742aca4b5ef85488dc37c06c3282295ffec960994b2c0d5ac2a25a9576
6",
  "tx": [
   "8c14f0db3df150123e6f3dbbf30f8b955a8249b62ac1d1ff16284aefa3d06d87",
   "fff2525b8931402dd09222c50775608f75787bd2b87e56995a7bdd30f79702c4",
   "6359f0868171b1d194cbee1af2f16ea598ae8fad666d9b012c8ed2b79a236ec4",
   "e9a66845e05d5abc0ad04ec80f774a7e585c6e8db975962d069a522137b80c1d"
  ],
  "time": 1293623863,  "mediantime": 1293622620,  "nonce": 274148111,
  "bits": "1b04864c", "difficulty": 14484.1623612254,
  "chainwork":
"000000000000000000000000000000000000000000000000000644cb7f5234089e",
  "previousblockhash":
"000000000002d01c1fccc21636b607dfd930d31d01c3a62104612a1719011250",
  "nextblockhash":
"00000000000080b66c911bd5ba14a74260057311eaeb1982802f7010f1a9f090"
}
```

Figure 2: Bitcoin block 100,000

government uploaded its 1 million health records on a blockchain to provide traceability, accessibility and security for the record [43]. The interesting features, benefits and importance of blockchain include:

1. **Distributed nature:**
Same blockchain data is stored by different users (nodes) on the blockchain network at the same time. If one node is faulty or lost its data, other nodes on the network still have the copy of the blockchain and keep updating it. The affected node can recopy the blockchain from the other existing nodes. This feature prevents data loss, record tampering as well as double spending in cryptocurrencies.

2. **Data integrity and security:**
Blockchain is tamper proof in the sense that whenever any data in any block is changed, the hash of the block changes as well. This change is detected since the new hash differs from the previously stored hash in the next block. Hence, an adversary has to change the hash of all the blocks down to genesis block for all the network computers to be successful. Practically, the adversary is incapable of overcoming the computers on the network to make his change valid. Hence data is secured on blockchain against tampering in this regard.

3. **Anonymity:**
The anonymity of blockchain allows transactions whose participants are unknown by their physical identities. Scrambled hex digits are used as identities (addresses) without using physical identities like names or photographs. Thus it is difficult to identify persons involved in a particular transaction. However, there is still fear of privacy with the use of some statistical analysis when some knowledge of one of the participants is known. Privacy issue could be overcomes using zero knowledge proofs [44]. In contrast, the real identities of the participants in private blockchains can be known for tracing any fraud or error to the originating node.

4. **Transparency and traceability:**
Since blockchain records are time stamped and stored on all full nodes on the network, all activities and transactions can be checked and seeing by everyone on the network. If the address of a node is known, all its activities and transactions could be traced. This makes blockchain transparent and traceable. It also makes it suitable for fraud detection and a good tool for auditing and public services [24, 42].

5. **Decentralised nature:**
Blockchain dispenses with central authorities and intermediaries making it much suitable for trustless systems. Blockchain allows systems to be autonomous and devoid the risks of intermediaries and central authorities. However, private blockchains may be partially or fully centralised but still benefits from other uses of blockchain [19].

6. **Cost saving:**
Using blockchain comes with huge cost savings as costs associated with intermediary systems are saved. About $20 billion per year could be saved by banks when using efficient blockchain [45]. This is one of the reasons why some banks and enterprises want to incorporate blockchain into their systems to reduce costs [46].

7. **Increased speed:**
Blockchain transactions could be seeing almost as soon as the transaction is added to the main blockchain. Bitcoin transaction takes average of 1 hour to settle after six confirmations. The time is much shorter in private blockchain since proof of work is unnecessary. Using blockchain removes latencies due to office verifications and intermediaries. International bank transactions will settle much faster (within few hours) using blockchain than its current 1-2 days [47].

8. **Efficiency:**
Blockchain allows systems to work autonomously with more efficiency resulting from the removal of intermediary subsystems. This is what many companies and countries are trying to gain from the use of blockchain.

9. **Interoperability:**
Blockchain allows for a secured data sharing enabling separate

parties to share the same data and synchronize their services. For example companies like banks and insurance companies may share data using blockchain for interoperability and other benefits [48].

10. **Verifiability:**
Due to the smart cryptography in blockchain, the authenticity of a record can be verified. This may be difficult to achieve in the databases currently in use because it requires using cryptographic mechanisms like digital signature which are already used in blockchain.

11. **Right to be forgotten:**
Many information systems store private and confidential data such as online transaction details, medical records, passwords and emails. It will be extremely damaging if this type of data leak to the public or to a wrong person. Even though blockchain is immutable, there is a requirement, either by law or by business practice, that certain data must be destroyed after a certain period of time. In addition, there can be illegal data (such as child pornography, proven defamed data) that have been put on the blockchain. Such data must be removed under court order. Traditional methods of protecting confidential information rely on upholding system integrity. However, ensuring integrity in todays interconnected world, where the same data may be replicated onto many servers in different locations, is extremely difficult. Hence, there is a need for an advanced and robust method and the ability to forget for imperative removal of data records by authorized persons [49, 50].

2.3. Types of Blockchain

Due to diversification of interests in blockchain applications, three main types of blockchain classified as public, private and consortium blockchains are currently used [51].

1. **Public blockchain:**
Public blockchain is permissionless, that is to say that it does not require permission to join its network. People everywhere in the world can join and participate in public blockchains by simply installing the blockchain wallet or application on their computers. All users of this network has right to participate in the consensus and can read or write to the blockchain. Bitcoin and Ethereum are examples of public blockchains. Public blockchain are fully decentralized, however they have privacy issues, selfish mining and 51% attack vulnerability [52, 37].

2. **Private blockchain:**
Private blockchain is permissioned unlike the public blockchain. Users need to be authorized to join and participate in private blockchain network. The authorized users can read or write on the blockchain as well as validate transactions. Normally, private blockchain is used for business process automation in a single organization with sub-divided departments that can act as blockchain nodes. Even though private blockchain is less secure and centralized, it is more scalable and has no 51% attack, privacy and selfish mining issues. Multichain is an example of private blockchain [23, 52].

3. **Consortium blockchain:**
Consortium blockchain is also permissioned but stands in between the public and the private blockchain. This blockchain networks are formed by independent organizations working together and share information with limited trust. Users (nodes) in consortium blockchain have to be given access authorization to join and transactions are only accepted upon validation by some pre-selected nodes (validators). Only the validators order transactions and create new blocks. The rest of the nodes can send transactions, read and verify new blocks. Consortium blockchain is partially centralized, has no 51% attack and less privacy and security concerns. Corda and Hyperledger are examples of consortium blockchains [51, 37].

Table 1 compares the three types of blockchains.

2.4. How Blockchain System Works

Blockchain is used where data is to be shared and there are multiple writers. A record is added to the blockchain by sending a message known as a transaction. When a new transaction is to be added, the transaction is signed first using digital signature with the senders private key for authentication. The transaction is then broadcasted to the blockchain peer to peer network. Other nodes verify the transaction and retransmit it through their neighbours. A special node (miner/orderer/validator) collects transactions and creates new block containing large number of transactions depending on the consensus algorithm used. Upon successful creation of a block by the node, the new block is then broadcasted to the network for further verification and acceptance. The rest of the nodes verify the new block and then add to their main blockchain if it is valid [53]. When fork occurs, that is, there are two chains at the same time, the longest chain is chose as the main blockchain while the shorter chain is discarded. This is why six (6) confirmations are required before accepting payments in Bitcoin. Figure 3 is an activity diagram showing how blockchain network works. The term network in the figure refers to all full blockchain nodes on the network including miners and other full blockchain nodes.

2.5. Consensus in Blockchain Technology

Since blockchain is a distributed system, there are concerns on how to synchronize the network to update the blockchain as well as which user (node) will create a new block at a particular instance of time. These issues are treated by a consensus agreement between the users (nodes) on the network. Blockchain generally uses the Byzantine Generals problem for its consensus.

Despite the need of consensus in blockchain, there are commercial and governmental situations that consensus management is not an advantage nor needed. Further more, the absolute requirement of consensus management has been questioned [54]. As a result, PoW (Proof of Work) and PoS (Proof of Stake) are irrelevant in some situations. The lack of the consensus in such cases brings more performance improvements. Examples of situations where consensus is not required are itemized as follows:

Table 1: Comparison of blockchain types

Blockchain	Participation	Members	Security	Centralization	Scalability	Efficiency	Energy spent	Examples
Public	Permissionless	Unknown	Best	Decentralized	Low	Low	High	Bitcoin, Ethereum
Private	Permissioned	Known	Good	Centralized	High	Higher	Very Low	Blockstack, Multichain
Consortium	Permissioned	Known	Better	Partial	Moderate	High	Very Low	Hyperledger, Corda

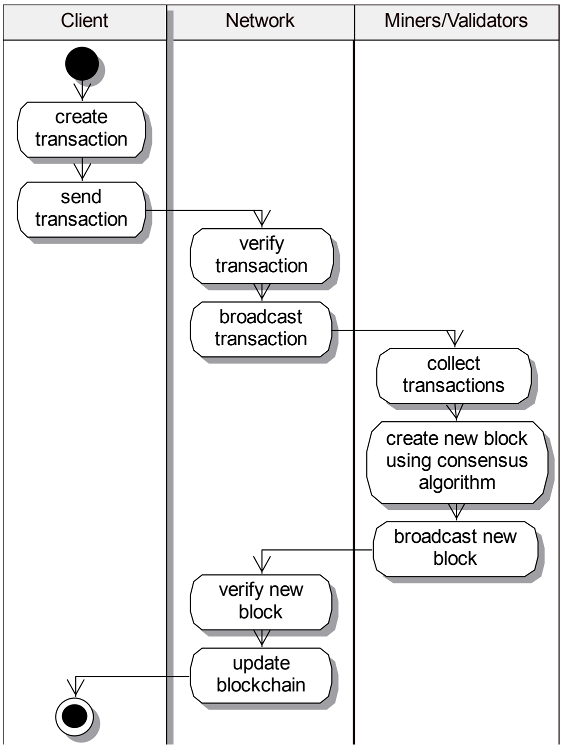


Figure 3: How blockchain network operates

- A consortium of known and trusted participants where one of the members can be given the lead authority. Examples:
  (1) A consortium of contractors and suppliers to one customer (OEM)
  (2) Provider of logistics that fulfils end-to-end order (e.g. DHL)
  (3) Loyalty programme owner leading the participants (e.g. airline alliances)

- Registration of users where trust can be vested on the registrar. Examples:
  (1) Tokenise assets platforms for online trading
  (2) Network of companies in bank clearing system.

- Internal Ledger of a single company where single user can be trusted:

There are several consensus mechanisms used by different blockchain applications.

1. **Proof of work (PoW):**
Computing power is the major factor to determine the creator of new block in PoW consensus. The idea of PoW was originally invented in 1993 by Cynthia Dwork and Naor Moni [55] but was named as "Proof of work" in 1999 by Markus Jacobson and Ari Juels [56]. PoW is solely used for mining process. In the mining process, some of the network nodes called miners compete in doing computation by solving complex mathematical puzzles in order to qualify for creating new block and minting new crypto coins. Any miner that gets the desired result first is the one to submit the new block as well enjoy some new coins as incentive in order to maintain the network. Miners repeatedly compute hash of their proposed block until the hash value is as small as a given difficulty value (nBits) in the block. If the desired value is not obtained, a nonce in the block is incremented for the next hashing trial. In Bitcoin, the difficulty is adjusted over time to maintain addition of 1 block in average of 10 minutes for security purpose [57].
PoW secures the network against double spending attack by distributing the hash rate, and mining power throughout the network. When a fork occurs, the longest chain is chose as the main chain. For this reason, six (6) confirmations are recommended before accepting payments in cryptocurrencies using PoW consensus. However, 51% attack and selfish mining are security concerns in network using PoW.
There is also so much concern over the enormous energy wasted by proof of work. This energy is currently estimated to around 2.55GW which is close to the energy consumed in countries like Ireland and more than the energy consumed individually by 159 countries. the energy wasted was estimated to be about 7.7GW in 2018 almost the same energy consumed by Austria [58, 59]. By the way, some other people and altcoins use or propose other ways of mining with lesser energy waste. Primecoin is a cryptocurrency that uses computations of special prime number sequence (Cunningham and bi-twin chains) as its proof of work instead of the hashing used in Bitcoin. It claimed to be secured and energy efficient since the prime numbers produced may be useful in other areas like cryptography and mathematics [60].

2. **Proof of Stake (PoS):**
Unlike the PoW, PoS is a different consensus mechanism where no mining computations is required but introduced a block validation method instead. Hence, PoS eliminates the puzzle solving methods, it completely diminish the usage of electricity and wasting the energy by executing random

Table 2: Comparison of blockchain Consensus protocols

Consensus	**PoW**	**POS**	**DPoS**	**PBFT**	**Raft**	**Tendermint**	**Ripple**
Year	1999	2012	2014	1999	2013	2014	2012
Type	Permissionless	Permissionless	Permissionless	Permissioned	Permissioned	Permissioned	Permissioned
Criteria	solving puzzle	Stake	voting+stake	BFT+voting	voting	voting	voting
Energy waste	Very high	Low	Very low	Very low	Very low	Very low	Very low
Security	More secure	less secure	Secure	Secure	Secure	Secure	Secure
Scalability	Very low	High	Very high	Low	Very high	Very high	High
Latency	Very High	Low	Very low	Low	Very low	Very low	Low
Trust	No	No	No	Semi	Semi	Yes	Yes
Throughput (tps)	< 20	100	100,000	100	$> 10,000$	10,000	1,500
Mining done	Yes	Yes	Yes	No	No	No	No
Record finality	No	No	No	Immediate	Immediate	Immediate	Immediate
Adversary tolerance	$< 50\%$	$< 50\%$	$< 50\%$	$\leq (n-1)/3$	-	$\leq (n-1)/3$	$\leq (n-1)/5$
Crash tolerance	$< 50\%$	$< 50\%$	$< 50\%$	$< 50\%$	$< 50\%$	$< 50\%$	$< 50\%$
Use case	Bitcoin,Ethereum	Peercoin, NVC	Bitshares	Hyperledger	Corda	Tendermint	Ripple

assumptions, as it no longer requires any complex mathematical problems. Validators collect and propose new blocks. The chance of a validator to add new block in PoS is related to the amount of the stake (coins/currency) owned by the miner node on the network. The node with higher stake has higher chance to submit new blocks. The idea here is that owners of large coins are unlikely to harm the network. However, the main issue with POS is the so-called nothing-at-stake problem. Essentially, in the case of a fork, stakeholders are not discouraged from staking in both chains, and the problems of double spending increases.

To enhance the security and avoid centralization, variant types of proof of stake are used in altcoins like Blackcoin and Peercoin [20]. Casper is a project aimed at upgrading Ethereum blockchain to PoS combined with Byzantine Fault Tolerant (BFT) consensus. However the developers are still working to address some issues with Casper for its full adoption [61].

3. **Practical Byzantine Fault Tolerance (PBFT):**

PBFT consensus is used in private and consortium blockchains where the participants are known and authenticated. The consensus works securely with f out of n nodes assumed to be malicious where $n = (3f + 1)$ and $f = (n - 1)/3$. This means that the system is only secure if the malicious nodes $(f)$are at most $1/3$ of the total nodes n. When n is low, the algorithm allows for higher throughput in thousands requests per second and very much lower latency. As n increases, the performance reduces due to the higher number of messages involved that is $O(n^2)$ [3].

PBFT operated in successive sessions/rounds called Views. Each view has an elected leader called primary and the other nodes (replicas) known as backups. The primary is responsible for coordinating new blocks creation. At the beginning, clients send requests (transactions) to the primary of a current view. The primary then starts the three phase protocol by multicasting the requests to all backups. The three phases are the pre-prepare, prepare and commit phases. In the pre-prepare phase, the primary assigns sequence number to each transaction and prepare a new block proposal which is sent to all the backups. The primary also broadcasts a pre-prepare message to the backups which contains the view number, the primary ID, the block ID and the block number. The aim of the pre-prepare message is to publicly agree and confirm the block to be created. Once the backups accepts the pre-prepare message, the backup then sends a prepare message to all backups and to the primary as its agreement on the new block to be created. When a backup receives $2f + 1$ prepare messages, it enters the commit phase. In the commit phase backups verify and validate requests in the proposed blocked. If all the requests are valid the backup sends a commit message to all othe backups. The new block is finally added to the blockchain if a backup receive at least $2f + 1$ matching commit messages i.e. at least $2/3$ of the nodes agree to add the new block. To enhance the performance and tolerance of PBFT, Proof-of-Authority (PoA) is hence created. In POA the primary replica is elected over time and the number of messages are less in detriment of consistency which affects its data integrity [62, 63, 64].

4. **Tendermint:**

Tendermint is a consensus algorithm following different way other than mining at all (zero energy waste). Similar to delegated proof of stake (DPOS), Three rounds of democratic voting among the block validators is used in Tendermint to select a block. Any validator node found cheating is punished. Tendermint coin uses the Tendermint consensus [65, 21].

5. **Other consensus protocols:**
Several other consensus algorithms proposed include the Raft, Ripple, Proof of Burn (PoB), Proof of Activity (PoA), Delegated Proof of Stake (DPoS), Federated Byzantine Fault Tolerance (FBFT), Ripple, Proof of Publication (PoP), proof of capacity (PoC), proof of existence (PoE), proof of elapsed time (PoET), proof of Space(PoS) and soon. Sliwinski and Wattenhofer [54] proposed ABC which is an asynchronous blockchain architecture that requires no consensus mechanism. ABC is a deterministic permissionedless blockchain that could be used for cryptocurrency applications but could not be used for other applications particularly smart contracts that involves an unknown entity. Table 2 compares some of the popular consensus algorithms. Figure 17 also shows the consensus mechanisms normally used in enterprise blockchain [32, 66, 16, 67, 17, 28, 34, 36].

3. CRYPTOGRAPHY BEHIND BLOCKCHAIN

The beauty of Satoshi's idea of blockchain technology is how he integrated the existing concepts in cryptography together with consensus and incentive mechanism. Blockchain is been supported and protected by cryptographic concepts such as hashing operations, digital signatures and Merkle root. Other cryptographic mechanisms used today mostly to enhance privacy and anonymity include the cryptographic accumulators, commitments and zero knowledge proofs [48, 68].

3.1. Hashing Operations in Blockchain

Hashing transforms strings of information into fixed length and scrambled hex string using special function called the hash function. For use in security applications hash functions are required to be collision free and possess one-way property. Collision free means that no two different inputs to the hash function will generate the same hash output (message digest). Any slight alteration to the input results in a different message digest. One-way property ensures that the input cannot be obtained (reverse engineered) from the message digest.

Hashing is used in blockchain to provide data integrity (security), create addresses and transactions. Furthermore, hashing is essential in PoW consensus mechanism as well as in digital signature schemes. Hash function is used to generate the transactions and the block hashes referred to as the Merkle root and block hash respectively. Tampering with any block data is detected because the hash of the block will change and differ from its previously stored value.

Most blockchain applications use SHA-256 hash function. RIPEMD160 is also used together with the SHA-256 for blockchain addresses as in Bitcoin. Few other hash functions have been created to be memory-hard in order resist ASIC mining (dominant in Bitcoin) so that more miners can participate using PCs and GPUs. Ethereum (ETH), Ethereum classic (ETC), Ethereum Fog, Metaverse, DaxxCoin (DAXX), Musicoin (MUSIC), Expanse (EXP), Elementrem (ELE) and Ellaism (ELLA) all use Ethash hash function for mining for its ASIC resistance [69]. Litecoin, Blackcoin, BitConnect, Stratis and some other altcoins use Scrypt hash function which is also asic resistant. Equihash [70] and X11 are another memory-hard hash functions used in Zcash and Dash cryptocurrencies respectively [68].

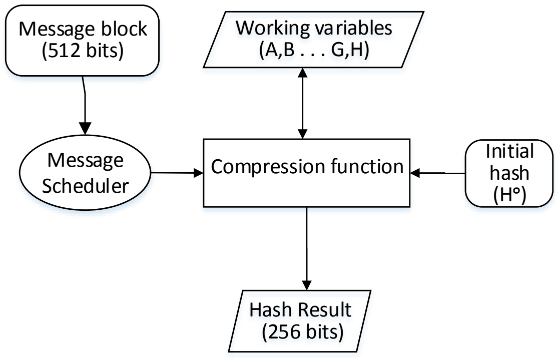


Figure 4: Block diagram of SHA-256 hash function

*3.1.1. **SHA-256 Hash Function***

In blockchain, SHA-256 hash function is mostly used. SHA-256 is considered to be collision free which is the major power harnessed in blockchain technology for data integrity and protection. Only the original input message can give the same hash output (message digest). In fact, the hash is computed twice in Bitcoin for more data integrity. Figure 4 describes the block diagram of SHA-256 hash function used in Bitcoin.

SHA-256 takes in message of length l bits (less than 2^{64} bits) and outputs a 256-bits message digest $H(M)$. The input message (M) is passed in blocks, each 512-bit wide. Padding is usually done to make the input message multiple of 512-bits. Each message block M^i is divided into 16 words $M_0^{(i)}$ to $M_{15}^{(i)}$ (32 bits each). The block is then passed to a message scheduler function which expands the 16 words block to further 64 words W_0 to W_{63} (32 bits each) which get into the compression function where the actual hashing occurs. Initial hash value ($H^{(0)}$) and working variables are used by the compression function for the hashing operation.

Padding:
Padding is adding extra bits to a message to make the number of bits of the input message multiple of 512 so that the message will have exactly n 512-bits blocks. Assuming the message has length l, the k number of zero bits to be padded is determined from (1) such that k is the smallest solution of the relation:

$$l + 1 + k = 448 \;\; mod \;\; 512 \tag{1}$$

At first a bit (1) is added to the message followed by k then followed by 64 bits which are equivalent to the value of the length l [71]. For example we take the message to be $M = abc$

with length *l=24 (bits)*, then:

$$k = 448 - (24 + 1) = 423 \ \ zero \ \ bits \tag{2}$$

The padded message block will therefore be a multiple of 512 in (3):

$$\underbrace{01100001}_{a}\ \underbrace{01100010}_{b}\ \underbrace{01100011}_{c}\ \underbrace{1}_{added}\ \underbrace{000....0}_{k(423bits)}\ \underbrace{00..011000}_{l(64bits)} \tag{3}$$

Initial Hash Value $H^{(0)}$:

The initial hash value is obtained from the fractional part (first 32 bits) of square root of first 8 prime numbers. It is used by the compression function as its initial hash for hashing the message blocks. This value consists of eight 32 bits vectors $H_0^{(0)}$ to $H_8^{(0)}$ shown in (4) below [72]:

$$\begin{aligned} H_0^{(0)} &= 6a09e667 & H_1^{(0)} &= bb7ae85 \\ H_2^{(0)} &= 3c6ef372 & H_3^{(0)} &= a54ff53a \\ H_4^{(0)} &= 510e527f & H_5^{(0)} &= 9b05688c \\ H_6^{(0)} &= 1f83d9ab & H_7^{(0)} &= 5be0cd19 \end{aligned} \tag{4}$$

The working variables *a, b, c, d, e, f g and h*:

The working variables represent the hash of previous round. Sixty four (64) rounds are performed for each block before the final message digest of the block. Each round applies the compression function on the previous round hash represented by the working variables together with the message schedule. Equation (5) shows how the eight working variables are initialized at the beginning of each round and *i* signifies round [72].

$$\begin{aligned} a &= H_0^{(i-1)} & b &= H_1^{(i-1)} \\ c &= H_2^{(i-1)} & d &= H_3^{(i-1)} \\ e &= H_4^{(i-1)} & f &= H_5^{(i-1)} \\ g &= H_6^{(i-1)} & h &= H_7^{(i-1)} \end{aligned} \tag{5}$$

Message Scheduler:

The message scheduler expands the 16 words $M_0^{(i)}$ to $M_{15}^{(i)}$ (32-bits each) of a message block (M^i) into 64 words W_0 to W_{63} (32-bits each) for use in the compression function. For each round (*i*) up to 64 rounds, the 64 words are generated from the expression:

$$W_t = \begin{cases} M_t^{(i)} & 0 \le t \le 15 \\ \sigma_1^{256}(W_{t-2}) + W_{t-7} + \sigma_0^{256}(W_{t-15}) + W_{t-16} & 16 \le t \le 63 \end{cases} \tag{6}$$

The compression function:

The compression function operates the intermediate (previous) hash values with the message scheduler words. The function takes in the initial 256-bits hash value represented by $H^{(0)}$. The function also uses the eight (8) working variables *(a,b,c,d,e,f,g,h)* in order to generate the 256 bit message digest as the hash result. The working variables are initialised with the hash of previous round and then shuffled with the message scheduler words repeated 64 times in each round. The hash at any round is given as [72]:

$$H^i = H^{i-1} + C_{M^{(i)}}(H^{(i-1)}) \tag{7}$$

Where: H^i is the hash value at ith round, C is the compression function, $M^{(i)}$ is the message block for ith round and $H^{(i-1)}$ is the hash of previous round.

In the compression function, six (6) logical functions each operating on 32-bit words represented as variables x, y, z. The output of each function is a new 64-bit word. The operations in the functions are bitwise, rotation and shifting operations as shown in Table3. The logical functions are given as:

$$Ch(x, y, z) = (x \wedge y) \oplus (\neg x \wedge z) \tag{8}$$

$$Maj(x, y, z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z) \tag{9}$$

$$\sum_0^{256}(x) = ROTR^2(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x) \tag{10}$$

$$\sum_1^{256}(x) = ROTR^6(x) \oplus ROTR^{11}(x) \oplus ROTR^{25}(x) \tag{11}$$

$$\sigma_0^{256}(x) = ROTR^7(x) \oplus ROTR^{18}(x) \oplus SHR^3(x) \tag{12}$$

$$\sigma_1^{256}(x) = ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x) \tag{13}$$

The compression function shuffles the working variables (after been initialised with the hash of previous round) with message scheduler words W_t as follows [72]:

Repeat for t=0 to 63 {

$$T_1 = h + \sum_1^{256}(e) + Ch(e, f, g) + K_t^{256} + W_t \tag{14}$$

$$T_2 = \sum_0^{256}(a) + Maj(a, b, c) \tag{15}$$

$$h = g \tag{16}$$

$$g = f \tag{17}$$

$$f = e \tag{18}$$

$$e = d + T_1 \tag{19}$$

$$d = c \tag{20}$$

$$c = b \tag{21}$$

$$b = a \tag{22}$$

$$a = T_1 + T_2 \tag{23}$$

}

After the shuffling of the working variables final hash vectors

Table 3: SHA256 hash function operations [72],(n=no of bit rotations, x= w bit word, $ROTR^n(x) = (x \gg n) \vee (x \ll w - n) and$, and $SHR^n(x) = (x \gg n) \vee (x \ll w - n)$)

SHA256 Operations	Notation
Bitwise AND	$\wedge$
Bitwise OR	$\vee$
Bitwise XOR	$\oplus$
Bitwise complement	$\neg$
Addition module 32	$+$
Rotate right(circular right shift)	$ROTR^n(x)$
Right shift	$SHR^n(x)$

$H_0^{(i)}$ to $H_8^{(i)}$ for the round i are computed as:

$$\begin{aligned} H_0^{(i)} &= a + H_0^{(i-1)} \\ H_1^{(i)} &= b + H_1^{(i-1)} \\ H_2^{(i)} &= c + H_2^{(i-1)} \\ H_3^{(i)} &= d + H_3^{(i-1)} \\ H_4^{(i)} &= e + H_4^{(i-1)} \\ H_5^{(i)} &= f + H_5^{(i-1)} \\ H_6^{(i)} &= f + H_6^{(i-1)} \\ H_7^{(i)} &= g + H_7^{(i-1)} \\ H_8^{(i)} &= h + H_8^{(i-1)} \end{aligned} \tag{24}$$

Then the hash value for round í´ $H^{(i)}$ is obtained by concatenating the hash vectors thus:

$$H^{(i)} = H_0^{(i)} \| H_1^{(i)} \| H_2^{(i)} \| H_3^{(i)} \| H_4^{(i)} \| H_5^{(i)} \| H_6^{(i)} \| H_7^{(i)} \tag{25}$$

After completing the 64th rounds for a block, the block's final hash (message digest) is:

$$H^{(64)} = H_0^{(i)} \| H_1^{(i)} \| H_2^{(i)} \| H_3^{(i)} \| H_4^{(i)} \| H_5^{(i)} \| H_6^{(i)} \| H_7^{(i)} \tag{26}$$

In summary,SHA-256 hashing is described in figure 5.

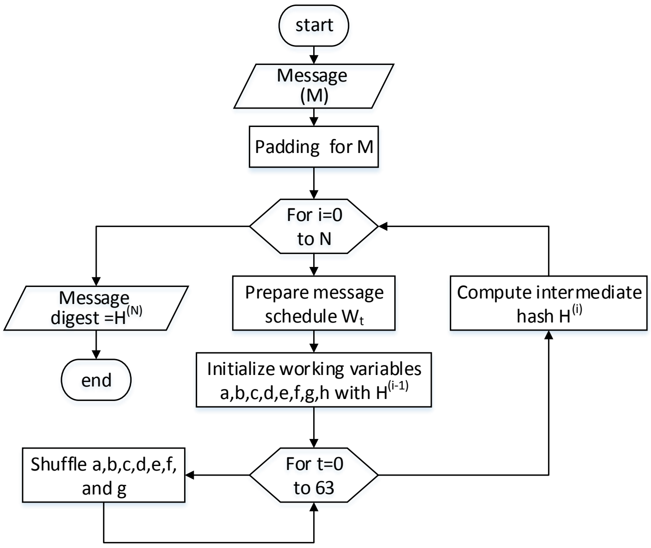

start
Message (M)
Padding for M
For i=0 to N
Message digest =H^(N)
end
Prepare message schedule W_t
Compute intermediate hash H^(i)
Initialize working variables a,b,c,d,e,f,g,h with H^(i-1)
Shuffle a,b,c,d,e,f, and g
For t=0 to 63

Figure 5: SHA-256 hash function

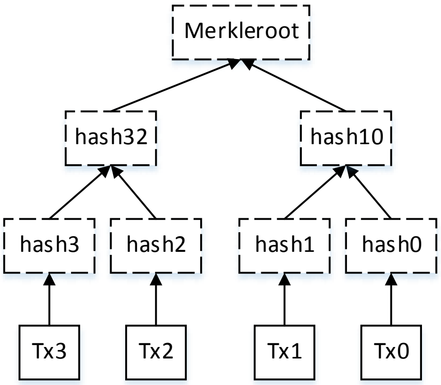


Figure 6: Merkle tree creation in blockchain

3.2. Merkle Root and Merkle Tree

All transactions in a block are represented by a single hash called the Merkle root stored in the block header. The Merkle root is the last hash value of the Merkle tree constructed from the hashes of the transactions. Figure 6 shows the construction of Merkle tree from an example block having four transactions. however, in blockchain, a block may contain thousands of transactions.

3.3. Digital Signature in Blockchain

Digital signatures are used to authenticate transactions in blockchain. This is to ensure that only the authentic sender sends the transaction and is unable to deny it at later time (non-repudiation). Elliptic Curve Digital Signature Algorithm (ECDSA) is used in Bitcoin and most blockchain applications to sign and verify transactions [73]. However, Monera and NaiveCoin use the Edwards-curve digital signature Algorithm (EdDSA) [74]. RingCoin and some other altcoins use Ring signatures for anonymity. One-time ring signature (OTS) [75] and Borromean ring signature (BRS) [76] are used together with ECDSA or EdDSA or rarely alone in some few applications such as Monero. Furthermore, most blockchain nowadays use multi-signature in addition to the ECDSA or EdDSA for privacy and more security [68]. For brevity, we review Elliptic Curve Cryptography (ECC) and the Elliptic Curve Digital Signature Algorithm (ECDSA).

3.3.1. Elliptic Curve Cryptography

Blockchain uses asymmetric cryptography where two different keys (public and private keys) are required. These keys are used for encryption, decryption and digital signatures. Most blockchain systems use elliptic curve over prime field for key pair creation and other operations like the digital signature. Elliptic curve cryptography (ECC) shows better

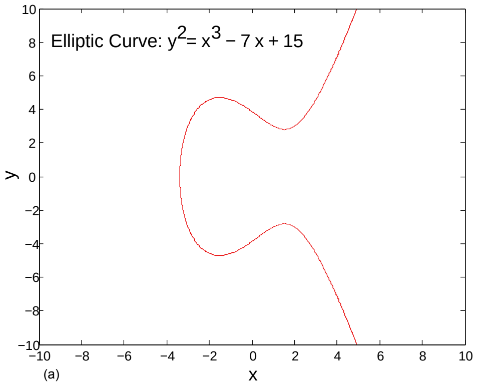


Figure 7: Plot of elliptic curve $y^2 = x^3 - 7x + 15$

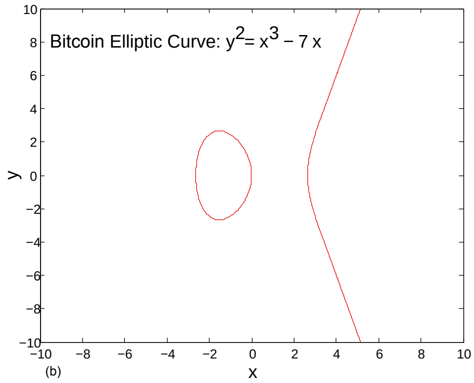


Figure 8: Plot of elliptic curve $y^2 = x^3 - 7x + 15$

implementation efficiency and better security for the same key size than other cryptography schemes like RSA and DSA. It is also more suitable for devices with low power, less memory and bandwidth capabilities [77, 78]. ECC was first invented in 1985 independently by Neal Koblitz [79] and Victor Miller [80]. The security of elliptic curve cryptos is based on the difficulty of their discrete logarithmic problem [81]. This means that, given a point P on an elliptic curve, it is easy to multiply P by a multiplier k to get another point Q. However, it is very much difficult (computationally infeasible with the current computing power) to get the multiplier by just knowing the two points P and Q. Therefore using ECC it is infeasible to get private key of someone by just knowing his public key and the curves generator point. In summary, elliptic curves are trap door functions utilized for cryptography.

3.3.2. *definition*

An elliptic curve E over the field $\mathbb{F}_p$ is defined by the equation:

$$E : y^2 = x^3 + ax + b \qquad mod\ p \tag{27}$$

where: $a, b \in \mathbb{F}_p : 4a^3 + 27b^2 \neq 0$
Parameters *a, b, p, G, n, h* are the global domain parameters chosen for a particular elliptic curve to determine the curve characteristics. The parameter p is usually a large prime number serving as the upper limit for the coordinates x and y, G is the generator point which is the base point of the curve that is used to generate all other points. The n and h are the order of the curve (determining the number of points on the curve) and a cofactor of the curve (#E($\mathbb{F}_p$)/n) respectively. For security purpose, n is usually chosen to be a very large integer value. All Parties in the same ECC application must use the same elliptic curve parameters [82].
An Elliptic curve having order of n, has *n-1* discrete points starting from 1 and including a point at infinity i.e.

$$\langle G \rangle = \{\infty, 1G, 2G, 3G........(n-1)G\} \tag{28}$$

Figure 7 and Figure 8 show the plots of elliptic curves $y^2 = x^3 - 7x + 15$ and $y^2 = x^3 - 7x$ (over real field) respectively. Elliptic curves over finite field are only represented by dotted points unlike the smooth curve as in the real field.

3.3.3. *The Elliptic Curve used in Blockchain*

NIST recommended 15 elliptic curves having varying levels of security [83]. Bitcoin and most other cryptocurrencies use the *secp256k1* elliptic curve defined over prime field with the following domain parameters given by Certicom [78], [81]:

$$\begin{aligned}
& a = 0; \qquad b = 7; \qquad h = 01; \\
& p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1 \\
& \quad = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFF \\
& \qquad FFFFFFFFFFFFFFFFFFFFFFFFFEFFFF \\
& \qquad FC2F \\
& G\ \ in\ \ compressed\ \ form : \\
& G = \qquad 0279BE667EF9DCBBAC55A06295CE870B \\
& \qquad 07029BFCDB2DCE28D959F2815B16F81798 \\
& G\ \ in\ \ uncompressed\ \ form : \\
& G = \qquad 0479BE667EF9DCBBAC55A06295CE870B \\
& \qquad 07029BFCDB2DCE28D959F2815B16F81798483A \\
& \qquad DA7726A3C4655DA4FBFC0E1108A8FD17B448A \\
& \qquad 68554199C47D08FFB10D4B8 \\
& n = FFFFFFFFFFFFFFFFFFFFFFFFFFFFF \\
& \qquad FFEBAAEDCE6AF48A03BBFD25E8CD0364141
\end{aligned} \tag{29}$$

Therefore most blockchain applications including bitcoin use the elliptic curve : $y^2 = x^3 + 7 \quad mod \quad p$

3.3.4. *Arithmetic Operations on Elliptic Curves*

Points on an elliptic curve are arithmetically operated to generate another point on the same curve. Point addition and point doubling are the basic operations for elliptic curves that are used for other operations like multiplication, inversion, square root and subtraction [82].

Point Addition on Elliptic Curves:

Geometrically, the sum of two points A and B on an elliptic curve is another point C which is a reflection of the point D at which straight line passing through A and B crosses the curve. This sum is referred to as point addition and is illustrated in

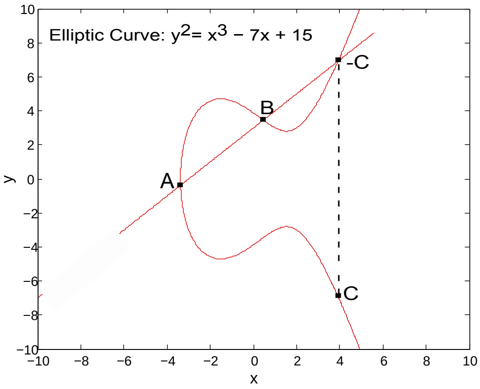


Figure 9: Point addition on elliptic curve

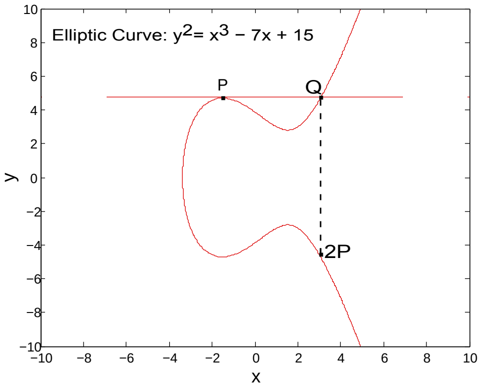


Figure 10: Point doubling on elliptic curve

Figure 9. Analytically:
Given $A(x_1, y_1) + B(x_2, y_2) = C(x_2, y_2)$ then,

$$x_3 = s^2 - x_1 - x_2 \tag{30}$$

$$y_3 = -y_1 + s(x_1 - x_3) \tag{31}$$

$$s = \frac{(y_1 - y_2)}{(x_1 - x_2)} \tag{32}$$

$$C = O \;\; (point \;\; at \;\; infinity) \;\; if \;\; A = -B \tag{33}$$

Point Doubling on Elliptic Curves:
Point doubling is the same as adding a point to itself i.e. $2P = P + P$. Geometrically, to double a point P on an elliptic curve, draw a tangent to the curve at P. The reflection of the point Q at which the tangent crosses the curve is twice the point P i.e. $Q = 2P$. This is illustrated in Figure 10.
Analytically:
Given the points $P(x_1, y_1)$ and $Q(x_2, y_2)$ such that $Q = 2P$ then,

$$x_2 = s^2 - 2x_1 \tag{34}$$

$$y_2 = -y_1 + s(x_1 - x_2) \tag{35}$$

$$s = \frac{(3x^2{}_1 + a))}{(2y_1)} \tag{36}$$

Scalar Multiplication on Elliptic Curves
To multiply a point with a scalar, point addition and the point doubling are used. For example,

$$5P = P + P + P + P + P = 2(2P) + P. \tag{37}$$

This elliptic curve scalar multiplication process is known as double and add method./

3.3.5. Key pair creation with Elliptic Curve

The algorithm 1 is used to create key pair with elliptic curve cryptography [84, 85]. The key pairs are used for purposes like encryption,decryption and wallet addresses.

3.3.6. Elliptic Curve Digital Signature Algorithm (ECDSA), Transaction signing and creation in blockchain

Blockchain transactions have to be signed and verified before added to a block. Signing transaction involves creating the transaction as a message. The message is then hashed and encrypted with the senders private key to create the digital signature (s). The sender then broadcasts both the digital signature together with the raw transaction. To verify a particular transaction, the signature is decrypted with the public key of the sender. The resulting ciphertext is compared with the hash of the raw transaction where it is said to be valid when they are the same. Normally, scripts are used to automate this transaction signing and verification.

Algorithm 1 Key Pair Creation with Elliptic Curve

```
  INPUT: Global domain parameters $(n, G, p)$
  OUTPUT: private key $d$ and public key $Q$

1: Select unique random or pseudorandom large integer $d$ :
   $d \in_R [1, n - 1]$
2: Compute public key $Q = dG$
3: return $(d, Q)$
```

Algorithm 2 Generation of ECDSA Signature

```
INPUT: private key $d$, public domain parameters $(G, n)$, hash
function $H$ and the message $m$
OUTPUT: signature $(r, s)$

1: choose unique random or pseudorandom large integer $k$ :
   $k \in_R [1, n - 1]$
2: compute the point $P(x, y) = kG$ mod n and convert $x$ to
   integer
3: assign $r = x$ goto 1 if $x = 0$
4: compute message hash $e = H(m)$
5: compute $s = k^{-1}(e + dr)$ mod $n$. If $s = 0$ then goto 1
6: return signature as the pair $(r, s)$
```

The algorithms 2 and 3 describe the ECDSA used for both signing and verifying blockchain transactions respectively [77, 84, 85]. ECDSA was first proposed as a response to NISTs proposal by Scott Vanstone in 1992 through John Anderson[86]. ECDSA was first accepted as an ISO standard in (1998)[87] and is also accepted as a standard for ANSI, IEEE and NIST [77, 81].

Algorithm 3 Verification of ECDSA digital signature (r, s)

INPUT: public key Q, public domain parameters (G, n), hash function H and the message m

OUTPUT: verification result ($TRUE$ or $FALSE$)

```
if $(r, s) \in_R [1, n-1]$, then
    valid signature, proceed to verify
else
    invalid signature, terminate
end if
compute message hash $e = H(m)$
compute $u_1 = s^{-1} \bmod n$
compute $u_2 = u_1 e \bmod n$, and $v_1 = u_1 r \bmod n$
compute $P(x, y) = u_2 G + v_1 Q \bmod n$,
if $x = r$ then
    return true
else
    return false
end if
```

3.4. *Blockchain Address*

Blockchain uses scrambled number (hex) to represent user accounts (addresses) instead of physical identities. In Bitcoin, ECDSA key pair, SHA-256 and RIPEMD160 hash are used to create the Bitcoin addresses. Key pairs and the addresses can independently be created for every transaction and then stored by the wallet software. The address is a 160-bit message digest resulting from the SHA-256 and RIPEMD160 hashing converted to Base58Check string encoding. The process of Bitcoin address creation is given in the algorithm 4: After key pair (private and public keys) is created, the public key is hashed using SHA-256 hash function. The 256-bit output is then hashed again using RIPEMD160 hash function which gives the 160-bit output (double hashing). A 1-byte network ID (0x00 for main network) version number is appended at the beginning of this output. To get a checksum the new output is hashed again twice with SHA-256 and the least significant 4 byte is the checksum. Now with the checksum appended to the right and the earlier version number appended to the left, the result is converted to Base58 using Base58Check encoding to string to get the final resulting Bitcoin address. Normally script codes are also used for this purpose and the addresses are checked for validity before making transactions by the wallet software [88].

Algorithm 4 Blockchain Address Creation

INPUT: ECDSA domain parameters (n, G), version number (network ID)

OUTPUT: private key d and Address

```
Create ECDSA key pair (private key $d$ and public key $Q$)
Compute $A_1 = Ripemd160(SHA256(Q))$
Append version number(1 byte): $A_2 = version\_no||A_1$
Compute $Sum = SHA256(SHA256(A_2))$
Assign $Checksum = Sum$(4 least significant bytes)
Append checksum: $A_3 = version\_no||A_1||checksum$
Convert to Base58: Address=Base58Encoding($A_3$)
return (private key,Address)
```

4. APPLICATIONS OF BLOCKCHAIN

Blockchain is important for systems where data is to be shared and protected with some autonomy and privacy. Blockchain evicts central authorities and intermediaries such that systems are self governed with saving the costs due to intermediaries. Thus blockchain boosts efficiency, speed and reduces costs. It also comes with other benefits such as transparency and traceability that fit it into several applications beside cryptocurrencies [46, 19]. There are many applications of blockchain as summarised in Figure 11.

1. **Cryptocurrencies:**

Blockchain underpins the most successful digital currency (Bitcoin) and many other cryptocurrencies such as Ether. As of March 28, 2020, the market capital of Bitcoin and Ether are \$113 billion and \$14 billion and sold at \$6188 and \$128 respectively [41]. Currently there are around 1200 cryptocurrencies including the Bitcoin-cash, Litecoin, Dash, Ripple, Monero and soon [14]. Researchers from Cambridge University estimated the number of cryptocurrency wallets active users to be around 2.9 million to 5.8 million [89].

Currently speaking cryptocurrencies are accepted by many companies and vendors. According to HSB's 2020 survey Bitcoin is accepted by 36% of small to medium businesses in US and 56% of them purchase the currency for their own use%. Bitcoin is being accepted by Microsoft, Expedia, Wikipedia, Burger King, KFC, Subway, NorwegianAir, and more. Cryptocurrency exchanges and ATMs could be used to change cryptocurrencies into cash and vice-varsa. There are many exchanges such as Coinbase and Cex.io that facilitate buying and selling of cryptocurrencies with cash. General Bytes [90] manufactures and has sold over 3322 cryptocurrency ATMs across over 63+ countries world wide. The ATMs support over 123 fiat currencies. Other cryptocurrency ATMs are the Genesiscoin and Lamassu [91].

Many countries have been putting efforts to create their own cryptocurrencies known as the central bank digital currencies (CBDCs) mostly to be used for inter bank and government transactions. The China's digital currency will soon be released likely in this year 2020. The cryptocurrency of Facebook (Libra) also planned to be released this year 2020 took so much media attention when the information was first released.

There are so many research publications on cryptocurrencies especially the Bitcoin. Bitcoin-NG presented a protocol to scale Bitcoin for high transactions per second. Ciaian [92] also studied Bitcoin pricing. Lightning network, Sidechain, sharding approaches were all proposed to speedup the cryptocurrency transactions [93].

2. **Smart contract:**

Contract is agreement between parties that is enforceable when the terms of the contract are fulfilled. Smart contract introduced since 1994 by Szabo [94] is a contract governed and enforced by computer program without the need for third party like lawyer. The program automatically executes the contract agreements fairly when its conditions are satisfied. Currently with the support of blockchain, smart contracts are secured and convenient. It is run on blockchain such as Ethereum, Hyperledger, Corda and Namecoin for applications such as decentralized applications (Dapps), voting and domain name service (DNS) [95].

Dapps hosting smart contracts run on the several computers of the blockchain network. New contracts are created on the blockchain such as Ethereum account and deployed to the blockchain network in form of new transaction. A transaction can call methods of a contract, create or transfer money to the contract. smart contract may also transact with other smart contracts through the transactions to achieve certain functionalities. Solidity is the most popular programming language designed for creating smart contracts. Currently, there are over 14 million smart contracts on Ethereum [96]. In Hyperledger the smart contracts are packaged as a chaincode.

Most blockchain applications beside cryptocurrencies such as supply chain use smart contract in one way or the other. Bartoletti and Pompianu [97] classified smarts contracts into five categories based on their use. The study analysed smart contracts on Bitcoin, Ethereum, Stellar, Counterparty, Lisk and Monax. According to the findings, smart contracts are used to provide Financial, notary, game, wallet and library services. Financial smart contracts such as DAO contracts provide cryptocurrency transfer and storage. Notary contracts perform documents and identity permanent storage on blockchain for ownership and provenance certification. Gaming is another common area for smart contracts while large number contracts are used to provide wallet and library services on the blockchain.

There are many literature on smart contract protocol, applications, privacy and security. Pinna [96] and Bartoletti [97] studied and analysed smart contracts. Zhang [98] is an access control based on smart contract for IoT. Hawk is a framework proposed by Kosba et al [99] for smart contracts to ensure privacy. The system hides transaction details from public for the privacy protection unlike in the existing Ethereum smart contracts. Mense and Flatscher [100] studied security vulnerabilities in smart contracts on Ethereum blockchain. In additon, several surveys such as [101] and [102] have been conducted on smart contracts and their applications.

3. **Stock Exchange:**

Traditional ways of buying and selling assets and stocks requires alot of undesired costs, trusts and intermediary involvements. With blockchain technology all the mentioned overhead could easily be overcome. Norbert Biedrzycki who is a head of services at Microsoft described the eminent transformation of stock exchange marketing by blockchain technology [103].

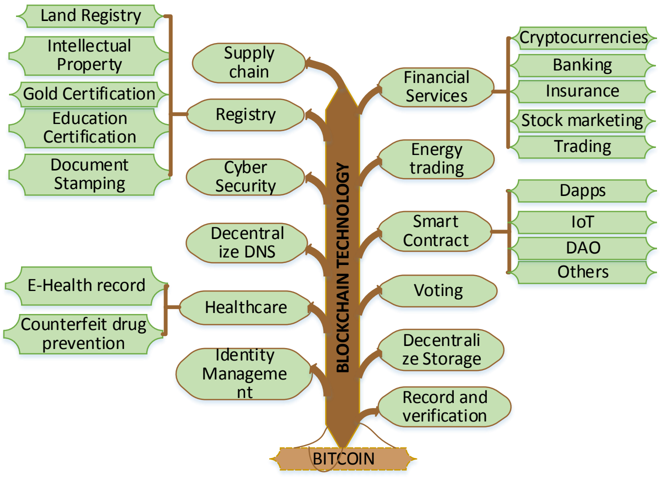


Figure 11: Blockchain applications tree

Although shares are not sold directly by banks, secondary markets buy and shell shares using blockchain. Bitshares, Augur, NASDAQ and Coinsetters have been using blockchain for stock marketing and exchanges [30]. The Australian Security Exchange (ASX Ltd) and the London Stock Exchange have all been working on integrating blockchain in their systems [104]. V-Chain [105] is a blockchain based platform proposed to efficiently provide car leasing services.

4. **Healthcare management:**

The current healthcare management system has several issues such as data inconsistency, duplicate records and the inability of patients to know and manage their own records. Blockchain when properly used could solve the afore mentioned challenges in Healthcare. Currently, blockchain is used to share and secure data for healthcare management. The records are uploaded on the blockchain to provide sharing, accessibility, security, reduction in cost and traceability. Different health institutions could interoperate without issues due to difference in database and the individual central authorities. Estonia is the first government to put its healthcare records on blockchain [43]. There are several companies such as Gem, HealthBank that use blockchain for health services including record sharing and fake drugs prevention [106]. Patients who want to share their health records are also being paid by the companies.

Blockchain in healthcare management has taken several attention of researchers. Blockchain applications in healthcare have been classified into four categories including medical record management, medical insurance, clinical and biomedical research and applications connecting healthcare providers [107]. Wang et al. proposed a parallel healthcare system based on ACP approach and powered by blockchain [108]. Griggs [109] proposed a blockchain based healthcare system to securely and autonomously monitor patients remotely. Zhang et al. [110] proposed FHIRChain, a blockchain architecture for scalable and secure sharing of clinical data. Healthchain [111] and OmniPHR [112] were proposed for protected healthcare information (PHI) and healthcare data integration respectively. McGhin [113] and Abujamra [114] are surveys of blockchain applications in healthcare.

5. **Insurance:**
There is increasing use of blockchain by insurance companies. Putting the insurance data on blockchain prevents fraud and allows data sharing and interoperability among the insurance companies. This prevents people from claiming same insurance from more than one companies. Everledger is an example of companies using blockchain for diamond certification history [30]. Raikwar et al designed a secured blockchain framework for insurance services. This will make insurance services more secured and efficient[115]. Etherisc, Insurwave and MedRec are another example use cases of blockchain in insurance.

6. **Banking and finance:**
Blockchain is capable of disrupting banking and finance industry due to its important features. For its benefits, many banks have been trying blockchain to improve their systems. In 2016 the first banking transaction with blockchain was carried out between Commonwealth Bank of Australia and Wells Fargo[116]. Nofer [19] studied defects in banking system and highlighted solutions using blockchain. Several other financial services like online payments, and digital assets are carried out with blockchain [20]. Garrick and Michel discovered that about 63% of central banks experiment with blockchain, with hope of integrating it with their system after successful trial [89].

7. **IoT industry:**
Blockchain has got attentions for the internet of things (IoT) because of the need of the IoT devices to be autonomous, communicate and share data without human intervention. Example blockchain application in IoT include the IBM's ADEPT, Filaments, GSF and Share&Charge. With ADEPT, IoT devices like home appliances can troubleshoot, upgrade and update themselves [20]. Golden state food (GSF) partnered with IBM for the use of blockchain with IoT sensors to monitor beef condition across its supply chain. Dorri [117] is a case study of smart home with blockchain. There are several proposals and surveys such as [3, 118] for the use of blockchain in IoT industry.

8. **Blockchain based DNS services:**
Blockchain is also used for domain name service (DNS) to avoid security attacks, censorship, and misuse by the central organizations or governments governing the DNS service for the internet. The DoS attack on *Dyn* DNS provider in October 2016 was a wakeup call for tighter security provisions in DNS service. DNSSec (DNS Security) and blockchain were used to secure DNS services. Blockstack [119] and Namecoin [120] provide DNS services using blockchain. EmerDNS is a blockchain alternative for DNSSec. Blockchain-DNS is a browser extension supporting blockchain services on blockchain [121]. Karaarslan [122] studied the blockchain based DNS and PKI solutions.

9. **Decentralized data storage:**
One threat of the existing cloud storage provided by companies like Google and drop box is the security of the data and centralization. Such traditional centralized systems serves as a single source of failure for data security and privacy breach. Hence blockchain is employed to store personal data in a decentralized manner with full control and management by the data owners. Blockchain storage has advantages of speed, security, flexibility and low cost. Storj is a decentralized cloud storage network using blockchain that is secure, private and ease to use [123, 124]. Gaia is another blockchain storage of blockstack [122]. Other blockchain based storage networks include Swarm, Sia, IPFS and SAFA networks [125]. Li et al [126] proposed a blockchain based data storage for IoT without the use of certificates.

10. **Intellectual properties and document stamping:**
Blockchain is also used to support intellectual properties and document stamping for prevention of forging documents. The documents are stored on the blockchain after been stamped and digitally signed. Since everyone can access the certified document on the blockchain for verification, forging of such documents is much more difficult and hard to achieve. Blockchain is used by companies such as Stampery, Ascribe, Block notary and Microsoft to certify emails, certificates and documents [30]. Vaultitude (formerly ipchain), Vechain and KODAKone are blockchain platforms that provide intellectual property management and protection. Muzika, Mycelia, BigchainDB provide blockchain IP for music and entertainment industry.

11. **Voting:**
Many countries especially developing ones are incapable of carrying out free and fair elections. Blockchain could be used to make transparent voting in organizations, meetings and even for national elections. BitCongress, Remotengrity and AgoraVoting are projects that provides good architecture for voting with blockchain [127]. Blockchain based e-Voting is been tested in sixteen (16) countries to promote free and fair election with a tamper proof record [128]. Slock.it implemented the Hutten decentralized digital organization (DDO) based on blockchain for Siemens to allow voting by their partnering company [129].

12. **Digital identity management:**
Identity management is one of the recent and effective applications of blockchain considered by some governments and organizations. Traditionally, government bodies or organizations provide identifications for individuals in form of passports, ID cards, certificates and so on. The traditional identity management is much vulnerable to lost, theft and fraud. Now with the advent of blockchain, identities could be securely managed autonomously without central authorities. Blockchain in conjunction with zero knowledge proof supports claiming and verification of identities stored on the blockchain in a secure and private way. Typical use case is the e-Identity of Estonia. Many other countries like USA, Japan, Switzerland, India and Finland are currently doing a trial for

its adoption[128]. United Nation in collaboration with Microsoft and Accenture showcased a prototype global refugee identity system based on blockchain during the United Nation ID2020 summit in New York. The system is a typical cross boarder application of blockchain and will be used to verify the identities of refuges for healthcare, education and so on [130]. Tykn is another blockchain platform that provides digital identity management and services.

13. **Cyber Security:**
Blockchain is used to enhance cyber security. Network history, configuration, log files and other network files are stored on blockchain to provide an immutable record denying attackers any chance to modify record. This concept is used by companies like Guardtime to provide Network security services against several network attacks [131, 132]. Blockchain is used to secure data in computer systems and IoT. Blockchain based DNS, PKI and storage secure web services against DDoS and other attacks. CertCoin uses blockchain for public key infrastructure (PKI). REMME is a startup that stores SSL certificates on blockchain to dispense with certificate authorities (CA). CryptoMove protects APIs and apps with blockchain, Hacken provides security tools based on blockchain for professionals in cybersecurity while Gladius protects DDoS using the blockchain. Other companies and startup using blockchain for cybersecurity include openAVN, block armour, Cryptyk, Sentinel Protocol, Megahoot and AnChain.ai [133].

14. **Asset Registry and Tokenization:**
As blockchain enables an immutable registry of information for assets. Assets are also represented as tokens and then trade or stored on the blockchain. Registry of assets can easily be kept in blockchain in a secure way to avoid fraud and asset theft. Blockchain provides secure asset tokenization, land registry, asset marketplaces and property data standardization. Georgia had its land registry records on blockchain. There are many trials of using blockchain for asset registries in UK, Sweden, India and Russia[128]. Codefi Assets platform of Consensys company provides blockchain based asset management services and platform. Securitize, Harbor, AlphaPoint, trustToken, Polymath provide blockchain based asset tokenization platforms. In addition, Meridio, Blockimmo, Propy and Imbrex provides real estate investment, marketplace and registry services on blockchain [134].

15. **Supply chain and trade management:**
Blockchain provides security, transparency, speed and reduced cost to supply chain and trade. Records of supplies of goods or trades could be stored for better tracking and verification. At any instant of time all parties involved in the supply chain will be aware that certain good has been supplied to a particular location or a certain trade occurred. The information is received much faster without relying on the central authority that have control of the information and may act maliciously. Using blockchain also may prevent loss of items and records. TradeLens is a blockchain based supply chain network founded by Maersk and is been used by about half of the global shipping companies [135]. Grainchain uses blockchain for selling, buying and tracking of grain and other agricultural commodities [136]. Medildger provides blockchain solution for pharmaceutical supply chain such as medicines tracking and payments.

Table 4: Blockchain Applications and use cases

Application	Example Use cases
Cryptocurrencies	Bitcoin, Ethereum, Libra
Smart contract	DAO, Clause, Namecoin, Agrello
Stock Exchange	Nasdaq, Coinsetters, Augur, Bitshares, V-chain
Healthcare	HealthBank, Gem, Healthchain, MeDShare, FHIRChain, OmniPHR, CoverUS
Insurance	Etherisc, Insurwave, MedRec
Banking and Finance	JPM coin, Wells Fargo coin, MonetaGo, Komgo, Studium, Khokha, Ubin
IoT	ADEPT, Filament, Dorri, GSF, netObjex, Share&Charge
DNS service	Blockstack, Namecoin, EmerDNS, DNSChain, Blockchain-DNS
Decentralize storage	Storj, Gaia, Swarm, Sia, IPFS, SAFA networks
Intellectual Property	Stampery, Ascribe, block notary, Vaultitude, Vechain, KODAKOne
Voting	Bitcongress, AgoraVoting, Siemens Hutten DDO, Kaspersky voting machine
Identity management	Evernym, Verified.me, ID2020, Tykn, Shocard
Cyber Security	Guardtime KSI,CertCoin, REMME, Gladius, CryptoMove, Hacken,block armour
Asset Registry	Georgia land registry, Codefi Asset,Blockimmo, Meridio, Propy, Imbrex
Supply chain	TradeLens, Grainchain, Waltonchain, Medildger, Walmart, Circulor
Energy	PowerLedger, Verv, Electron, EWF, Grid+, Ondiflo, Enerchain,

16. **Energy Trading and Management:**
Energy is another sector that has been disrupted by blockchain technology. In smart grid, Energy is been produced and consumed by different individuals. Blockchain is currently used to coordinate this energy trade on the microgrid without the central authority [21]. Blockchain could be used for electricity distribution and data management as well as oil and gas exploration, trading and resource management. PowerLedger is a company based in Australia that provides blockchain platform for people to sell and buy energy. Electron, Verv, EWF, Grid+, Wepower, Settlemint, Enerchain, and Ondiflo are example companies that provide blockchain services in energy sector.

17. **Contract Management:**
Traditional contract management is inefficient and involves alot of risks and increased operational costs. There are many companies now that provide blockchain solutions and platforms for contract management. Contractors and their clients use the platforms for tracking and managing their contracts efficiently. The solutions are used in construction and other projects. Currently, Monax, Corda, Oracle, Konfidio and Icertis all provide the blockchain based contract management platforms and solutions. Although, these solutions might be costly but they are more efficient over their traditional counterparts such as Apttus and Coupa.

Other blockchain applications are found in areas including public services, building services, trust management, music industry and more [95, 137, 138]. Table 4 summarises the blockchain applications citing their example use cases.

5. BREAKTHROUGH AND STATE OF THE ART OF BLOCKCHAIN

This section discusses the journey of blockchain technology from its inception. The breakthrough and progress of the technology in various industries and countries were also discussed. The emergence of various applications using blockchain and wider adoption of the blockchain in several countries and companies are the major breakthrough of the blockchain technology.

5.1. Blockchain Journey Brief

In 2008, Satoshi Nakamoto brought the idea of blockchain in his endeavor to solve the Europes economic crisis. He proposed the use of chain of blocks (coined as blockchain) in Bitcoin as new peer to peer electronic cash system that works without central bank and solves double spending problem. Bitcoin was launched in 2009 supported by the blockchain and started getting more attention around 2012 [40]. Currently there are around 1200 cryptocurrencies using blockchain technology [14].

In the beginning of Bitcoin, CPU was used for mining and succeeded by GPUs. FPGA was later used to provide higher hash rates than GPU. Currently, ASICs miners dominate the CPU, GPU and the FPGA for their much higher throughput [23, 139]. The current hash rate of Bitcoin is about 120 million TH/sec [140]. Taylor [141] examined the trend of hardware used for bitcoin mining from CPU to GPU to FPGA and finally to the ASICS. Some blockchain systems using non-PoW consensus only use CPU or rarely GPUs. To avoid centralization in ASIC and FPGA mining, some PoW cryptocurrencies such as Ethereum, Litecoin and Zcash develope memory hard algorithms that are unsuitable for mining with ASICs in order to allow users use their normal computers or GPUs [142].

Blockchain transforms from Bitcoin blockchain known as blockchain 1.0 to blockchain 2.0 which consists of smart contracts and Dapps. The next generation blockchain is predicted to be a blockchain of things [24]. More enterprise blockchain networks and platforms are been created to allow enterprises use blockchain other than public blockchain that is more suitable for their own requirements.

In 2014, Ethereum platform was formally announced and invented by Vitalik Buterin [143]. Ethereum unlike Bitcoin runs distributed applications (Dapps) known as smart contract using a Ether as its currency. Ethereum is used in many public blockchain applications ranging from DAO to IoT using smart contracts [144], [145]. As of January 2020, Ethereum has over 86 million users (unique addresses)[146]. After Bitcoin, Ethereum is the second highest public blockchain platform with its cryptocurrency Ether having a market capital of $20 Billion and pricing $190 as of February 2020.

Hyperledger project hosted by Linux foundation provides several open-source platforms for building enterprise blockchain applications and networks. Hyperledger was officially launched in 2016 with 30 founding corporate members under the Linux foundation [147]. The most popular Hyperledger platform is Hyperledger Fabric [148] which was contributed to the Hyperledger by IBM in 2015. Currently around 40% of enterprise blockchain networks use Hyperledger Fabric [12]. The Fabric can support over 3500 transactions per seconds [149]. Other Hyperledger platforms include the Hyperledger Sawtooth, Iroha, Indy, Burrow and Besu. Hyperledger Sawtooth allows for both permissioned and permissionless networks while Hyperledger Iroha focuses on mobile applications. Hyperledger Indy provides platform for distributed identity, Hyperledger Burrow is a permissioned smart contract virtual machine. Finally, the Hyperledger Besu is a Java based Ethereum client [150].

Corda [5] is another consortium blockchain platform provided by R3 [6] in 2016 for financial enterprises. Other blockchain platforms which are mostly consortium include the J.P. Morgan's quorum [151], Enterprise Ethereum Alliance [152], Multichain [153], Kadena [154], Axoni [155], SETL.io [156], Digital Asset Holdings[157] and clearmatics [158, 12]. Table 5 compares some of the existing popular blockchain platforms.

5.2. Breakthrough in industries and companies

Blockchain has achieved major breakthrough and adoptions in industries especially in 2018 and 2019. The year 2019 was termed as the year of enterprise blockchain adoption. Figure 12 depicts the forecasted timeline of blockchain adoption in industries from 2014. The ideation stage is the beginning, where ideas of using the blockchain in industries started to be generated. Proof of concepts were created to preliminarily test the generated ideas. After the PoC, many companies started prototypes and trials in 2016/2017. Many projects entered pilot stage in 2017/2018 while large number of them are currently moving to production phase. It has been believed that most blockchain projects will be in production stage around 2022. In the year 2025, blockchain will attain the mainstream adoption and be matured [159].

In this section, we discuss some major breakthrough and adoptions of blockchain classified into five periods of time starting from 2012. only Bitcoin existed prior to this time .

Table 5: Comparison of blockchain platforms

Platform	Blockchain Type	Consensus Supported	Currency Used	Language	Throughput (T/S)	Usage
Bitcoin	Permissionless	PoW	Bitcoin (BTC)	C++	3-4	Cryptocurrencies
Ethereum	Permissionless	PoW-PoS	Ether (ETC)	Solidity	15-20	Dapps, DAO
Hyperledger Fabric	Permissioned	PBFT,Kafka,Raft	No currency	Go,js,Java	20,000	Business networks
Corda	Permissioned	Raft,BFT-SMaRt	No currency	Kotlin,Java	up to 6300	Business networks
Ripple	Permissioned	Ripple	XRP	C++	1500	Currency exchange
Quorum	Permissioned	Raft,QuorumChain	JPM coin	Solidity	752	Business networks
Multichain	Permissioned	Multichain consensus	No currency	JavaScript	2000-2500	Business networks

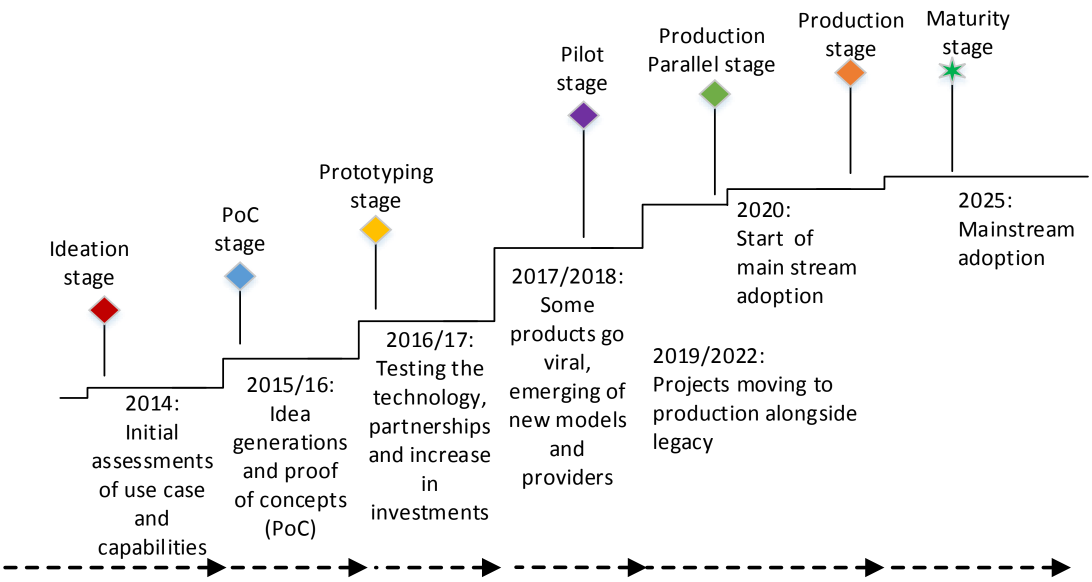

Ideation stage
PoC stage
Prototyping stage
Pilot stage
Production Parallel stage
Production stage
Maturity stage
2014: Initial assessments of use case and capabilities
2015/16: Idea generations and proof of concepts (PoC)
2016/17: Testing the technology, partnerships and increase in investments
2017/2018: Some products go viral, emerging of new models and providers
2019/2022: Projects moving to production alongside legacy
2020: Start of main stream adoption
2025: Mainstream adoption

Figure 12: Timeline for blockchain adoption in industries

1. **2012 - 2014:**
In this period, no much activities of blockchain in companies. Companies using blockchain at this time mainly use it for cryptocurriences and its exchanges. An example of such companies are Coinbase, Coinsetters and PeerCoin which opened in 2012 and 2013 respectively.

2. **2014 - 2016:**
Some companies started realizing the benefits of blockchain mostly after the launch of Ethereum in 2014. NASDAQ started using blockchain since 2014 for stock exchange. In 2015, NASDAQ unveiled the Nasdaq Linq blockchain for keeping security records. They further collaborate with Citi to develop a blockchain payment solution [160].
In 2015, IBM and Samsung unveiled the Autonomous Decentralized Peer to Peer Telemetry (ADEPT) platform using proof of concept with blockchain. ADEPT connects IoT devices and allows them to communicate between themselves for autonomous maintenance, self-services, upgrades and updates. Samsung washing machine (W9000) connected to ADEPT ordered for detergent from a retailer when the detergent went low. The washing machine checked its warranty information and even paid for the bills using smart contract [161].
Also in this period, Gem, Storj and Augur were founded. Gem uses blockchain for healthcare, Storj is a decentralized cloud storage, Augur uses blockchain for market predictions however fully relaunched in 2018. Bitshares is a Cryptocurrency exchange company also founded in 2014.

3. **2016 - 2018:**
In October 2016, the first blockchain international transaction between banks was made by Wells Fargo and the Commonwealth Bank of Australia through the use of many blockchain applications different from Bitcoin. The transaction was for the shipment of 88 bales of cotton totaling $35,000

from U.S to China. It marked a great milestone for blockchain technology adoption in banks [116].

Microsoft in 2017 created an add-in for Microsoft office outlook which uses the so called Stampery API created to stamp and verify documents using the Bitcoin and Ethereum blockchain. The add-in helps customers to certify documents and emails from within the outlook app without going to the third party page for certification and authentication. The Stampery API embeds hash of a document in the blockchain which could later be used for the document certification [162].

IBM and Microsoft in 2017 unveiled their cloud blockchain platforms that is, the IBM blockchain and Microsoft Coco respectively. IBM blockchain is the first fully managed blockchain cloud service based on Hyperledger technology. It eases applications development, governance and operation of business networks. The Microsoft Coco framework was revealed later in August 2017. It integrates with several blockchain and distributed ledgers like the R3s Corda, Ethereum, JPMorgans quorum and Intels Sawtooth Lake. Microsoft decided to build this blockchain framework to enable business enterprise networks realize the enterprise requirements lacking in the pre-existing blockchain protocols in terms of performance, governance, desired processing power and confidentiality [163, 164].

R3 as a consortium consisting of over 200 financial institutions has been using blockchain since 2016 for trading, redeeming and issuance of fixed income products for adoption. R3 secured the ever highest distributed ledger technology (blockchain) investment of $107m in 2016 from its over 40 member institutions across 15 countries. Corda partners with other companies to provide blockchain solutions. They also provide contract management blockchain solution for contractors [43, 22, 165].

There was wider acceptance of cryptocurrencies by companies like World Press, Microsoft and Dell. More than 100,000 merchants accept Bitcoin worldwide since 2015 [22, 166]. Wepower, Settlemint, Enerchain, PowerLedger and Electrify.Asia are energy trading platforms using blockchain since 2016 and 2017. Survey made by Cambridge university in 2017 revealed that 67% of central banks were experimenting with blockchain and many of them now reported successful trials [89].

4. **2018 - 2020:**

In May 2018, the giant automobile companies and largest automakers in the world (i.e. BMW, Ford, Renault and GM) formed a consortium in collaboration with blockchain developer (Hyperledger and Consensys), IBM, Accenture and some manufacturers of car-parts (ZF and Bosch) for using blockchain in automobile industry. The consortium called the Mobility Open Blockchain Initiative (MOBI) will be looking at using blockchain for payments and data sharing between cars by using some common standards developed with the blockchain. Other target areas include data generated by cars from their sensors. This data could be efficiently harnessed using the blockchain [167].

Oracle followed its counterparts such as Microsoft and unveiled its giant autonomous cloud blockchain platform (OABCS). The company intended to attract small and big firms to use blockchain for business networks. Oracles also provide several blockchain solutions on their cloud platform. They provide contract management solution for construction companies and others [168].

FedEx have been exploring and using blockchain for tracking high-value cargoes. They are currently working to extend the use of blockchain and IoT for the other logistics. In 2018, FedEx Institute of Technology partnered with Good Shepherd Pharmacy in a project called REMEDI which uses blockchain to trace and collect unused cancer medicines to be distributed to poor cancer patients across the world. FedEx is among the top freight logistic companies and has joined the Blockchain in Transport Alliance (BiTa) in 2018. BiTa coordinates and promotes the use of blockchain among the transport and freight industries [169].

In September 2018, a Korean carrier LG Uplus, arm of LG Corporation announced its trial for an overseas payment service based on blockchain in 2019. The company is collaborating with partners in United State (TBCASoft), Taiwan (Far EasTone Telecommunications) and Japan (SoftBank) to provide the cross barrier payment system (CCPS) based on blockchain platform. The payment service is aimed at avoiding the high international transaction costs associated with credit cards and also making payments faster. Subscribers of the companies (excluding TBCASoft) will enjoy the international payments within Taiwan, Korea and Japan with less charges and faster settlement provided by the CCPS [170]

In October, 2018, Healthbank revealed their project of using blockchain healthcare. Currently, Icertis, Monax, and Konfidio use blockchain for efficient contract management on cloud. Securitize, Harbor, Polymath, AlphaPoint and TrustToken are blockchain based solutions for asset tokenization. Several companies also use blockchain for identity management, Blockpass, Civic, Selfkey, Shocard and Zamna are another blockchain based solutions used for validation and digital identities.

The Australian Security Exchange (ASX Ltd) released its new implementation plan for replacement of its clearing and settlement system the Clearing House Electronic Subregister System (CHESS) with blockchain. The commencement date is postponed to start March to April 2021. This will make ASX the first exchange in the world to use blockchain. The decision was made after two years of successful testing with the blockchain in order to reduce cost for their customers in addition to increased speed, simplicity and efficiency [104].

The shipping giant Maersk and IBM in August 2018 launched a blockchain based supply chain shipping tracking platform *TradeLens*. The platform was aimed for reducing costs, information sharing and increased the efficiency of the global ocean shipment supply chain [171, 172]. In July 2019, Maersk announced that other major shipping companies Hapag-Lloyd and Ocean Network Express will join TradeLens after MSC and CMA-CGM joined two month earlier. TradeLens now covers almost half of the global ocean shipping industry. Over

100 shipping operators partners in TradeLens including the top global shipping companies [135].

Towards the middle and the end of 2019, stablecoins took alot of media attention. Facebook's stablecoin Libra [10] planned to be launched in 2020 took the highest media news coverage. While the giant fintech company JPMorgan (JPM) proposed its stablecoin JPM coin, Walmart secured a digital currency patent. Walmart together with other nine food industries are partnering with IBM for using blockchain in food logistics and supply chain.

Barclays bank and Swiss bank have been experimenting with blockchain to improve settlement time which could save them 20 billion USD middlemen costs. Barclays in May 2019, invested in a blockchain based peer to peer payment startup, Crowdz. Crowdz works with companies for digital invoice automation and payment collection [173].

The giant bank Wells Fargo and the communication tech leader Verizon have all revealed their plan for using blockchain. Wells Fargo is going to have its own cryptocurrency for use in its internal banking. On the other hand, Verizon have applied for a patent which will allow it issue virtual sim card vSIM on blockchain [174].

Recently on 27th February 2020, the cybersecurity company Karspersky unveiled their blockchain based voting machine prototype which is first of its kind. The voting machine was built on top of their Polys online election system created last year now integrated with blockchain technology. Voters will be issued with token or QR code which they will use to cast their votes in polling centres or using their mobile phones or computers. The voters can also verify if their votes are recorded on the blockchain. Universities, businesses, political parties and governments can all use the voting platform fo r free and fair elections [175]. With the blockchain the election is believed to be more transparent and secure.

5. **ParallelChain and future adoptions:**

In the future we envisage more adoptions of blockchain. In the Deloitte's 2019 survey, 86% of the respondents believed that blockchain will finally get mainstream adoption. Many trials and projects are expected to get completed in 2020 [13].

ParallelChain is a next generation hybrid private blockchain with very high performance and scalability. The blockchain can achieve speed of 100,000 transaction per second which is around much higher than its counterparts like Hyperledger and Corda. ParallelChain is interoperable and possesses both permissioned and permissionedless features in a private blockchain in order to improve the shortcomings of the counterpart blockchains such as Bitcoin and Hyperledger. ParallelChain is the only blockchain platform/fabric that offers the feature of "right to be forgotten". ParallelChain can emulate the smart contract in Hyperledger and Ethereum and operate them faster than them operating in their native modes because of the high transaction rate of 100,000 TPS. Behind the ParallelChain, is a high performance parallel computing architecture that runs multiple parallel chains used by multiple applications concurrently.

Digital transaction limited (DTL) is a Hong Kong based company and the owner of the ParallelChain. They provide high performance industry specific blockchain solutions on ParallelChain. Such solutions are typical parallel chain use cases for business applications. DTL provides killer applications namely; ChattleChain, ConstructionChain and PreventiveChain, partner applications (loyalty program and QR code verification) and custom decentralized applications on their high performance ParallelChain. ChattleChain is used for fast tokenization and fraud protection while ConstructionChain provides digital records for work inspection and work flow tracking [176].

Table 6: Adoption of blockchain in various industries

Company	**Blockchain usage**
R3	Corda- blockchain platform for finance
IBM	IBM cloud blockchain platform, ADEPT
Microsoft	COCO - cloud blockchain platform
Oracle	OABCS - cloud blockchain platform
Facebook	Libra coin - Stable coin
Maersk	TradeLens - Shipping network
Wallmart	Digital currency patent, food supply chain
Wells Fargo	Internal stablecoin
Verizon	Blockchain virtual SIM patent
LG Uplus	Payment service
J.P Morgan	JPM coin - stable coin
BMW, Ford, Renault	MOBI - blockchain consortium
Healthbank, Gem	Healthcare management
Hyperledger	Enterprise blockchain platforms
Storj	Decentralize cloud storage solution
Grainchain	Blockchain trading solution for farmers
Verv, Grid+, Wepower, EWF, PowerLedger	Peer to peer energy trading and management
Blockstack, Namecoin	Decentralize DNS
BanQu	Cassava farming supply chain and trading
Spring Labs	Global B2B information sharing platform
Vechain, Kodakone	Intellectual property
CoverUS	Blockchain healthcare marketplace
Australian Security Exchange (ASX)	blockchain based clearing and settlement system
Monax, Konfidio, Icertis	Contract management
Kerspersky	blockchain voting platform/machine
Civic, Selfkey, Zamna	Identity management and validation
Digital transaction	ParallelChain solutions for businesses

Table 6 summarises the major blockchain adoptions by various industries. There are myriad number of blockchain adoptions in startups however, the table only selects major adoptions.

5.3. Breakthrough in various countries

Many countries have been experimenting and using blockchain for public services. Singapores government has been using blockchain to secure banks against invoice fraud. This prevents customers to duplicate invoices as it happened when almost $200 million were lost by the Standard Shartered due to the same act [177].

Georgia is the first government to keep land titles on Bitcoin blockchain. Bitfurry had been working with the government of Georgia building a public land registry using blockchain technology since 2016. The project after successful tests has been expanded in 2017 to enable other land services like sells, mortgage, new land title and notary[178]. Another company (Factom) has been aiming to build a blockchain based secure land registry for the Honduras government. The company has been in talks with the government since 2015 [179].

UK Government in September 2017 awarded a contract to a startup company *Electron* for trying blockchain solution in power grid balancing. In January 2018, Japanese giant power company (TEPCO) invested in the Electron for using blockchain in the energy industry [180, 181]. Beside the Electron there are myriad number of companies and startups currently using blockchain for energy services [182]. UK earlier disclosed that it was testing blockchain for its land registry as Sweden went far on its second phase trial of the blockchain for land registry [128].

In the mid-2018, United Arab Emirate (UAE) launched it blockchain strategy 2021. It was hoping that by 2021 50% of the UAE government transactions will be based on blockchain, hence therefore regulations were set for using crypto assets such as cryptocurrencies [183]. Earlier in December 2017, the central bank governor of the UAE disclosed that the UAE was collaborating with the Saudi Arabia government with a view of creating their own cryptocurrency for their central banks. The digital currency will be used for efficient cross-border transactions between banks in the two countries[184].

In another hand, the Swedish land registry is starting blockchain transaction for land trades after successful testing for two years[185].

The Moscow government in August 2018 disclosed its plan to use Ethereum blockchain to upload applications by over 20,000 farmers for allocation of trading plots for 2019 farmers market in Moscow. This is to allow transparency and credibility in the competitive application. Earlier in December 2017, the Russian government integrated blockchain in their Active Citizen e-Voting platform to allow citizens take part in taking decisions on city management and urban transformation. There is also further plan to extend blockchain for healthcare in Russia [186].

Malta is the first country in the world to pass regulatory law supporting cryptocurrencies and other blockchain applications. For this regulation, Malta is been referred as ”First blockchain Island”. Currently, more blockchain investments are rushing into Malta due to the inacted blockchain regulations. The governor of Colorado inaugurated the Colorado council for the advancement of blockchain Technology in 2018. The council in July 2019 reported the issues they identified on the adoption and regulation of the technology. The council also proposed possible solutions to the identified issues [187].

Table 7: Adoption of blockchain in various countries

Country	**Blockchain usage**
Georgia	Land registry
UAE	Bank payments, shareholder proxies, identity
Saudi Arabia	internal bank payments
USA	State archive, stock trade, birth and land registry, voting, healthcare
UK	Grants distribution, land registry and energy
Sweden	Estate transactions, land registry
Chile	Energy data tracking
Indonesia, Japan, Switzerland	Identity management
India	Land registry, education certification
South Korea	Banking ecosystem
Russia	trading plots allocation, e-Voting, secure trading, healthcare
Kenya	Education certification
Australia	Stock exchange, voting
Singapore	Trade invoice fraud protection
Mexico	Public contract and bidding
Ghana	Property ownership
Canada	Government funding
Malta	Cryptocurrency, DLT regulatory framework
Japan, South Korea	Voting
China	Digital currency, blockchain service network

The ID2020 Alliance unveiled their two pilot projects based on blockchain at September 14, 2018 ID2020 Summit in New York. The first project was a digital identification aimed for recording and verifying the identities of refugees in Thailand using iris recognition. The refugees digital identities will be used for healthcare services and later be extended to education. The second project was to facilitate the disbursement of subsidy from liquid propane gas (LPG) for Indonesian government using biometric digital wallet and blockchain [188].

China’s central bank announced in August 2019 that its cryptocurrency whose development started 5 years ago was almost ready. It is evident that the digital currency will be released as soon as possible in 2020. In April 2020, China will also launch a national blockchain service network (BSN) in 100 cities. The network is hoped to reduce the costs of businesses using blockchain in China by 80% and become a global standard [189, 190].

There are several other developments on blockchain [53]. Table 7 summarizes some of the blockchain adoptions in various countries across the world .

6. BLOCKCHAIN QUANTITATIVE SURVEYS AND ANALYSIS

There are various quantitative surveys and analysis on blockchain conducted by several organizations and departments. Quantitative surveys provide statistical and quantitative data on various aspects of blockchain such as state of adoption of the technology. The data is got from hundreds of participants through questionnaires, interviews or via emails. This section reviews the quantitative surveys on blockchain technology.

6.1. The quantitative Analysis and Surveys Sources

The Cambridge Centre for Alternative Finance conducted its second global benchmarking study on enterprise blockchain released in September, 2019. The study contacted and analysed 67 live and deployed enterprise blockchain networks that are already in production from 25 countries across the world. They also analysed data collected from over 160 enterprises across 49 countries world like. The enterprises include 60 blockchain vendors, 56 blockchain network operators and 45 public sectors such as central banks all coming from 25, 22 and 33 countries across the world respectively. These companies include start-ups, medium and large enterprises, other public sector institutions (OPSIS), government agencies and central banks. The method used for data collection ranges from direct survey through invitation by email, social networks and a help from R3 and Hyperledger companies [12].

In order to find out the way blockchain can most effectively be used, centre for social innovation, Stanford University surveyed 110 organizations through phone interviews and digital surveys. They reported findings based on six (6) sectors where blockchain is being used that is; Agriculture, finance, environment, governance, digital identity and finally the health sectors [191].

The giant fintech company, Deloitte interviewed 1386 top executives of high revenue companies in 12 countries for their 2019 global blockchain survey. They also surveyed a group of 31 firms with view of investing in blockchain technology [13].

PWC in their 2018 global blockchain surveyed 600 respondents who are executives in big business companies across 15 regions globally. Most of the respondents are involved with blockchain with 32% under development, and 15% running live project. However in 2019 saw many more adoptions and progress [192].

Ipsos is a leading market research company. In 2018 and 2019, Ipsos conducted a global research on internet security and trust including blockchain technology for the Centre for International Governance Innovation (CIGI). Over 10,000 people from 25 countries were surveyed through and online interview and face to face interview of approximately 10 and 20 minutes respectively [193].

Other blockchain statistical analysis studied include [194, 195, 196, 7, 197, 8, 198].

6.2. The quantitative survey findings

6.2.1. Analysis of current state of blockchain adoption

According to the survey findings, blockchain gets more and more adoptions with increasing use cases in 2019. The latest findings shown in Table 8 by Deloitte revealed that 86% of the respondents believed that blockchain will get finally mainstream adoption and is widely scalable [13]. Earlier survey by PWC [192] showed that 86% of 600 respondents were actively engaged with blockchain. Expectedly, enterprise blockchain gets more adoption now with many networks getting production ready state at the end of 2019. Figure 13 shows the state of adoption analysis for enterprise blockchain networks [12].

6.2.2. Survey of blockchain platforms in use

Generally speaking, Ethereum is the most widely used platform among both the permission and permissionless blockchains [191]. However, Hyperledger Fabric is the most used blockchain platform among the enterprise blockchain networks in deployment. Figure 14 shows the analysis of blockchain platforms as reported by [12, 191]. Earlier PWC survey [192] showed that 40% of the 389 respondents use permissioned blockchains such as the Hyperledger and Corda while 34% use permissionless blockchain. The rest 26% use the hybrid (consortium) blockchain.

6.2.3. Multi-party blockchain Vs blockchain meme networks

Multi-party blockchain networks run the blockchain as a fully distributed ledger technology (DLT) with multi-party consensus and shared record keeping. On the other hand, blockchain meme networks only implement some of the components of the DLT such as the cryptographic mechanisms without actually implementing the multi-party consensus. Many blockchain memes have the goal of becoming full multi-party blockchain systems in the near future. Findings by [12] revealed that most blockchain live networks (77% of 67 surveyed) are currently blockchain memes while 20% are considered potential multiparty DLTs. Only 3% are fully multi-party DLT networks.

6.2.4. Analysis of sectors using blockchain

Finance and Insurance industries are the dominant sectors where blockchain is being used. They host most of the live enterprise blockchain networks as well as the public blockchain networks [12, 192]. Figure 15 (a) and (b) show the surveys of sectors where blockchain technology is being currently used based on the findings of [12] and [192] respectively.

6.2.5. Analysis of blockchain use cases

Record verification and validation is the most common use case of blockchain generally speaking. However in enterprise blockchain atmosphere, supply chain tracking is the most widely used use case having 19% of the 67 live networks surveyed in [12]. Figure 16 (a) and (b) show the surveys of the blockchain use cases based on the findings of [191] and [12]

Table 8: Quantitative Analysis of blockchain Adoption

Survey Statement	**Response (%)**
Blockchain will get mainstream adoption	86%
Blockchain becomes our critical priority (in top 5)	53%
We are planning to replace our record systems	81%
We will lose competitive advantages without blockchain	77%
Our industry will be distrupted by blockchain	56%
Blockchain is overhyped	43%

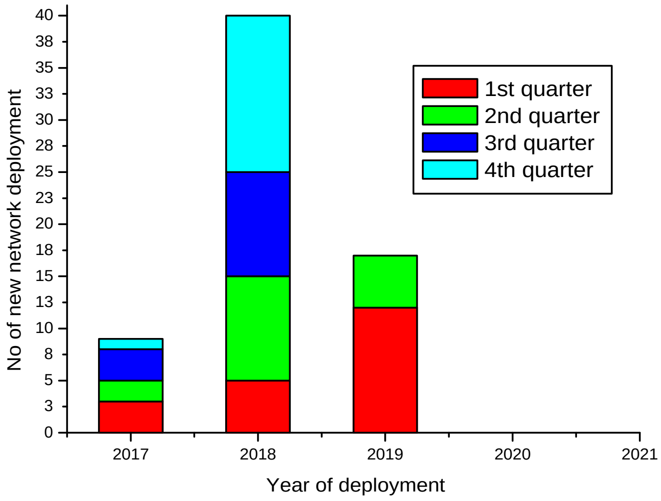


Figure 13: Survey of blockchain adoption between N=67 live networks

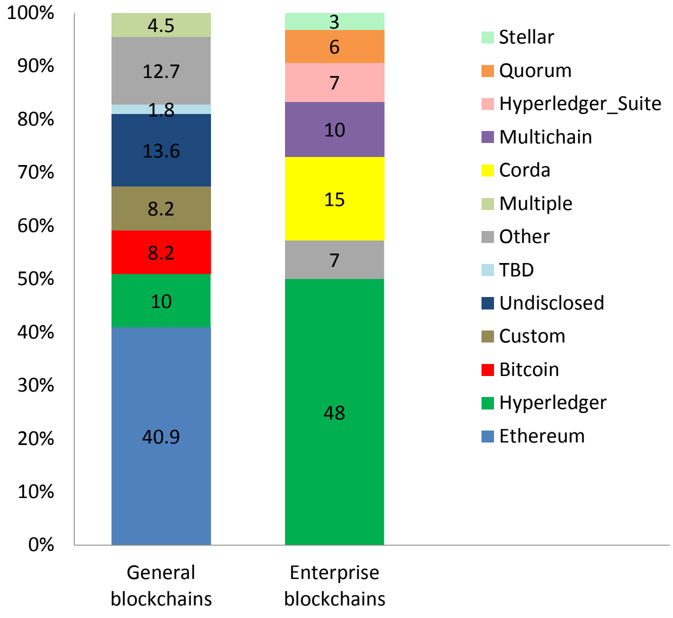


Figure 14: Blockchain platforms in use analysis

Table 9: Blockchain use cases Survey N=138

Use case	**Response (%)**	**Use case**	**Response (%)**
Data validation	43	Asset transfer	24
Data sharing	40	Revenue sharing	23
Identity	39	Asset backed tokens	22
Payments	37	Tokenized equity	21
Digital currency	36	Tokenized assets	20
Trade and trace	32	Time stamping	19
Certification	30	Custody	16
Access to IP	30	Not sure/other	2
Records reconciliation	25	None	1

respectively. Table 9 summarises the blockchain use cases analysis based on the findings of [13].

6.2.6. *Analysis of the Smart contract languages in use*

Most of blockchain projects (69%) use the existing general purpose smart contract languages such as Java and solidity. Others (56%) and (12%) use new general-purpose and fixed-purpose smart contracting languages [12].

6.2.7. *Enterprise blockchain consensus algorithms analysis*

As enterprise blockchain aimed for high scalability and performance PoW is undesirable. Currently, the Practical Byzantine Fault Tolerance (PBFT) consensus is the most widely used. Figure 17 shows the consensus algorithm survey for the enterprise blockchain platforms [12].

6.2.8. *Privacy and Confidentiality methods Analysis*

Different privacy preserving methods are being used in the existing blockchains. Zero Knowledge Proof (zk) is still in the experimental state and not used by many platforms. Restricted transaction visibility and the pseudonomous addresses are the most widely used privacy methods in enterprise blockchain networks. Figure 18 shows the analysis of the privacy-enhancing methods used in the existing enterprise blockchain platforms [12].

6.2.9. *Key Motivation/driver of enterprise blockchain networks*

Most of the existing enterprise blockchain networks currently target costs reduction [12, 197]. Survey findings in [12] shows that 72% of the respondents propose cost reduction, 8% new market models, 6% revenue generation and 14% hybrid propositions. In the analysis of 90 use cases [197], 70% of the immediate value targeted was cost reduction. However, Table 10 indicated that new revenue generation is the ultimate future goal and motivation for most of the companies [13].

Table 10: Key motivation for Enterprise blockchain N=138

Motivation	Response (%)
New revenue generation	43
Efficiency improvement across boundaries	62
Transparency improvement	62
Cost savings	55
Efficiency improvement within boundaries	26
Competitive advantages	14
Assets trading	10
Moral hazards reduction	5
Other	10

Table 11: Platform selection criteria N=138

Criteria	Response(%)	Criteria	Response(%)
Vendor maturity	52	Security	20
Scalability/Performance	44	Privacy/Confidentiality	24
Use case compatibility	24	Interoperability/extensibility	16
Costs	12	Open source	8
Unique features	8	Other	8

Table 12: Causes of blockchain project discontinuation Analysis 1

Cause	Response (%)
Cost	51
Unsure how to start	45
Lack of governance	45
Users not realize benfit	10
No executive buy-in	9
Compliance/Audit demands	7
Regular discomforts	6

Table 13: Causes of blockchain project discontinuation Analysis 2

Cause	Response(%)
Failed to realise tangible benefits	62
Privacy and confidentiality concerns	38
Not suitable for business case	25
Technical issues	19
Funding issues	12
No executive buy-in	12
Market competition	6
Other	31

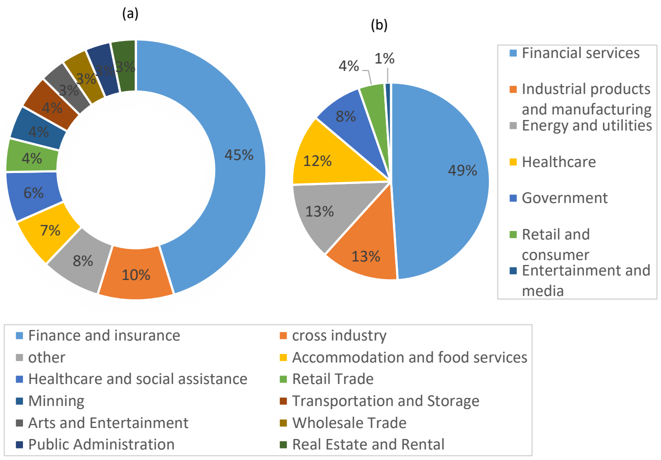


Figure 15: Survey of sectors using blockchain

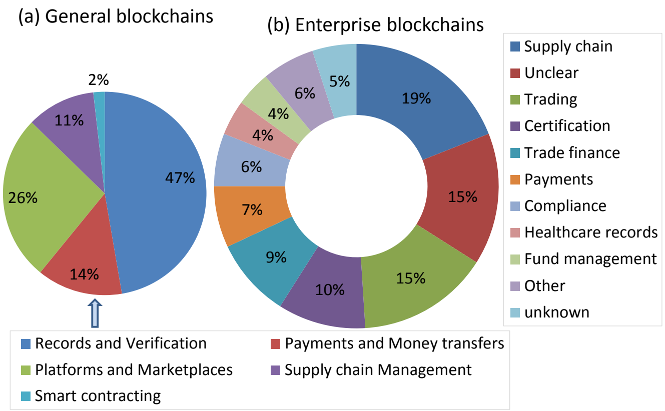


Figure 16: Blockchain use cases analysis

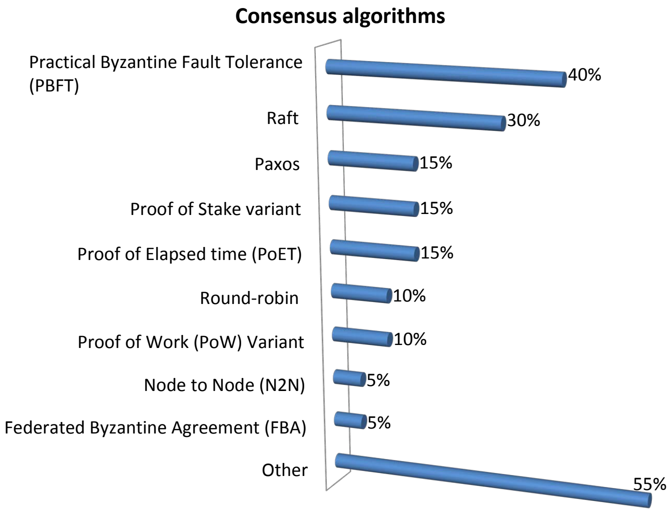


Figure 17: Consensus algorithms in enterprise blockchain platforms

6.2.10. Duration of blockchain project completion

It roughly takes 25 months on average to complete a blockchain project up to production. This includes the initial background study, the creation of the proof of concept (PoC),

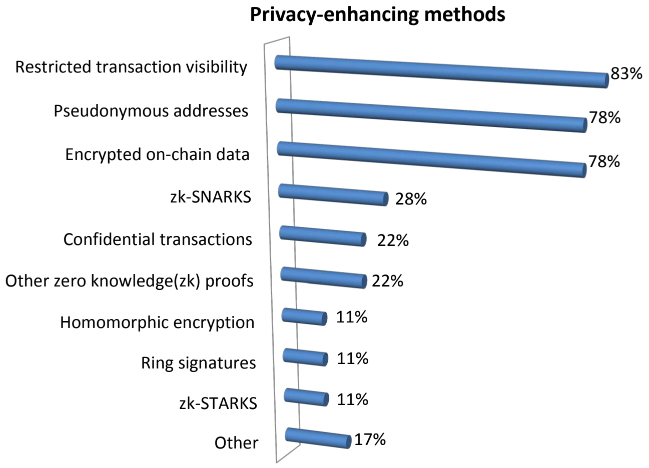


Figure 18: Privacy methods in enterprise blockchain platforms

Table 14: Survey of blockchain adoption inhibitors 1

Adoption inhibitor	Response(%)
Regulatory issue	30
Replacing/adapting existing legacy systems	30
Possible security threat	29
Uncertain benefit/return	28
Lack of understanding and skills	28
Fear of competitive information sensitivity	25
Lack of compelling application	23
Consortium formation challenges	22
Blockchain is unproven	20
Insufficient funding	20
Not our business priority	17
No barrier to adoption	8

pilot trial and the final production. Majority of the time (about 2/3) is spent in the PoC and the pilot trial state [12]. Majority of companies expect to reach customers in 6 months. According to Deloitte[13], many industries (47% of the respondents) expect 1-3 years to get a measurable return from an investment on blockchain. Other views (30%), (14%) and (6%) expected 3-5 years, less than a year, and greater than 5 years respectively.

6.2.11. *Criteria for platform selection*

Vendor maturity is the criteria mostly used for selecting a blockchain platform. Choosing a suitable is very essential to deriving the desired benefits in using blockchain technology. Table 11 shows Analysis of the criteria used for the protocol selection [12].

6.2.12. *Cause of blockchain project discontinuation*

Earlier survey shown in Table 12 by PWC [192] described costs and lack of know-how as the major reasons for discontinuing blockchain projects. However, more recent survey [12] shown in Table 12 revealed the failure of companies to realise significant benefits as the major reason. Such failure is due to the obstacles such as law regulation and lack of understanding of the technology.

Table 15: Survey of blockchain adoption inhibitors 2

Adoption inhibitor	Response(%)
Regulatory uncertainty	48
Users not trusting each other	45
Ability to integrate network	44
Interoperability	41
Scalability issues	29
Concerns for intellectual property	30
Concerns for Audit/compliance	20

6.2.13. *Overall satisfaction of existing blockchain*

Most of the live blockchain networks are satisfied by the results of their blockchain projects and its benefits. This is shown by Figure.

6.2.14. *Survey of obstacles impeding wider blockchain adoption*

Regulatory issues, lack of understanding are the biggest obstacles inhibiting the wider adoption of blockchain. Central banks and OPSIs consider blockchain hype as one of its adoption inhibitors due to fear of unrealistic expectation. Other inhibitors listed by the central banks include the lack of compelling use case, vendor inmaturity, lack of standardization and shortage of skilled blockchain developers. On the other hand, reluctance to replace the current systems, and shortage of skilled blockchain developers are the other inhibitors for the OPSIs. Performance and Scalability also blockchain adoption inhibitors [192, 12, 13]. About 68% of companies in Asia-pacific region do not trust blockchain due to lack of its understanding [198]. Table 14 and Table 15 summarises the survey data of blockchain adoption inhibitors according to [13] and [192] respectively.

6.2.15. *Other key survey findings*

Table 16 gives the summary of the other major quantitative survey findings [193, 194, 195, 196, 7, 197, 198]

7. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

Despite its strength and successes, blockchain technology has some challenges that hinder its full adoption in some areas. These challenges include[15], [32]:

Table 16: Summary of the other key quantitative survey findings

SN	Other survey findings
1	Blockchain is more secure than the existing IT systems according to 71% of survey respondents.
2	50% of blockchain vendor platforms are open-source
3	Efficiency, risk, time and cost savings are the main metrics used for measuring results of blockchain project.
4	About 22% of citizens in the world are familiar with blockchain technology
5	43% of blockchain networks are deployed as new technology stack.
6	71% of blockchain networks are founded by single organization
7	Poor understanding, reluctance to change current systems, and uncertain cost-benefits are the major operational challenges of blockchain
8	68% of 10000 people believe that blockchain technologies will affect all Economic sectors.
9	60% of those familiar with blockchain adviced for using blockchain in national elections.
10	48% of 740 agree that blockchain will likely disrupt their business in the next 3 years.
11	41% of 740 will likely implement blockchain in the next 3 years.
12	Global blockchain device market was forecasted to grow from $218 million to $1,285 million between 2019 and 2024.
13	Business value added by blockchain will reach more than $176 billion by 2025 and $3.1 trillion by 2030.
14	Most central banks are or will start experimenting with CBDC.
15	Morethan 40% of 1871 are very confident of blockchain industry.
16	Blockchain is not trusted by 68% of 576 Asia Pacific companies (excluding china) due to its lack of understanding

7.1. TECHNICAL CHALLENGES

1. **Scalability and throughput issues:**

Scalability and throughput issues are one of the biggest challenges of blockchain mostly found in public blockchains. The issues are caused by the long block interval and the large blockchain size (more than 261GB for Bitcoin) [140]. The earlier affects the transaction throughput while the later affects the response throughput of blockchain queries. The huge blockchain size discourages running full nodes especially by small devices such as IoT.

Blockchain applications lag much behind their counterparts like Visa and PayPal in terms of scalability and throughput. For example, Bitcoin and Ethereum handle 3-4 and 20 transactions per seconds respectively [199]. In comparison, Visa and PayPal handle 24,000 and 193 transactions respectively [200, 199]. The huge size of the blockchain also affect the blockchain read performance. For this reason, blockchain APIs like Blockcypher serving lightweight nodes with blockchain data lag so much when compared to non-blockchain counterparts like YouTube. For example Blockcypher has limit of only 3 requests per second while YouTube and Google achieve 67,620 searches and 74,256 views per second respectively [201].

Several approaches such as sharding, lightning network, sidechains, new consensus algorithms and changing the blockchain architecture were proposed for blockchain scalability.

2. **Security related issues:**

Some security threats and vulnerabilities have been found in blockchain applications especially public blockchains (mostly cryptocurrencies) despite the security of blockchain technology. Private and consortium blockchains are far more secure due to their restricted access and trusts. Scams, malware attacks, denial of service (DoS), Sybil attacks, application and network vulnerabilities are the commonly reported security issues. Loss of private keys due to the attacks, accidents or recklessness also causes huge security breaches[202, 203, 204, 3, 31]. Cryptocurrency worth $2 billion have been stolen mostly from exchanges since 2017 [205]. LedgerOPS in its 2018 blockchain security threat report [206] estimated such cryptocurrency losts to $1.604 billion in 2018 alone.

There were reports of attacks on Bitcoin, Ethereum and other altcoins with the famous ones on MtGox and DAO causing loss of 450 million USD and 60 million USD respectively. Bitfinnex exchange in Hong Kong suffered $72 million lost in 2016 and DoS attack in 2017 [31]. Money could also be stolen from cryptocurrencies through Border Gateway Protocol (BGP) attacks. About 83,000 USD was estimated to be lost from BGP attacks within just two months.

Blockchain using PoW consensus has vulnerability of 51% attack. The network can be attacked when a particular node or a mining pool possesses 51% of the network's computing power. With this immense power, the attacker can overcome the remaining nodes and successfully add false blocks that get into the main blockchain. The 51% attacker could censor transactions and carry out other forms of attacks such as double spending, DoS and eclipse attacks. The attack further weakens the security of the network by discouraging other miners from mining. GHash.IO Bitcoin mining pool once got 54% of the Bitcoin network computing power in July 2014. Due to public concerns, the pool had to shed its power before finally closing in 2016 [207, 95, 16]. Early 2019, Ethereum classic also experienced 51% attack where $1.1 million was suspected to be stolen. Gate.io confirmed losing $200,000 with about half was later returned after few days of the attack [205]. In 2018 alone, several cryptocurrencies such as ZenCash, Monacoin, Verge and Bitcoin Gold encountered 51% attack causing then to loss over $20 million [208].

Selfish mining is another security concern. Miners with bad intentions and a high computing power could refuse to publish their mined valid blocks until they aggregate a very long chain of blocks without competitors. By publishing their blocks, the new chain having their mined blocks becomes the longest chain and subsequently get accepted as the main chain. As a result, the other valid blocks mined by the honest miners before the selfish mined blocks gets rejected. Selfish mining discourages other honest miners from mining and causes them to incur losses. Hence the scalability and security of the network gets affected with the fewer miners and many selfish miners [209, 210, 211].

Vulnerabilities sometimes exist in blockchain programming and smart contracts. Such vulnerabilities lead to attacks such as the over $60 million Ethereum DAO's attack (The DAO) in 2016 which caused the hard fork on the Ethereum network [212, 213, 214]. Out of 19,366 Ethereum smart contracts 8,833 were found to be vulnerable to potential security bugs [215].

Other forms of attacks possible on blockchain include the double spending, eclipse attacks, DNS hijacking, consensus delay, liveness and balance attacks [38]. Marcus [204] uncovered eclipse attack threats on Ethereum which are similiar to those in found on Bitcoin [216]. Li [38] extensively surveyed the security of blockchain systems. Conti [16] presented a detailed survey of the privacy and security issues in Bitcoin. Atzei [214] surveyed the vulnerabilities and attacks on Ethereum while Saad [31] further explores attacks on blockchain. Several proposals were made to curtail the security issues in blockchain. Trustchain [217] was proposed as a sybil resistant and scalable blockchain. SmartPool was proposed to prevent 51% attack in mining pools [218]. A DDoS solution architecture was proposed by Rodrigues [219]. Other security counter measures were also proposed in [220, 221, 222, 215].

3. **Privacy issues:**

Even though the blockchain tried to be anonymous or pseudonymous, the physical identity of users could be revealed over critical analysis of the transactions from a particular node or by the analysis of the network activities and the blockchain data. [223, 224, 15]. Alternatively, the user's IP addresses could be extracted and linked with the user's wallet thus breaking their privacy[225, 3]. Goldfeder [226] demonstrated how web cookies (third party trackers) could be used to uncover user's original identity upon online payments with cryptocurrencies.

Various methods of solving the privacy issues on blockchain have been proposed. In one category, intermediary is used to provide exchange of the identity with another identification such as voucher to evade privacy detection [227, 228, 228, 229, 230, 231, 126]. Another category of authors propose methods to enhance the existing privacy methods while some authors propose new cryptographic method for the privacy provision in blockchain [232, 233].

Zero-Knowledge proofs such as Zero Knowledge Succinct Noninteractive Argument of Knowledge (ZK-SNARKs), Idemix and AZTEC are cryptographic protocols for enhancing privacy in blockchain. They allow blockchain transactions to be verified without revealing the transaction details (addresses and data) [234, 235]. Conti [16] is a survey of privacy issues on Bitcoin while Merve [26] gives a comprehensive survey of privacy and anonymity in Bitcoin-like cryptocurrencies.

Zcash and some cryptocurrencies and is based on the zero knowledge proof (ZK-SNARKs) to guarantee privacy [236, 234]. Vitalik Buterin proposed the use of the ZK-SNARKs to scale asset transfer on Ethereum up to 500 transactions per second [237]. A privacy solution API on Ethereum (AZTEC) uses ZKP protocol AZTEC for privacy provision [238]. Hyperledger Fabric and Indy also use a ZKP variant protocol known as the identity mixer(Idemix) for privacy [239]. Further researches on the existing and new privacy and anonymity methods is still demanded for better performance and security of the methods. Figure 18 shows the privacy enhancing methods used by enterprise blockchain networks [12]. The Figure shows that restricted transaction visibility is the most widely used in the enterprise blockchain network unlike the zero knowledge proof which is considered still experimental for enterprises.

4. **Usability:**

Swan [240] opined that blockchain APIs are difficult to use from the developers perspective even though some software can parse and extract information from the blockchain.

5. **Quantum computing threat:**

There are many researches and projects going on quantum computing . Some companies like Google, Rigetti, IBM and Microsoft have been working to create a commercial quantum computer that much out performs the speed of the current computers. On October 2019, Google announced that achieved quantum supremacy by doing in 200 seconds, a task that would take supercomputers 10,000 years to achieve. [241, 242, 243].

Many blockchain use the elliptic curve digital signature (ECDSA) or the RSA which could easily be broken with quantum computers using algorithms of Shor and Grover. Kiktenko et al. [244] claimed that blockchain signatures are vulnerable to attacks using quantum computers and will be broken in future. Hence, they proposed a post quantum digital signature whose security is theoretical and rather unproven.

7.2. REGULATORY ISSUES

Lack of regulations is one of the greatest issues that empedes blockchain adoptions worldwide especially for central banks. According to the PWC's Survey 48% of the respondents chosed regulatory issues as the major setback for blockchain adoption [192]. Most governments are skeptical of legalizing blockchain activities especially the cryptocurrencies due to the fear of illegal activities and its impact on their national currencies. For this reason, many countries are considering creating their own digital currencies.

7.3. LACK OF UNDERSTANDING OF THE TECHNOLOGY

Another major setback for blockchain adoption is lack of understanding of the technology. Many people find it difficult to understand blockchain technology or do not trust it as they thought the technology is being used for illegal activities. Survey revealed that 68% of the 576 Asia pacific company (excluding China) do not trust blockchain because they lack understanding of the technology [198]. According to the Deloitte's 2019 survey of 1386 executives, 28% counted lack of understanding of blockchain as a major barrier of its greater adoption [13] .

7.4. RELUCTANCE TO CHANGE CURRENT SYSTEMS

It is natural to get reluctance when moving to a new system until its well matured. Blockchain too suffers from this issue. Many companies are reluctant to replace or modify their existing systems with blockchain. Out of the 1386 executives surveyed by Deloittes, 30% opined that reluctance to replace existing system is the greatest barrier to blockchain adoption [13].

7.5. FUTURE RESEARCH DIRECTION ON BLOCKCHAIN

There are many rooms for research on blockchain to make it more efficient, mature and beneficial.

1. **Scalability:**
Scalability of blockchain is a big issue but less researched compared to other blockchain aspects like the security [15]. There is a big opportunity to conduct researches on how to make blockchain more scalable. The throughput and latency issues of blockchain need to be further improved. Efficient ways to surmount the huge increasing size of the blockchain data should be studied and proposed.

2. **Big Data Analytics:**
The large data contained in blockchain create space for big data analytics of the blockchain. Other forms of big data storage for example using tensors, could also be enhanced to efficiently store and process the blockchain data for space, faster accessibility and other benefits.

3. **Blockchain Verification:**
With the advent of several blockchains created by different companies and communities, there is need to verify the blockchains for their authenticity in order to avoid fake blockchain creations[32]. Efficient and secured systems for blockchain authenticity verification are hence required.

4. **Blockchain Interoperability:**
Interoperability of blockchain is also an area to look into. Many of the different blockchain platforms may interoperate to enhance their security, operability and efficiencies. Blockchain should also be able to complement some compatible existing systems. Many companies want to adopt blockchain but do not like to abandon their existing systems without big problems. There is need to research the best way how the blockchain will work with existing systems in a company. It is also pertinent to research how different blockchain systems can effectively interoperate for mutual benefits.

5. **Efficient and Secure Consensus Protocols:**
There are many consensus algorithms for blockchain trying to replace the PoW consensus due its huge energy waste. However these alternative protocols come with new security issues or may be infeasible to implement in reality [245]. There is a research opportunity within the blockchain consensus protocols. Stronger and realizable protocols that are more secured than PoW with least energy consumption are the quest for future researches. More work needs to be done to ensure the right protocol is been used in the right applications [16].

6. **Post quantum blockchain cryptosystems:**
With the threat of quantum computers to blockchain security, there is a demand for an efficient and well proven post quantum digital signature schemes and other relevant studies to protect blockchain against all kind of threats of quantum computers. Having quantum computers affordable is a welcome development, however there is much need to protect systems like blockchain whose security could be breached by the computers.
There are other cryptographic systems (post-quantum cryptos) apart from ECDSA, RSA and DSA that have not been discovered to be affected by the quantum computers. Such systems exist in the hash based cryptography (e.g. Merkle signature system), code-based cryptography (e.g. McEliece public key system) and Symmetric key cryptography (e.g. AES). Others are found in the Lattice based cryptography (e.g. NTRU public key cryptosystem) and Multivariate quadratic public key systems. There is still room for research in ways to improve the usability (key size), efficiency and the confidence of such post-quantum cryptosystems for their use in blockchain against the post quantum computer threats [246]. There is also an opportunity in studying quantum channels as well as developing efficient post quantum consensus algorithms [244].

7. **Integrating blockchain with other technologies:**
Nowadays, artificial intelligence, IoT and cloud computing are other big directions that draw attentions from researchers. There is research opportunity in studying what and how blockchain could be efficiently integrated with such technologies. Integrating the blockchain in the appropriate AI, cloud computing and IoT systems may enhance the efficiency, security and the autonomy of the systems. The IBM's ADEPT is a suitable example use case where IoT devices can achieve

autonomous transactions (like auto repair, update and maintenance), better privacy and security [24].

8. CONCLUSION

Blockchain is a promising technology with immense benefits such as data security, cost savings, anonymity, speed, transparency, traceability and most importantly the eviction of intermediaries especially the central authorities. Blockchain is bringing digital revolution by disrupting many industries. Currently, there are many applications of blockchain beside cryptocurrencies with several adoptions from many countries and companies. We envisage more adoptions as the technology matures and many trials reveal successful results. It has been believed that blockchain will finally get mainstream adoption across the globe. In this paper we survey the breakthrough and the state of the art of blockchain technology covering recent developments in its adoptions, applications and challenges. We also review the details of the cryptography behind the blockchain technology. We review quantitative analysis of blockchain technology and finally outlined the future research directions of the technology.

References

[1] A. Farouk, A. Alahmadi, S. Ghose, A. Mashatan, Blockchain platform for industrial healthcare: Vision and future opportunities, Computer Communications 154 (2020) 223 – 235. doi:https://doi.org/10.1016/j.comcom.2020.02.058.
URL http://www.sciencedirect.com/science/article/pii/S014036641931953X

[2] J. Frizzo-Barker, P. A. Chow-White, P. R. Adams, J. Mentanko, D. Ha, S. Green, Blockchain as a disruptive technology for business: A systematic review, International Journal of Information Management 51 (2020) 102029. doi:https://doi.org/10.1016/j.ijinfomgt.2019.10.014.
URL http://www.sciencedirect.com/science/article/pii/S0268401219306024

[3] X. Wang, X. Zha, W. Ni, P. Liu, Y. G. Jay, X. Niu, K. Zheng, Survey on blockchain for internet of things, Computer Communications 136 (2019) 10 – 29. doi:https://doi.org/10.1016/j.comcom.2019.01.006.
URL http://www.sciencedirect.com/science/article/pii/S0140366418306881

[4] L. Mearian, What is blockchain? The most disruptive tech in decades, Computerworld (2017) 1–8.
URL https://www.computerworld.com/article/3191077/security/what-is-blockchain-the-most-disruptive-tech-in-decades.html

[5] R. G. Brown, The Corda Platform: An Introduction, Corda platform White Paper (2018) 1–21.
URL https://www.corda.net/wp-content/uploads/2018/05/corda-platform-whitepaper.pdf

[6] R3, The R3 Story (2018).
URL https://www.r3.com/about/

[7] D. Furlonger, R. Valdes, Practical blockchain: a gartner trend insight report (2017).
URL https://blockcointoday.com/wp-content/uploads/2018/04/Practical-Blockchain_-A-Gartner-Trend-Insight-Report.pdf

[8] Cisco, Blockchain by cisco - build trust-based business networks for digital transformation, Cisco Blockchain White paper (2018).

[9] A. Lannquist, Central banks and distributed ledger technology: How are central banks exploring blockchain today?, World Economic Forum White Paper (2019).
URL http://www3.weforum.org/docs/WEF_Central_Bank_Activity_in_Blockchain_DLT.pdf

[10] L. Association, Libra white paper (2019).
URL https://libra.org/en-US/white-paper/

[11] President xi jinping endorses developing blockchain technology in china (2019).
URL https://forkast.news/president-xi-jinping-endorses-developing-blockchain-technology-in-china/

[12] M. Rauchs, A. Blandin, K. Bear, S. B. McKeon, 2nd global enterprise blockchain benchmarking study, Cambridge Centre for Alternative Finance Available at SSRN (2019).
URL https://ssrn.com/abstract=3461765

[13] L. Pawczuk, R. Massey, J. Holdowsky, Deloitte 2019 global blockchain survey - blockchain gets down to business, Deloitte insights (2019).
URL https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf

[14] Cryptoreport, All Cryptocurrency Prices, Live Charts, and Market Data - Crypto Report (2019).
URL https://cryptoreport.com/all

[15] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, Where is current research on Blockchain technology? - A systematic review, PLoS ONE 11 (10) (2016) 1–27. doi:10.1371/journal.pone.0163477.

[16] M. Conti, E. Sandeep Kumar, C. Lal, S. Ruj, A survey on security and privacy issues of bitcoin, IEEE Communications Surveys and Tutorials 20 (4) (2018) 34163452. doi:10.1109/comst.2018.2842460.
URL http://dx.doi.org/10.1109/COMST.2018.2842460

[17] F. Tschorsch, B. Scheuermann, Bitcoin and beyond: A technical survey on decentralized digital currencies, IEEE Communications Surveys Tutorials 18 (3) (2016) 2084–2123. doi:10.1109/COMST.2016.2535718.

[18] D. Romano, G. Schmid, D. Romano, G. Schmid, Beyond Bitcoin: A Critical Look at Blockchain-Based Systems, Cryptography 1 (2) (2017) 15. doi:10.3390/cryptography1020015.
URL http://www.mdpi.com/2410-387X/1/2/15

[19] M. Nofer, P. Gomber, O. Hinz, D. Schiereck, Blockchain, Business & Information Systems Engineering 59 (3) (2017) 183–187. doi:10.1007/s12599-017-0467-3.
URL http://link.springer.com/10.1007/s12599-017-0467-3

[20] Z. Zheng, S. Xie, H.-N. Dai, H. Wang, Blockchain Challenges and Opportunities : A Survey, International Journal of Web and Grid Services (2017) 1–24doi:10125/41338.
URL http://inpluslab.sysu.edu.cn/files/blockchain/blockchain.pdf

[21] A. A. Monrat, O. Schelén, K. Andersson, A survey of blockchain from the perspectives of applications, challenges, and opportunities, IEEE Access 7 (2019) 117134–117151.

[22] O. Firica, Blockchain technology: Promises and realities of the year 2017, Quality - Access to Success 18 (October) (2017) 51–58.

[23] H. Vranken, Sustainability of bitcoin and blockchains, Current Opinion in Environmental Sustainability 28 (2017) 1–9. doi:10.1016/j.cosust.2017.04.011.
URL http://dx.doi.org/10.1016/j.cosust.2017.04.011

[24] L. Yang, The blockchain: State-of-the-art and research challenges, Journal of Industrial Information Integration 15 (2019) 80 – 90. doi:https://doi.org/10.1016/j.jii.2019.04.002.
URL http://www.sciencedirect.com/science/article/pii/S2452414X19300019

[25] A. Miglani, N. Kumar, V. Chamola, S. Zeadally, Blockchain for internet of energy management: Review, solutions, and challenges, Computer Communications 151 (2020) 395 – 418. doi:https://doi.org/10.1016/j.comcom.2020.01.014.
URL http://www.sciencedirect.com/science/article/pii/S0140366419314951

[26] M. C. Kus Khalilov, A. Levi, A survey on anonymity and privacy in bitcoin-like digital cash systems, IEEE Communications Surveys Tutorials 20 (3) (2018) 2543–2585. doi:10.1109/COMST.2018.2818623.

[27] L. S. Sankar, M. Sindhu, M. Sethumadhavan, Survey of consensus protocols on blockchain applications, in: 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), 2017, pp. 1–5. doi:10.1109/ICACCS.2017.8014672.

[28] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, D. I. Kim, A survey on consensus mechanisms and mining strategy management in blockchain networks, IEEE Access 7 (2019) 22328–22370. doi:10.1109/ACCESS.2019.2896108.

[29] M. Swan, P. de Filippi, Toward a Philosophy of Blockchain: A Symposium: Introduction, Metaphilosophy 48 (5) (2017) 603–619. doi:10.1111/meta.12270.

[30] M. Crosby, BlockChain Technology: Beyond Bitcoin, Applied Innovation Review Issue "" (2) (2016).

[31] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, A. Mohaisen, Exploring the attack surface of blockchain: A systematic overview, CoRR abs/1904.03487 (2019). arXiv:1904.03487.
URL http://arxiv.org/abs/1904.03487

[32] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017 (2017) 557–564doi:10.1109/BigDataCongress.2017.85.

[33] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, H. Janicke, Blockchain technologies for the internet of things: Research issues and challenges, IEEE Internet of Things Journal 6 (2) (2019) 2188–2204. doi:10.1109/JIOT.2018.2882794.

[34] K. Salah, M. H. U. Rehman, N. Nizamuddin, A. Al-Fuqaha, Blockchain for ai: Review and open research challenges, IEEE Access 7 (2019) 10127–10149. doi:10.1109/ACCESS.2018.2890507.

[35] G. Drakopoulos, E. Kafeza, H. Al Katheeri, Proof systems in blockchains: A survey, in: 2019 4th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), 2019, pp. 1–6. doi:10.1109/SEEDA-CECNSM.2019.8908397.

[36] K. Sharma, D. Jain, Consensus algorithms in blockchain technology: A survey, in: 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019, pp. 1–7. doi:10.1109/ICCCNT45670.2019.8944509.

[37] C. Cachin, M. Vukolić, Blockchain Consensus Protocols in the Wild, arXiv preprint arXiv:1707.01873 (2017). arXiv:1707.01873, doi:10.4230/LIPIcs.DISC.2017.1.
URL http://arxiv.org/abs/1707.01873

[38] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Generation Computer Systems (2017). arXiv:arXiv:1011.1669v3, doi:10.1016/j.future.2017.08.020.
URL http://dx.doi.org/10.1016/j.future.2017.08.020

[39] M. Belotti, N. BoÅi, G. Pujolle, S. Secci, A vademecum on blockchain technologies: When, which, and how, IEEE Communications Surveys Tutorials 21 (4) (2019) 3796–3838. doi:10.1109/COMST.2019.2928178.

[40] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, www.bitcoin.org (2008) 9arXiv:43543534534v343453, doi:10.1007/s10838-008-9062-0.
URL https://bitcoin.org/bitcoin.pdf

[41] Bitcoin.info, Bitcoinprice (2019).
URL https://bitcoin.info/

[42] Government Office for Science, Distributed Ledger Technology: beyond block chain, Tech. rep., "" (2016).
URL https://assets.publishing.service.gov.uk/government/uploads/system/\\uploads/attachment{_}data/file/492972/gs-16-1-distributed-ledger-technology.pdf

[43] B. insider, Estonia is using the technology behind bitcoin to secure 1 million health records (2016).
URL http://www.businessinsider.de/guardtime-estonian-health-records-industrial-blockchain-bitcoin-2016-3

[44] L. Xu, N. Shah, L. Chen, N. Diallo, Z. Gao, Y. Lu, W. Shi, Enabling the Sharing EconomyPrivacy Respecting Contract based on Public Blockchain, Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts - BCC '17 (2017) 15–21arXiv:1803.03567, doi:10.1145/3055518.3055527.
URL http://dl.acm.org/citation.cfm?doid=3055518.3055527

[45] H. Van Steenis, B. L. Graseck, F. Simpson, J. E. Faucette, Global Insight: Blockchain in Banking: Disruptive Threat or Tool?, Morgan Stanley Research (2016) 1–31.
URL http://www.ameda.org.eg/files/Morgan-Stanley-blockchain-report.pdf

[46] L. Cocco, A. Pinna, M. Marchesi, Banking on blockchain: Costs savings thanks to the blockchain technology, Future Internet 9 (3) (2017) 1–21. doi:10.3390/fi9030025.

[47] Y. Guo, C. Liang, Blockchain application and outlook in the banking industry, Financial Innovation 2 (1) (2016) 24. doi:10.1186/s40854-016-0034-9.
URL http://jfin-swufe.springeropen.com/articles/10.1186/s40854-016-0034-9

[48] A. Narayanan, J. Clark, Bitcoin's academic pedigree, Communications of the ACM 60 (12) (2017) 36–45. doi:10.1145/3132259.
URL http://dl.acm.org/citation.cfm?doid=3167461.3132259

[49] A. Bayle, M. Koscina, D. Manset, O. Perez-Kempner, When blockchain meets the right to be forgotten: Technology versus law in the healthcare industry, in: 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), IEEE, 2018, pp. 788–792.

[50] R. Jurdak, A. Dorri, S. S. Kanhere, Protecting the right to be forgotten in the age of blockchain, "" (2018).
URL https://theconversation.com/protecting-the-right-to-be-forgotten-in-the-age-of-blockchain-104847

[51] V. Buterin, On Public and Private Blockchains (2015).
URL https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[52] I.-C. Lin, T.-C. Liao, A Survey of Blockchain Security Issues and Challenges, International Journal of Network Security 1919 (55) (2017) 653–659. doi:10.6633/IJNS.201709.19(5).01).
URL http://ijns.jalaxy.com.tw/contents/ijns-v19-n5/ijns-2017-v19-n5-p653-659.pdf

[53] FICCI-PWC, Blockchain: The next innovation to make our cities smarter, Tech. rep., "" (2018).
URL https://www.pwc.in/assets/pdfs/publications/2018/blockchain-the-next-innovation-to-make-our-cities-smarter.pdf

[54] J. Sliwinski, R. Wattenhofer, Abc: Asynchronous blockchain without consensus, "" (2019). arXiv:1909.10926.

[55] C. Dwork, M. Naor, Pricing via processing or combatting junk mail, in: E. F. Brickell (Ed.), Advances in Cryptology — CRYPTO' 92, Springer Berlin Heidelberg, Berlin, Heidelberg, 1993, pp. 139–147.

[56] M. Jakobsson, A. Juels, Proofs of Work and Bread Pudding Protocols(Extended Abstract), Springer US, Boston, MA, 1999, Ch. "", pp. 258–272. doi:10.1007/978-0-387-35568-9_18.
URL https://doi.org/10.1007/978-0-387-35568-9_18

[57] Z. Zheng, Z. Chen, Pool Strategies Selection in PoW-Based Analysis, IEEE Access PP (c) (2018) 1. doi:10.1109/ACCESS.2018.2890391.

[58] A. de Vries, Bitcoin's Growing Energy Problem, Joule 2 (5) (2018) 801–805. doi:10.1016/J.JOULE.2018.04.016.
URL https://www.sciencedirect.com/science/article/pii/S2542435118301776

[59] Powercompare, Bitcoin Mining Now Consuming More Electricity Than 159 Countries Including Ireland & Most Countries In Africa (2017).
URL https://powercompare.co.uk/bitcoin/

[60] S. King, Primecoin: Cryptocurrency with Prime Number Proof-of-Work, King, Sunny 4 (2) (2013) 6.
URL https://bravenewcoin.com/assets/Whitepapers/primecoin-paper.pdf

[61] V. Buterin, V. Griffith, Casper the Friendly Finality Gadget, arXiv preprint arXiv:1710.09437 (2017) 1–10arXiv:arXiv:1710.09437v2.

[62] H. Sukhwani, J. M. Martnez, X. Chang, K. S. Trivedi, A. Rindos, Performance modeling of pbft consensus process for permissioned blockchain network (hyperledger fabric), in: 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS), 2017, pp. 253–255. doi:10.1109/SRDS.2017.36.

[63] M. Castro, B. Liskov, et al., Practical byzantine fault tolerance mit, in: OSDI, Vol. 99, 1999, pp. 173–186.

[64] L. Seeley, B. IO, Introduction to sawtooth pbft, "" (2019).
URL https://www.hyperledger.org/blog/2019/02/13/introduction-to-sawtooth-pbft

[65] J. Kwon, TenderMint : Consensus without Mining, the-Blockchain.Com

6 (2014) 1–10.
URL tendermint.com/docs/tendermint.pdf

[66] N. Chalaemwongwan, W. Kurutach, State of the art and challenges facing consensus protocols on blockchain, International Conference on Information Networking 2018-Janua (2018) 957–962. doi:10.1109/ICOIN.2018.8343266.

[67] I. Bentov, A. Gabizon, A. Mizrahi, Cryptocurrencies without proof of work, in: Financial Cryptography and Data Security, Springer Berlin Heidelberg, Berlin, Heidelberg, 2016, pp. 142–157.

[68] L. Wang, X. Shen, J. Li, J. Shao, Y. Yang, Cryptographic primitives in blockchains, Journal of Network and Computer Applications 127 (2019) 43–58. doi:https://doi.org/10.1016/j.jnca.2018.11.003.
URL http://www.sciencedirect.com/science/article/pii/S108480451830362X

[69] Coinguides, What is ethash? a list of all ethash coins ethash pow algorithm, CoinGuides (2018).
URL https://coinguides.org/ethash-coins/

[70] A. Biryukov, D. Khovratovich, Equihash: Asymmetric proof-of-work based on the generalized birthday problem, Ledger 2 (04 2017). doi:10.5195/LEDGER.2017.48.

[71] NISTb, Blockchain and Distributed Ledger Technologies: Opportunities, Challenges and Future Work (2017).
URL https://csrc.nist.gov/CSRC/media/Presentations/NIST-Block-Chain-Research-Project/images-media/ar-dy-blockchain-combined.pdf

[72] NIST, Secure Hash Standard (SHS), FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION CATEGORY: (FIPS PUB 180-4) (2015). doi:10.6028/NIST.FIPS.180-4.
URL http://dx.doi.org/10.6028/NIST.FIPS.180-4

[73] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, E. Wustrow, Elliptic curve cryptography in practice, IACR Cryptology (2014) 157–175doi:10.1007/978-3-662-45472-5_11.
URL http://link.springer.com/chapter/10.1007/978-3-662-45472-5{_}11

[74] S. Josefsson, I. Liusvaara, Edwards-curve digital signature algorithm (eddsa), in: Internet Research Task Force, Crypto Forum Research Group, RFC, Vol. 8032, 2017, p. "".

[75] L. Lamport, Constructing digital signatures from a one-way function, Tech. rep., Technical Report CSL-98, SRI International (1979).

[76] G. Maxwell, A. Poelstra, Borromean ring signatures, Accessed: Jun 8 (2015) 2019.

[77] D. Johnson, A. Menezes, S. Vanstone, The Elliptic Curve Digital Signature Algorithm (ECDSA), International Journal of Information Security 1 (1) (2001) 36–63. arXiv:arXiv:1011.1669v3, doi:10.1007/s102070100002.
URL http://link.springer.com/10.1007/s102070100002

[78] Certicom, Standards for Efficient Cryptography 2 (SEC 2) : Recommended Elliptic Curve Domain Parameters, Standards for Efficient Cryptography 2 (Sec 2) (2010) 37.
URL http://www.secg.org/sec2-v2.pdf

[79] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation 48 (177) (1987) 203–203. doi:10.1090/S0025-5718-1987-0866109-5.
URL http://www.ams.org/jourcgi/jour-getitem?pii=S0025-5718-1987-0866109-5

[80] V. S. Miller, Use of Elliptic Curves in Cryptography, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 218 LNCS (1986) 417–426. doi:10.1007/3-540-39799-X_31.

[81] H. Mayer, ECDSA Security in Bitcoin and Ethereum : a Research Survey, "" (2016) 1–10.

[82] S. William, Cryptography and Network Security: Principles and Practice , Sixth Edition, 6th Edition, Pearson Education, Inc., New York, 2014.
URL http://www.pearsonhighered.com/stallings/

[83] NIST, FIPS 186-2: Digital Signature Standard (DSS), FIPS PUB 186-2 2 (category: Computer Security) (2000).

[84] D. Hankerson, A. J. Menezes, S. Vanstone, Guide to Elliptic Curve Cryptography, Springer Science & Business Media, 2006. doi:10.1007/b97644.

[85] A. ANSI, X9. 62-1998: Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm (ecdsa), American National Standards Institute (ANSI), Washington, DC (1998).

[86] R. L. Rivest, M. Hellman, J. Anderson, J. Lyons, Responses to NIST's Proposal, Communications of the ACM 35 (7) (1992) 50–52. doi:10.1145/129902.129905.

[87] ISO, ISO/IEC 14888-3:1998-Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms (1998).
URL https://www.iso.org/standard/25996.html

[88] D. Lee Kuo Chuen, Handbook of digital currency : bitcoin, innovation, financial instruments, and big data, 1st Edition, Elsevier Inc, Amsterdam, 2015.
URL https://www.sciencedirect.com/science/book/9780128021170

[89] G. Hileman, M. Rauchs, 2017 Global Cryptocurrency Benchmarking Study, SSRN Electronic Journal 44 (0) (2017). doi:10.2139/ssrn.2965436.

[90] G. Bytes, Bitcoin and cryptocurrency atms, "" (2020).
URL https://www.generalbytes.com/en/

[91] O. Beigel, Who accepts bitcoin as payment?, "" (2020).
URL https://99bitcoins.com/bitcoin/who-accepts/

[92] P. Ciaian, M. Rajcaniova, d. Kancs, The economics of bitcoin price formation, Applied Economics 48 (19) (2016) 1799–1815.

[93] A. I. Sanka, R. C. C. Cheung, Efficient High Performance FPGA Based NoSQL Caching System for Blockchain Scalability and Throughput Improvement, in: 2018 26th International Conference on Systems Engineering (ICSEng 2018), Australia, IEEE, 2018, pp. 1–8. doi:10.1109/ICSENG.2018.8638204.

[94] N. Szabo, Formalizing and Securing Relationships on Public Networks, First Monday 2 (9) (sep 1997). doi:10.5210/fm.v2i9.548.
URL http://journals.uic.edu/ojs/index.php/fm/article/view/548

[95] D. Romano, G. Schmid, Beyond Bitcoin: A Critical Look at Blockchain-Based Systems, Cryptography 1 (2) (2017) 15. doi:10.3390/cryptography1020015.
URL http://www.mdpi.com/2410-387X/1/2/15

[96] A. Pinna, S. Ibba, G. Baralla, R. Tonelli, M. Marchesi, A massive analysis of ethereum smart contracts empirical study and code metrics, IEEE Access 7 (2019) 78194–78213. doi:10.1109/ACCESS.2019.2921936.

[97] M. Bartoletti, L. Pompianu, An empirical analysis of smart contracts: platforms, applications, and design patterns, CoRR abs/1703.06322 (2017). arXiv:1703.06322.
URL http://arxiv.org/abs/1703.06322

[98] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, J. Wan, Smart contract-based access control for the internet of things, IEEE Internet of Things Journal 6 (2) (2019) 1594–1605. doi:10.1109/JIOT.2018.2847705.

[99] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts, in: 2016 IEEE Symposium on Security and Privacy (SP), IEEE, 2016, pp. 839–858. doi:10.1109/SP.2016.55.
URL http://ieeexplore.ieee.org/document/7546538/

[100] A. Mense, M. Flatscher, Security vulnerabilities in ethereum smart contracts, in: Proceedings of the 20th International Conference on Information Integration and Web-Based Applications and Services, iiWAS2018, Association for Computing Machinery, New York, NY, USA, 2018, p. 375380. doi:10.1145/3282373.3282419.
URL https://doi-org.ezproxy.cityu.edu.hk/10.1145/3282373.3282419

[101] S. Rouhani, R. Deters, Security, performance, and applications of smart contracts: A systematic survey, IEEE Access 7 (2019) 50759–50779. doi:10.1109/ACCESS.2019.2911031.

[102] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, F. Wang, Blockchain-enabled smart contracts: Architecture, applications, and future trends, IEEE Transactions on Systems, Man, and Cybernetics: Systems 49 (11) (2019) 2266–2277. doi:10.1109/TSMC.2019.2895123.

[103] N. Biedrzycki, Will blockchain transform the stock market?, Data driven investor (2019).
URL https://www.datadriveninvestor.com/2019/04/09/will-blockchain-transform-the-stock-market/

[104] ASX, CHESS Replacement: New Scope and Implementation Plan, Response to consultation feedback (September 2018).
URL https://www.asx.com.au/documents/public-

consultations/response-to-chess-replacement-consultation-feedback.pdf

[105] K. O. . Obour Agyekum, Q. Xia, E. Boateng Sifah, S. Amofa, K. Nketia Acheampong, J. Gao, R. Chen, H. Xia, J. C. Gee, X. Du, M. Guizani, V-chain: A blockchain-based car lease platform, in: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1317–1325. doi:10.1109/Cybermatics_2018.2018.00228.

[106] M. Mettler, Blockchain technology in healthcare: The revolution starts here, 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services, Healthcom 2016 (2016) 16–18doi:10.1109/HealthCom.2016.7749510.

[107] A. A. Mazlan, S. Mohd Daud, S. Mohd Sam, H. Abas, S. Z. Abdul Rasid, M. F. Yusof, Scalability challenges in healthcare blockchain systema systematic review, IEEE Access 8 (2020) 23663–23673. doi:10.1109/ACCESS.2020.2969230.

[108] S. Wang, J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, Y. Guo, F. Wang, Blockchain-powered parallel healthcare systems based on the acp approach, IEEE Transactions on Computational Social Systems 5 (4) (2018) 942–950. doi:10.1109/TCSS.2018.2865526.

[109] K. Griggs, O. Ossipova, C. Kohlios, A. Baccarini, E. Howson, T. Hayajneh, Healthcare blockchain system using smart contracts for secure automated remote patient monitoring, Journal of Medical Systems 42 (7) (2018) 1–7.

[110] P. Zhang, J. White, D. C. Schmidt, G. Lenz, S. T. Rosenbloom, Fhirchain: Applying blockchain to securely and scalably share clinical data, Computational and Structural Biotechnology Journal 16 (2018) 267 – 278. doi:https://doi.org/10.1016/j.csbj.2018.07.004.
URL http://www.sciencedirect.com/science/article/pii/S2001037018300370

[111] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, B. Amaba, Blockchain technology innovations, in: 2017 IEEE Technology Engineering Management Conference (TEMSCON), 2017, pp. 137–141. doi:10.1109/TEMSCON.2017.7998367.

[112] A. Roehrs, C. A. Da Costa, R. Da Rosa Righi, Omniphr: A distributed architecture model to integrate personal health records, Journal of Biomedical Informatics 71 (2017) 70–81.

[113] T. McGhin, K.-K. R. Choo, C. Z. Liu, D. He, Blockchain in healthcare applications: Research challenges and opportunities, Journal of Network and Computer Applications 135 (2019) 62 – 75. doi:https://doi.org/10.1016/j.jnca.2019.02.027.
URL http://www.sciencedirect.com/science/article/pii/S1084804519300864

[114] R. Abujamra, D. Randall, Chapter five - blockchain applications in healthcare and the opportunities and the advancements due to the new information technology framework, in: S. Kim, G. C. Deka, P. Zhang (Eds.), Role of Blockchain Technology in IoT Applications, Vol. 115 of Advances in Computers, Elsevier, 2019, pp. 141 – 154. doi:https://doi.org/10.1016/bs.adcom.2018.12.002.
URL http://www.sciencedirect.com/science/article/pii/S006524581830069X

[115] M. Raikwar, S. Mazumdar, S. Ruj, S. Sen Gupta, A. Chattopadhyay, K. Y. Lam, A Blockchain Framework for Insurance Processes, 2018 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018 - Proceedings 2018-January (2018) 1–4. doi:10.1109/NTMS.2018.8328731.

[116] Reuters, Commonwealth and Wells Fargo Mark 1st International Blockchain Trade — Fortune (2016).
URL http://fortune.com/2016/10/24/commonwealth-bank-well-fargo-blockchain/

[117] A. Dorri, S. S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for iot security and privacy: The case study of a smart home, in: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2017, pp. 618–623. doi:10.1109/PERCOMW.2017.7917634.

[118] A. Boudguiga, N. Bouzerna, L. Granboulan, A. Olivereau, F. Quesnel, A. Roger, R. Sirdey, Towards better availability and accountability for iot updates by means of a blockchain, in: 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), 2017, pp. 50–58. doi:10.1109/EuroSPW.2017.50.

[119] M. Ali, R. Shea, M. J. Freedman, Blockstack: A New Decentralized Internet, Whitepaper "" (Version 1.0.1) (2017) 1–22.
URL https://blockstack.org/blockstack{_}whitepaper.pdf

[120] Namecoin, Decentralize all the things (2018).
URL https://namecoin.org/

[121] Emercoin, Emerdns, "" (2020).
URL https://emercoin.com/en/documentation/blockchain-services/emerdns/emerdns-introduction

[122] E. Karaarslan, E. Adiguzel, Blockchain based dns and pki solutions, IEEE Communications Standards Magazine 2 (3) (2018) 52–57. doi:10.1109/MCOMSTD.2018.1800023.

[123] S. L. Inc., Decentralized cloud object storage that is affordable, easy to use, private, and secure, "" (2019).
URL https://storj.io/

[124] R. E. Bansarkhani, M. Geihs, J. Buchmann, PQChain: Strategic Design Decisions for Distributed Ledger Technologies against Future Threats, IEEE Security & Privacy 16 (4) (2018) 57–65. doi:10.1109/MSP.2018.3111246.
URL https://ieeexplore.ieee.org/document/8425622/

[125] V. Saini, Storagepedia: An encyclopedia of 5 blockchain storage platforms, StoragePedia (2018).
URL https://hackernoon.com/storagepedia-an-encyclopedia-of-5-blockchain-storage-platform-8aa13c630ace

[126] R. Li, T. Song, B. Mei, H. Li, X. Cheng, L. Sun, Blockchain for large-scale internet of things data storage and protection, IEEE Transactions on Services Computing 12 (5) (2019) 762–771. doi:10.1109/TSC.2018.2853167.

[127] G. Foroglou, A. L. Tsilidou, Further applications of the blockchain, Conference: 12th Student Conference on Managerial Science and Technology, At Athens (2015) 0–8doi:10.13140/RG.2.1.2350.8568.

[128] A. Third, K. Quick, M. Bachler, P. John, Government services and digital identity, in: European Union Blockchain Observatory and Forum, 2018, pp. 1–52.

[129] Slock.it, Governance (voting/dao)., use cases (2019).
URL https://slock.it/use-cases/

[130] Fortune, Microsoft and Accenture Unveil Global ID System for Refugees (2018).
URL http://fortune.com/2017/06/19/id2020-blockchain-microsoft/

[131] T. Salman, M. Zolanvari, A. Erbad, R. Jain, M. Samaka, Security Services Using Blockchains: A State of the Art Survey, IEEE Communications Surveys & Tutorials (2018) 1–1doi:10.1109/COMST.2018.2863956.
URL https://ieeexplore.ieee.org/document/8428402/

[132] N. Kshetri, Blockchain's roles in strengthening cybersecurity and protecting privacy, Telecommunications Policy 41 (10) (2017). doi:10.1016/j.telpol.2017.09.003.

[133] S. Mire, Blockchain in cybersecurity: 11 startups to watch in 2019, Disruptor Daily (2019).
URL https://www.disruptordaily.com/blockchain-startups-cyber-security/

[134] B. Don, b. AG, S. Rajah, Dharma Ott, K. Fromm, Enterprise ethereum alliance real estate special interest group1real estate use casesfor blockchain technology, Enterprise Ethereum Alliance-Volume 1, 2019 (2019).
URL https://entethalliance.org/wp-content/uploads/2019/05/EEA-Real-Estate-SIG-Use-Cases-May-2019.pdf

[135] Maersk, Tradelens blockchain-enabled digital shipping platform continues expansion with addition of major ocean carriers hapag-lloyd and ocean network express, Accessed:January, 2020 (2020).
URL https://www.maersk.com/news/articles/2019/07/02/hapag-lloyd-and-ocean-network-express-join-tradelens

[136] Grainchain, Revolutionary blockchain platform for the agricultural business ecosystem fast and secured transactions for real commodities (2019).
URL https://www.grainchain.io/

[137] Ž. Turk, R. Klinc, Potentials of Blockchain Technology for Construction Management, Procedia Engineering 196 (June) (2017) 638–645.

doi:10.1016/j.proeng.2017.08.052.
URL http://dx.doi.org/10.1016/j.proeng.2017.08.052

[138] H. Hyvärinen, M. Risius, G. Friis, A Blockchain-Based Approach Towards Overcoming Financial Fraud in Public Sector Services, Business & Information Systems Engineering 59 (6) (2017) 441–456. doi:10.1007/s12599-017-0502-4.
URL http://link.springer.com/10.1007/s12599-017-0502-4

[139] M. Bedford Taylor, Bitcoin and the age of Bespoke Silicon, in: 2013 International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES), IEEE, 2013, pp. 1–10. doi:10.1109/CASES.2013.6662520.
URL http://ieeexplore.ieee.org/document/6662520/

[140] Blockchain Luxembourg S.A.R.L, Blockchain Size - Blockchain (2020).
URL https://www.blockchain.com/charts/blocks-size

[141] M. B. Taylor, Bitcoin and the age of Bespoke Silicon, 2013 International Conference on Compilers, Architecture and Synthesis for Embedded Systems, CASES 2013 (September 2013). doi:10.1109/CASES.2013.6662520.

[142] S. John, Getting started with Litecoins (after Bitcoin) - John Stevenson - Google Books, John Stevenson Publishing, 2013.

[143] V. Buterin, A next-generation smart contract and decentralized application platform, Etherum White paper (2014) 1–36doi:10.5663/aps.v1i1.10138.
URL http://buyxpr.com/build/pdfs/EthereumWhitePaper.pdf

[144] T. Gerring, Cut and try: building a dream - Ethereum Blog (2016).
URL https://blog.ethereum.org/2016/02/09/cut-and-try-building-a-dream/

[145] Ethereum Foundation, Ethereum Blockchain App Platform (2018).
URL https://www.ethereum.org/

[146] Etherscan, Ethereum unique address chart, Accessed: February, 2020 (2020).
URL https://etherscan.io/chart/address

[147] T. L. Foundation, About hyperledger, Accessed: Jan.2020 (2018).
URL https://www.hyperledger.org/about

[148] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, et al., Hyperledger fabric: A distributed operating system for permissioned blockchains, in: Proceedings of the Thirteenth EuroSys Conference, EuroSys 18, Association for Computing Machinery, New York, NY, USA, 2018, p. 15. doi:10.1145/3190508.3190538.
URL https://doi.org/10.1145/3190508.3190538

[149] IBM, Behind the architecture of hyperledger fabric, IBM Research Blog (2018).
URL https://www.ibm.com/blogs/research/2018/02/architecture-hyperledger-fabric/

[150] T. L. Foundation, About hyperledger, Accessed: Jan.2020 (2018).
URL https://www.hyperledger.org/

[151] Quorum, Evolve with quorum. the proven blockchain solution for business, Quorum (2019).
URL https://www.goquorum.com/

[152] E. E. Alliance, About the eea, Accessed: Jan.2020 (2020).
URL https://entethalliance.org/

[153] MultiChain, Enterprise blockchain. that actually works, Accessed: Jan.2020 (2020).
URL https://www.multichain.com/

[154] K. LLC, Kadena's feature set is the industry's future roadmap, Accessed: Jan.2020 (2019).
URL https://www.kadena.io/

[155] I. Schvey, Axonis distributed ledger technology provides secure, multi-party data infrastructure with unparalleled performance., Technology (2020).
URL https://axoni.com/technology/

[156] N. Pennington, An introduction to setl blockchain, SETL Blog (2019).
URL https://setl.io/blog/an-introduction-to-setl-blockchain/

[157] L. Digital Asset Holdings, Digital asset transforming the way multi-party applications are built and deployed, "" (2020).
URL https://digitalasset.com/

[158] C. T. LTD, Building the decentralised financial market infrastructure (dfmi) of the future, Clearmatics (2020).
URL https://www.clearmatics.com/about/

[159] C. Brennan, B. Zelnick, M. Yates, W. Lunn, Blockchain 2.0, Credit Suisse: Global Equity Research Technology (2018).

[160] P. Bajpai, How stock exchanges are experimenting with blockchain technology, "" (2018).
URL https://www.nasdaq.com/articles/how-stock-exchanges-are-experimenting-blockchain-technology-2017-06-12

[161] S. Panikkar, S. Nair, P. Brody, V. Pureswaran, ADEPT : An IoT Practitioner Perspective, "" (2015) 1–20.
URL http://ibm.biz/devicedemocracy

[162] Microsoft, Stampery Blockchain Add-in for Microsoft Office - Developer Blog (2017).
URL https://www.microsoft.com/developerblog/2017/04/10/stampery-blockchain-add-microsoft-office/

[163] A. Stanley, Oracle's Entrance: Database Giant Unveils Enterprise Blockchain Strategy - CoinDesk (2017).
URL https://www.coindesk.com/oracles-entrance-database-giant-unveils-enterprise-blockchain-strategy/

[164] R. Mark, Announcing the CoCo Framework for enterprise blockchain networks: Microsoft Azure (2017).
URL https://azure.microsoft.com/sv-se/blog/announcing-microsoft-s-coco-framework-for-enterprise-blockchain-networks/

[165] Corda, R3 secures record-breaking $107m investment from 40 institutions - corda.net (2017).
URL https://www.corda.net/2017/05/r3-secures-largest-ever-investment-distributed-ledger-technology-usd-107-million-40-institutions/

[166] Bitpay, Bitcoin: A New Global Economy (2018).
URL https://blog.bitpay.com/bitcoin-a-new-global-economy/

[167] Allison I., BMW, Ford, GM: World's Largest Automakers Form Blockchain Coalition - CoinDesk (2018).
URL https://www.coindesk.com/bmw-ford-gm-worlds-largest-automakers-form-blockchain-coalition/

[168] Oracle, Autonomous Blockchain Cloud Service : Oracle Cloud (2018).
URL https://cloud.oracle.com/en{_}US/blockchain

[169] R. Florea, How fedex is benefiting from blockchain technology, "" (2020).
URL https://blockchainflashnews.com/how-fedex-is-benefiting-from-blockchain/

[170] J. Ji-hye, LG Uplus to offer blockchain-based overseas payment service (2018).
URL http://www.koreatimes.co.kr/www/tech/2018/09/133{_}255620.html

[171] Tradelens, About tradelens, Accessed:January, 2020 (2020).
URL https://www.tradelens.com/about/

[172] M. White, Tradelens: powered by blockchain, ready to transform your supply chain, Accessed:January, 2020 (2018).
URL https://medium.com/tradelens-blog/tradelens-powered-by-blockchain-is-here-to-transform-your-supply-chain-f5e31525219

[173] cbinsight, Banking is only the beginning: 55 big industries blockchain could transform, Research Portal (2019).
URL https://www.cbinsights.com/research/industries-disrupted-blockchain/

[174] D. Moadel, Verizon and wells fargo are getting on the blockchain, Market realist (2020).
URL https://articles2.marketrealist.com/2019/09/verizon-wells-fargo-getting-on-blockchain/

[175] E. Daniel, Kaspersky unveils blockchain-based voting machine, Verdict Media Limited UK (2020).
URL https://www.verdict.co.uk/kaspersky-blockchain-voting/

[176] D. T. Limited, Digital transaction, "" (2020).
URL https://www.digital-transaction.com/

[177] Basu Medha, Singapore Government builds blockchain system to protect banks (2016).

URL https://govinsider.asia/smart-gov/singapore-government-builds-blockchain-system-to-protect-banks/

[178] L. Shin, The First Government To Secure Land Titles On The Bitcoin Blockchain Expands Project (2017).
URL https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/{\#}67aee1a04dcd

[179] Reason Foundation, Can Blockchain Technology Reduce Third-World Poverty? - Hit & Run : Reason.com (2016).
URL http://reason.com/blog/2016/04/30/bitfury-desoto-blockchain-land-registry

[180] De Nikhilesh, TEPCO Invests in Blockchain Startup in Bid to Decentralize Systems - CoinDesk (2018).
URL https://www.coindesk.com/tepco-buys-stake-uk-blockchain-startup-bid-decentralized-systems/

[181] Finextra, Electron wins UK Government Award to advance blockchain in balancin... (2017).
URL https://www.finextra.com/pressarticle/70874/electron-wins-uk-government-award-to-advance-blockchain-in-balancing-electricity-markets

[182] SolarPlaza, Comprehensive guide to companies involved in blockchian and energy, Blockchain Business (2018) 44.
URL http://ipci.io/wp-content/uploads/2017/12/Energy-Blockchain-Report.compressed.pdf

[183] A. Shafi, K. Patel, Cryptocurrency laws and regulations in UAE 2018 (2018).
URL https://www.vantageasia.com/cryptocurrency-law-uae/

[184] S. Carvalho, UPDATE 1-UAE, Saudi working on digital currency for cross-border deals (2017).
URL https://www.reuters.com/article/emirates-saudi-currency/update-1-uae-saudi-working-on-digital-currency-for-cross-border-deals-idUSL8N1OD2LP

[185] M. J. Zuckerman, Swedish Government Land Registry Soon To Conduct First Blockchain Property Transaction (2018).
URL https://cointelegraph.com/news/swedish-government-land-registry-soon-to-conduct-first-blockchain-property-transaction

[186] M. Custodio, Moscow Plans To Use Ethereum Blockchain To Increase Commerce Efficiency (2018).
URL https://blocktribune.com/moscow-plans-to-use-ethereum-blockchain-to-increase-commerce-efficiency/

[187] C. B. Council, Blockchain Council Report to the Community: Colorado Office of Economic Development and International Trade, ”” (2019).
URL https://choosecolorado.com/blockchain/

[188] ID2020 Alliance, ID2020 Alliance launches inaugural pilots, welcomes new partners at annual Summit (2018).
URL https://www.prnewswire.com/news-releases/id2020-alliance-launches-inaugural-pilots-welcomes-new-partners-at-annual-summit-300713089.html?tc=eml{_}cleartime

[189] Reuters, China’s sovereign digital currency is ’almost ready’: Pboc official, ”” (2020).
URL https://www.reuters.com/article/us-china-cryptocurrency-cenbank/chinas-sovereign-digital-currency-is-almost-ready-pboc-official-idUSKCN1V20RD

[190] N. Stockton, China launches national blockchain network in 100 cities, IEEE Spectrum (2020).
URL https://spectrum.ieee.org/computing/software/china-launches-national-blockchain-network-100-cities

[191] J. Galen, Doug, A. Abdualiyev, W. Chong, S. Iyer, R. Kim, J. Ma, D. Mann, E. Owen, G. Park, Junhyung (Edward)and Portelance, O. Seideman, N. Thakur, U. of Oregon Blockchain Club, Blockchain for social impact 2019, Centre for social innovation Stanford Graduate School of Business (2019).
URL https://www.gsb.stanford.edu/sites/gsb/files/publication-pdf/csi-report-2019-blockchain-social-impact.pdf

[192] P. China, PwC Global Blockchain Survey 2018 - Blockchain is here. Whats your next move?, research and insights (2018).
URL www.pwccn.com/global-blockchain-survey-2018

[193] F. O. Hampson, E. Jardine, Cigi-ipsos global survey on internet seurity and trust 2019 part 5: Cryptocurrencies, blockchain, bark web, product certification, Ipsos public affairs (2019).
URL https://www.cigionline.org/internet-survey-2019

[194] K. LLP, Kpmg technology industry innovation survey: Blockchain, ”” (2019).
URL https://assets.kpmg/content/dam/kpmg/us/pdf/2019/02/blockchain-tech-survey-2019-infographic.pdf

[195] C. Barontini, H. Holden, Proceeding with caution a survey on central bank digital currency, Bank for International Settlements (BIS) Papers No 101 (2019).
URL https://www.bis.org/publ/bppdf/bispap101.pdf

[196] Research, Markets, , ”” (2019).
URL https://www.researchandmarkets.com/reports/4841785/blockchain-devices-market-by-type-blockchain?utm_source=CI&utm_medium=PressRelease&utm_code=mjlgxq&utm_campaign=1300320+-+Global+Blockchain+Devices+Market+Report%2c+2019-2024&utm_exec=chdo54prd

[197] B. Carson, G. Romanelli, P. Walsh, A. Zhumaev, Blockchain beyond the hype: What is the strategic business value?, McKinsey Quarterly ”” (4) (2018) 118 – 127.
URL http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=133693412&site=ehost-live

[198] M. Huillet, Ey: Blockchain not understood by almost 70asia-pacific, https://cointelegraph.com/news/ey-blockchain-not-understood-by-almost-70-of-firms-in-asia-pacific (2019).

[199] Altcointoday, Bitcoin and Ethereum vs Visa and PayPal Transactions per second - Altcoin Today (2017).
URL https://altcointoday.com/bitcoin-ethereum-vs-visa-paypal-transactions-per-second/http://www.altcointoday.com/bitcoin-ethereum-vs-visa-paypal-transactions-per-second/

[200] Visa, Security and reliability (Visa speed) (2018).
URL https://usa.visa.com/run-your-business/small-business-tools/retail.html

[201] I. live stats, 1 Second - Internet Live Stats (2018).
URL http://www.internetlivestats.com/one-second/{\#}google-band

[202] S. Barber, X. Boyen, E. Shi, E. Uzun, Bitter to Better How to Make Bitcoin a Better Currency, Financial Cryptography, LNCS 7397 (2012) 399 414.
URL http://elaineshi.com/docs/bitcoin.pdf

[203] M. Vasek, M. Thornton, T. Moore, Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem, FC 2014 Workshops, LNCS 8438, pp. 5771, 2014. (2014) 57–71doi:10.1007/978-3-662-44774-1.
URL https://link.springer.com/content/pdf/10.1007{\%}2F978-3-662-44774-1{_}5.pdf

[204] Y. Marcus, E. Heilman, S. Goldberg, , ”” (2018) 15.
URL https://www.cs.bu.edu/%7Egoldbe/projects/eclipseEth.pdf

[205] M. Orcutt, Once hailed as unhackable, blockchains are now getting hacked, ”” (2019).
URL https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/

[206] LedgerOPS, Blockchain security threat report: 2018 review, ”” (2018).
URL https://documentcloud.adobe.com/link/track?uri=urn:aaid:scds:US:eae0e5e7-d798-4854-b3fa-4dae1686eb3f

[207] C. Farivar, Bitcoin pool ghash.io commits to 40breach, ARS Tecnica (2014). doi:10.1109/comst.2018.2842460.

[208] C. Ajay, Top five blockchain security issues in 2019 (2019).
URL https://ledgerops.com/blog/2019/03/28/top-five-blockchain-security-issues-in-2019

[209] C. Grunspan, R. Pérez-Marco, On profitability of selfish mining, CoRR abs/1805.08281 (2018). arXiv:1805.08281.
URL http://arxiv.org/abs/1805.08281

[210] J. Göbel, H. P. Keeler, A. E. Krzesinski, P. G. Taylor, Bitcoin blockchaindynamics: The selfish-mine strategy in the presence of propagation delay, Performance Evaluation 104 (2016) 23–41. arXiv:1505.05343, doi:10.1016/j.peva.2016.07.001.

URL http://dx.doi.org/10.1016/j.peva.2016.07.001

[211] I. Eyal, E. G. Sirer, Majority is not enough: Bitcoin mining is vulnerable, in: N. Christin, R. Safavi-Naini (Eds.), Financial Cryptography and Data Security, Springer Berlin Heidelberg, Berlin, Heidelberg, 2014, pp. 436–454.

[212] M. I. Mehar, C. L. Shier, A. Giambattista, E. Gong, G. Fletcher, R. Sanayhie, H. M. Kim, M. Laskowski, Understanding a revolutionary and flawed grand experiment in blockchain: the dao attack, Journal of Cases on Information Technology (JCIT) 21 (1) (2019) 19–32.
URL dx.doi.org/10.2139/ssrn.3014782

[213] X. Zhao, Z. Chen, X. Chen, Y. Wang, C. Tang, The dao attack paradoxes in propositional logic, in: "", 2017, pp. 1743–1746. doi:10.1109/ICSAI.2017.8248566.

[214] N. Atzei, M. Bartoletti, T. Cimoli, A survey of attacks on ethereum smart contracts (sok), in: M. Maffei, M. Ryan (Eds.), Principles of Security and Trust, Springer Berlin Heidelberg, Berlin, Heidelberg, 2017, pp. 164–186.

[215] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, A. Hobor, Making smart contracts smarter, in: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, 2016, pp. 254–269.

[216] E. Heilman, A. Kendler, A. Zohar, S. Goldberg, Eclipse attacks on bitcoin's peer-to-peer network, in: 24th USENIX Security Symposium (USENIX Security 15), USENIX Association, Washington, D.C., 2015, pp. 129–144.
URL https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/heilman

[217] P. Otte, M. de Vos, J. Poulwelse, TrustChain:A Sybil-resistant scalable blockchain, Future Generation Computer Systems 29 (5) (2017) 333–335. doi:10.1016/j.future.2017.08.048.
URL http://dx.doi.org/10.1016/j.future.2017.08.048

[218] L. Luu, Y. Velner, J. Teutsch, P. Saxena, Smartpool: Practical decentralized pooled mining, in: 26th USENIX Security Symposium (USENIX Security 17), USENIX Association, Vancouver, BC, 2017, pp. 1409–1426.
URL https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/luu

[219] B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, B. Stiller, A blockchain-based architecture for collaborative ddos mitigation with smart contracts, in: D. Tuncer, R. Koch, R. Badonnel, B. Stiller (Eds.), Security of Networks and Services in an All-Connected World, Springer International Publishing, Cham, 2017, pp. 16–29.

[220] B. Lee, J.-H. Lee, Blockchain-based secure firmware update for embedded devices in an internet of things environment, The Journal of Supercomputing 73 (3) (2017) 1152–1167. doi:10.1007/s11227-016-1870-0.
URL https://doi.org/10.1007/s11227-016-1870-0

[221] J.-W. Hu, L.-Y. Yeh, S.-W. Liao, C.-S. Yang, Autonomous and malware proof blockchain based firmware update platform with efficient batch verification for Internet of Things devices, Computers and Security 86 (2019) 238 – 252. doi:https://doi.org/10.1016/j.cose.2019.06.008.
URL http://www.sciencedirect.com/science/article/pii/S016740481831438X

[222] Z. Elkhadir, B. Mohammed, A cyber network attack detection based on gm median nearest neighbors lda, Computers and Security 86 (2019) 63–74. doi:https://doi.org/10.1016/j.cose.2019.05.021.
URL http://www.sciencedirect.com/science/article/pii/S0167404819301142

[223] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, S. Savage, A fistful of bitcoins: characterizing payments among men with no names, in: Proceedings of the 2013 conference on Internet measurement conference, 2013, pp. 127–140.

[224] A. Biryukov, D. Khovratovich, I. Pustogarov, Deanonymisation of clients in bitcoin p2p network, in: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, CCS 14, Association for Computing Machinery, New York, NY, USA, 2014, p. 1529. doi:10.1145/2660267.2660379.
URL https://doi.org/10.1145/2660267.2660379

[225] M. A. Harlev, H. Sun Yin, K. C. Langenheldt, R. Mukkamala, R. Vatrapu, Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning, in: Proceedings of the 51st Hawaii International Conference on System Sciences, 2018, p. "".
URL http://hdl.handle.net/10125/50331

[226] S. Goldfeder, H. Kalodner, D. Reisman, A. Narayanan, When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies, Proceedings on Privacy Enhancing Technologies 2018 (4) (2018) 179–199.

[227] E. Heilman, F. Baldimtsi, S. Goldberg, Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions, in: J. Clark, S. Meiklejohn, P. Y. Ryan, D. Wallach, M. Brenner, K. Rohloff (Eds.), Financial Cryptography and Data Security, Springer Berlin Heidelberg, Berlin, Heidelberg, 2016, pp. 43–60.

[228] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, E. W. Felten, Mixcoin: Anonymity for bitcoin with accountable mixes, in: N. Christin, R. Safavi-Naini (Eds.), Financial Cryptography and Data Security, Springer Berlin Heidelberg, Berlin, Heidelberg, 2014, pp. 486–504.

[229] E. Heilman, L. Alshenibr, F. Baldimtsi, A. Scafuro, S. Goldberg, Tumblebit: An untrusted bitcoin-compatible anonymous payment hub, in: Network and Distributed System Security Symposium, 2017, p. "".

[230] M. Green, I. Miers, Bolt: Anonymous payment channels for decentralized currencies, in: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 17, Association for Computing Machinery, New York, NY, USA, 2017, p. 473489. doi:10.1145/3133956.3134093.
URL https://doi.org/10.1145/3133956.3134093

[231] J. Camenisch, M. Drijvers, M. Dubovitskaya, Practical uc-secure delegatable credentials with attributes and their application to blockchain, in: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017, pp. 683–699.

[232] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, C. Rong, A comprehensive survey of blockchain: From theory to iot applications and beyond, IEEE Internet of Things Journal 6 (5) (2019) 8114–8154.

[233] T. Ruffing, P. Moreno-Sanchez, A. Kate, P2p mixing and unlinkable bitcoin transactions., in: NDSS, 2017, p. "".
URL https://eprint.iacr.org/2016/824.pdf

[234] D. Lavrenov, Zero-knowledge proof: Verifying blockchain transactions with less risk, Altros Report (2019) 26.
URL https://www.altoros.com/research-papers/zero-knowledge-proof-verifying-blockchain-transactions-with-less-risk/?utm_campaign=Hyperledger_org&utm_source=hlblog

[235] E. coin company, What are zk-snarks? (2019).
URL https://z.cash/technology/zksnarks/

[236] E. coin company, Zcash (2019).
URL https://z.cash/g

[237] V. Buterin, On-chain scaling to potentially 500 tx/sec through mass tx validation, Research (2018).
URL https://ethresear.ch/t/on-chain-scaling-to-potentially-500-tx-sec-through-mass-tx-validation/3477

[238] S. H. Ltd, The privacy engine on ethereum (2020).
URL https://www.aztecprotocol.com/

[239] Hyperledger, Msp implementation with identity mixer, Accessed: Dec.2019 (2017).
URL https://hyperledger-fabric.readthedocs.io/en/release-1.2/idemix.html

[240] M. Swan, Blockchain : blueprint for a new economy, 1st Edition, O'Reilly Media, Incorporated, Cambridge, 2015.
URL https://ebookcentral.proquest.com/lib/cityuhk/detail.action?docID=1929181

[241] D. Castelvecchi, Quantum computers ready to leap out of the lab in 2017, Nature 541 (7635) (2017) 9–10. doi:10.1038/541009a.
URL http://www.nature.com/doifinder/10.1038/541009a

[242] A. Bouguera, How will quantum computing affect blockchain?, Consensys-Blockchain Development (2019).
URL https://consensys.net/blog/blockchain-development/how-will-quantum-supremacy-affect-blockchain/

[243] E. Gibney, Inside Microsoft's quest for a topological quantum computer, Nature (oct 2016). doi:10.1038/nature.2016.20774.

URL http://www.nature.com/doifinder/10.1038/nature.2016.20774

[244] E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, A. S. Trushechkin, R. R. Yunusov, Y. V. Kurochkin, A. Lvovsky, A. Fedorov, Quantum-secured blockchain, Quantum Science and Technology 3 (3) (2018) 035004.

[245] A. Shoker, Brief Announcement : Sustainable Blockchains through Proof of eXercise, Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing (2018) 269–271doi:10.1145/3212734.3212781.
URL https://dl-acm-org.ezproxy.cityu.edu.hk/citation.cfm?id=3212781

[246] D. J. Bernstein, Introduction to post-quantum cryptography, in: Post-quantum cryptography, Springer, 2009, pp. 1–14.