IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 7, 2019, accepted July 28, 2019, date of publication August 19, 2019, date of current version September 4, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2936094

A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities

AHMED AFIF MONRAT, OLOV SCHELÉN, (Member, IEEE), AND KARL ANDERSSON, (Senior Member, IEEE)
Department of Computer Science, Electrical and Space Engineering, Lulea University of Technology, 931 87 Skelleftea, Sweden

Corresponding author: Ahmed Afif Monrat (ahmed.monrat@ltu.se)

The financial support for the research is provided by the Swedish Energy Agency under Grant 43090-2, and in part by the Cloudberry Datacenters.

ABSTRACT Blockchain is the underlying technology of a number of digital cryptocurrencies. Blockchain is a chain of blocks that store information with digital signatures in a decentralized and distributed network. The features of blockchain, including decentralization, immutability, transparency and auditability, make transactions more secure and tamper proof. Apart from cryptocurrency, blockchain technology can be used in financial and social services, risk management, healthcare facilities, and so on. A number of research studies focus on the opportunity that blockchain provides in various application domains. This paper presents a comparative study of the tradeoffs of blockchain and also explains the taxonomy and architecture of blockchain, provides a comparison among different consensus mechanisms and discusses challenges, including scalability, privacy, interoperability, energy consumption and regulatory issues. In addition, this paper also notes the future scope of blockchain technology.

INDEX TERMS Blockchain, distributed ledger, consensus procedures, cryptocurrency, smart contract, selfish mining, energy consumption.

I. INTRODUCTION

Unlike traditional methods, blockchain enables peer-to-peer transfer of digital assets without any intermediaries [1]. Blockchain was a technology originally created to support the famous cryptocurrency Bitcoin. Bitcoin was first proposed in 2008 and implemented in 2009 by Nakamoto [2]. Since then, it has seen huge growth with the capital market, reaching 10 billion dollars in 2016. Blockchain is basically a chain of blocks that store all committed transactions using a public ledger [3]. The chain grows continuously when new blocks are appended to it. Blockchain works in a decentralized environment that is enabled by comprising several core technologies, such as digital signatures, cryptographic hash, and distributed consensus algorithms. All the transactions occur in a decentralized manner that eliminates the requirement for any intermediaries to validate and verify the transactions [4]. Blockchain has some key characteristics, such as decentralization, transparency, immutability, and auditability [5].

Although Bitcoin is the most famous application of blockchain, it can be applied to diverse applications far beyond cryptocurrencies. Since it allows payments to be finished without any bank or any intermediary, blockchain can be used in various financial services, such as digital assets, remittance and online payment [6]. The blockchain itself has taken on a life of its own and permeated a broad range of applications across many industries, including finance, healthcare, government, manufacturing, and distribution [7]. The blockchain is poised to innovate and transform a wide range of applications, including goods transfer (supply chain), digital media transfer (sale of art), remote services delivery (travel and tourism), platforms for example, moving computing to data sources and distributed credentialing [8]. Additional applications of blockchain include distributed resources (power generation and distribution), crowdfunding, electronic voting, Identity management and governing public records.

Despite the fact that blockchain technology shows great potential that may replace many of the current digital platforms, it has some technical constraints. Scalability is a huge concern for blockchain based platforms [9]. In Bitcoin, the limited size and frequency of the blocks along with the number of transactions the network can process can be considered a scalability problem [10]. The average block creation time in Bitcoin is 10 minutes, and the block size is limited to 1 megabyte which constrains the network's throughput [11].

The associate editor coordinating the review of this article and approving it for publication was Chien-Ming Chen.

Bitcoin's ability to scale depends on the size of the block and is limited to the complexity of the mathematical puzzle independent of the nodes in the network. In general, the transaction processing capacity of Bitcoin is between 3.3 to 7 transaction per second [12]. However, due to the increased size of recently generated blocks, the transaction throughput is being effectively limited to 2-4 transactions per second, which is incapable of high-frequency trading. At present, there are more than 36 million wallet users, and with time, it will increase and create an adverse impact on the network's throughput. Different issues such as the blockchain congestion problem, transaction delays, and increased transaction fees will raise concerns. As a result, the technology may not be a sustainable approach for government or private sectors to build their business model upon the blockchain platform. Moreover, increased block size requires substantial storage space and cause slower propagation in the blockchain network [13], which will also lead towards centralization and trust issues as users would like to operate and maintain such a large blockchain. Therefore, it has become a great challenge to deal with the tradeoff between blockchain size and trust.

Blockchain has some other issues regarding interoperability, privacy, energy consumption, selfish mining, security, and regulation policy. The interoperability issue arises due to the lack of standard protocol for adopting and integrating blockchain-based solutions among companies. Privacy leakage may also happen within the blockchain, although the system claims to be extensively secured as users only make transactions with digital signatures that associate public-private key encryption [14]. Furthermore, it is possible to track the user's real IP address. Consensus mechanisms such as proof-of-work (PoW) and proof-of-stake (PoS) are also facing serious concerns. For instance, PoW is known for consuming a large extent of electrical energy due to the competitive nature of miners for creating blocks by solving complex mathematical puzzles [15]. In PoS, the rich become gradually richer as the chance of obtaining a block depends on how much stake the miners have [16]. Another drawback of blockchain technology is selfish mining, where miners can gain better revenue than their fair share by keeping their blocks private [17]. Blockchain can also suffer from 51% attacks, where some node attains the majority in a network and abuses it. Furthermore, it is believed that blockchain technology may not reach its peak or anticipated large-scale adoption by stakeholders because of uncertainties that arise with potential government regulations [18]. One of the major underlying reasons could be that the decentralized nature of blockchain eliminates intermediary links to central banks to control the economy, which does not bode well with the government. Hence, some measures need to be put forward to address these issues in blockchain.

This survey paper focuses on state-of-art blockchain studies including blockchain architecture, consensus algorithms, applications of blockchains, trade-off and challenges. The rest of this survey paper is organized as follows. Section II introduces blockchain architecture. Section III shows typical consensus algorithms used in the blockchain. Section IV introduces several typical blockchain applications. Section V summarizes the tradeoffs and technical challenges, in this area. Section VI discusses some possible future directions and Section VII concludes the paper.

II. BLOCKCHAIN ARCHITECTURE

A node initiates a transaction in a decentralized blockchain network by employing a digital signature using private key cryptography. A transaction can be considered as a data structure that represents transfer of digital assets between peers on the blockchain network. All the transactions are stored in an unconfirmed transaction pool and propagated in the network by using a flooding protocol known as Gossip protocol. Then, peers need to choose and validate these transactions based on some preset criteria. For example, the nodes try to verify and validate these transactions by checking whether an initiator has sufficient balance to trigger a transaction or by trying to fool the system by enforcing double spending. Double spending refers to using the same input amount for two or more different transactions [19]. Once the transaction is verified and validated by the miners, it is included in a block. Peers who use their computational power to mine for blocks are called miners [20]. Miner nodes need to solve a computational puzzle and spent a sufficient amount of their computing resources to publish a block. The miner who can solve the puzzle first will become a winner and obtains the opportunity to create a new block. A small amount of incentive is given upon successfully creating a new block. All the peers in the network then verify the new block using a consensus mechanism, which is a technique that assist a decentralized network comes to an agreement on certain matters. After that the new block will be added to the existing chain and the local copy of each peer's immutable ledger. At this point, the transaction is confirmed. The next block links itself with the newly created block by using a cryptographic hash pointer. Now the block obtains its first confirmation while the transaction obtains the second confirmation. Similarly, with every time a new block is appended to the chain, the transaction will be reconfirmed. In general, a transaction needs six confirmations in the network to be considered final [21].

Later in this segment, Section II-A discusses the transaction process of blockchain with some example platforms, such as Bitcoin and Ethereum, Section II-B introduce the basic block structure and the process of cryptographic hash functions while Blockchain key characteristics are explained in Section II-C and Section II-D represents the taxonomy of blockchain.

A. BLOCKCHAIN TRANSACTION PROCESS

A Blockchain transaction can be defined as a small unit of a task that is stored in public records. These records are also known as blocks [22]. These blocks are executed, implemented and stored in blockchain for validation by all miners involved in the blockchain network. Each previous transaction can be reviewed at any time but cannot be updated [23].

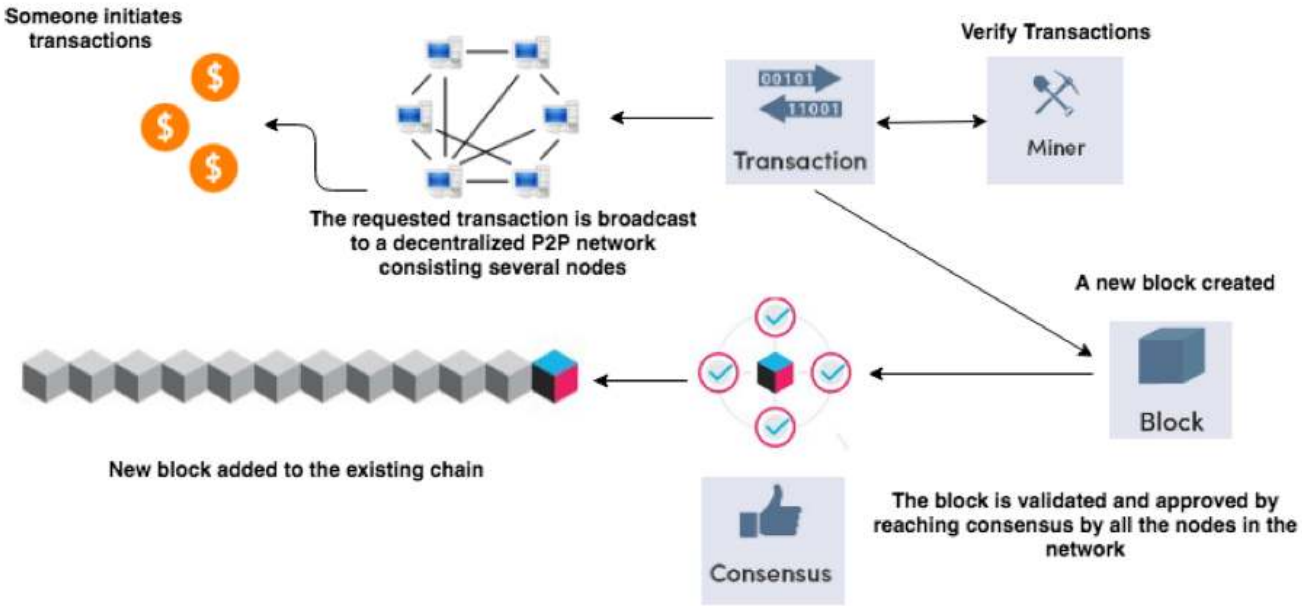


FIGURE 1. Functional diagram of a Blockchain network.

Blockchain is the underlying technology of Bitcoin, and it facilitates transactions that occur within a peer to peer global network in a decentralized fashion. That makes Bitcoin a borderless, censorship-resistant digital currency. In general, trust may be the main concern regarding traditional centralized systems, such as a banks, where people need to put their solemn confidence in the system. This is the sweet spot for public blockchain technology, in that it does not require any trust while handing over the ownership of digital assets from one peer to another. Blockchain is a trustless system that provides trust through the functions that propagate all the activities within the network [24]. Security is another aspect to consider while initiating transactions. Blockchain mining and consensus mechanisms that rely heavily on a cryptographic hash function can address the security issues. For example, Bitcoin uses a 256 bits' secure hash algorithm known as SHA-256 [25]. Bitcoin can take any type of input, such as text, numbers, string or even a computer-generated file of any length, to produce 256 bits or the 64 characters output called hash [26]. Given the same input, the converted hash output will always remain exactly similar. However, a small change to the input will change the output completely, which is also called a one-way function, meaning that from the output, it is not feasible to calculate the input. One can only guess what the input was, and the odds of guessing it right are rather astronomical, in other words, it is secure.

The first step of the transaction process is to verify the identity of the sender, which means the transaction between the sender and the receiver is requested by the sender, and not by anyone else. Figure 2 demonstrates the verification process with a simple example of a transaction between Bob and Alice. Let us assume both Alice and Bob has Bitcoin balance, and Alice wants to pay 10 Bitcoins to Bob. Now, to send the money, Alice will broadcast a message with the information for the transaction in the blockchain network. To do this, Blockchain employs digital signatures (public and private keys) [27]. For the broadcast, Alice provides Bob's information, such as his public address and transaction amount, along with her public key and digital signature. Alice used her private key to make that digital signature. Transaction validation is carried out independently by all miners based on different criteria that we have discussed later in this section. Elliptic curve digital signature algorithm (ECDSA) is used by blockchain [28]. This algorithm ensures that the funds can only be spent by their true possessors.

The signature in each transaction contains 256 bits, if anyone wants to fake this signature to make a fraudulent transaction, he or she has to guess 2^{256} cases, which is infeasible and waste of resources for a malicious peer/attacker [29]. In addition to checking the validity of the sender, the verifier also has to check the validity of the transaction regarding whether the sender has enough money to send to the receiver, or not. It could be performed by looking at the ledger, which holds information about every past successful transaction.

1) BITCOIN TRANSACTION

According to the original Bitcoin whitepaper, the main purpose of this digital cryptocurrency was to allow a decentralized electronic cash payment system between different parties by eliminating central intermediaries [30]. A Bitcoin transaction transfers the ownership of some bitcoin amount to another bitcoin address. Generally, it is initiated by a bitcoin wallet of a client and later broadcast to the network. The nodes on the network will rebroadcast the transaction and include it in the block they are mining only if the transaction is valid. It takes approximately 10 minutes to include the

transaction along with other transactions in a block [31]. The receiver should see the amount of transaction in their wallet by this point.

The main element of a bitcoin structure is unspent transaction output (UTXO), which refers to the output amount of a transaction that is received by a user and the capability of spending it in the future [32]. Consider that cash or coins in a physical wallet get mixed up, which is not in the case of the received amount in Bitcoin. All the received amount in a Bitcoin wallet remains as a separate entity. For example, when we receive two distinct amounts ($2 and $3) and keep it in the same physical or online wallet, it will obtain summed up to $5. Whereas in the Bitcoin wallet, it will still show the exact amounts and remain as individual entities. Let us consider that Alice has three separate UTXO (0.01, 0.2 and 3) in her wallet, and she wants to send 0.15 BTC to Bob. To do that, the wallet needs to select a spend candidate from these three output UTXO. If the wallet chooses 0.2 as an output, then it will unlock this amount and spend the whole amount as an input UTXO for the 0.15 BTC transaction. Then, 0.15 BTC will be transferred to Bob's address wallet as an output UTXO.

Miners will be incentivized by their effort in managing and validating all these transactions and creating a new block that will eventually add to the existing chain [33]. A successful miner obtains the block creation rewards and transaction fees [34]. While sending transactions, users usually assign a transaction fee upon successful block creation for the miners. There will not be any header information regarding the transaction fee. The users can attach a transaction fee by sending a lesser amount to the recipients than the total input UTXO. This unassigned transaction amount can be considered as transaction fee as depicted in Eq. 1.

$$Inputs - outputs = Transactionfees \tag{1}$$

Miners include their individual coinbase transaction along with the transaction data that they are trying to verify and validate while mining a block. A coinbase transaction is a unique type of bitcoin transaction that can only be created by a miner. This type of transaction has only outputs, and there is one created with each new block that is mined on the network. This is the transaction that rewards a miner with the block reward for their work. Any transaction fees collected by the miner are also sent in this transaction. The peers in the network check whether the transaction is level out and then decide to put this record in the distributed ledger. The coinbase transaction will send the block reward and the sum of the transaction fees to the given address of the miner. That shows that a miner has to assign his reward while creating a block. However, every node in the network will check whether the block adheres to the requirement, and as shown in Eq. 2. Therefore, a miner is eligible to use the block reward and transaction fees only after the block is verified.

$$sum(BlockOutputs) \leq sum(BlockInputs) + BlockReward \tag{2}$$

2) ETHEREUM TRANSACTION

The Bitcoin state is defined in the terms of UTXO, a reference implementation of the wallet application that held the account reference. However, Ethereum introduced the concept of an account as a part of the protocol that is the originator and target of a transaction. Hence, transactions directly update the account balances as opposed to maintaining the state, such as in the Bitcoin UTXOs, allowing transfer of values, messages and data between the accounts that may result in the state transitions [35]. Ethereum has two types of account: Externally Owned Account (EOA) and Contract Account (CA). While EOA is owned by private keys, CA is controlled by the code and activated only by an EOA [36]. EOA is needed to participate in the Ethereum network and interacts with the blockchain using transactions, whereas, CA represents a smart contract (SC). SC is a piece of code deployed in the blockchain's node and adds a layer of logic and computation to the trust infrastructure [37]. Execution of an SC is initiated by a message embedded in the transactions.

In Ethereum, the transferable amount is known as ether. The denomination of ether is known as Wei [38]. An Ethereum transaction has fields for transferring ether as well as messages to trigger smart contracts [39]. Ethereum uses attributes similar to Bitcoin, for instance, previous block hash, nonce, and transaction details. Additionally, it uses some other fields such as fees limit, state of SC, and so on. For a simple ether transfer, the amount to transfer and the target address are specified, together with the fees, gas points, and the respective accounts. All the transactions generated will be validated by checking time stamp, nonce combination, and availability of sufficient fees for execution.

Ethereum also uses an incentive based model for block creation. Any action in Ethereum requires crypto fuel or gas. Gas is used as fees instead of ether for ease of computation. The main reason behind that is that gas is a cryptocurrency independent of valuation for the transaction fee and computation fee. Ether, as a cryptocurrency, varies in value with market swings, but gas points do not vary. The mining process computes gas points required for the execution of a transaction. If the fee specified in the gas points in transaction is not sufficient, it is rejected. The gas points needed for the execution must be in the account balance and the proposed transaction for the execution to happen. The leftover amount after executing the transaction will be returned to the originating account. Etherreum has a mining incentive model where the miners are competing for block creation. The miner who solves the puzzle first is called the winner and the miners who solve it afterwards are called ommers [40]. The winner block is added to the main chain and ommer blocks are added as side blocks in the main chain. The winner block receives three ethers as a base fee along with the transaction fees as gas points. The ommers block receives a small percentage of total gas points.

B. BLOCK STRUCTURE

The Blockchain comprises a sequence of blocks, which stores the information of all the transactions, similar to a public ledger. These blocks are linked to each other via a reference hash that belongs to the previous block known as the parent block. The starting block is called the genesis block, which does not have any parent block. A block consists of the block header and the block body [41]. The block header includes metadata such as block version, parent block hash, Merkle tree root hash, timestamp, nBits, and nonce as shown in Table 1 and Fig. II-B.

TABLE 1. Block header attributes.

Header Attributes	Definition
Block Version	Indicates which set of block validation rules to follow.
Previous Block Hash	A 256-bit hash value that points to the previous block.
Merkle tree root	The hash value of all the transactions in the block.
Timestamps	Current timestamp as seconds since 1970-01-01T00:00 UTC.
nBits	Current hashing target in a compact format.
Nonce	A 4-byte field, which usually starts with 0 and increases for every hash calculation.

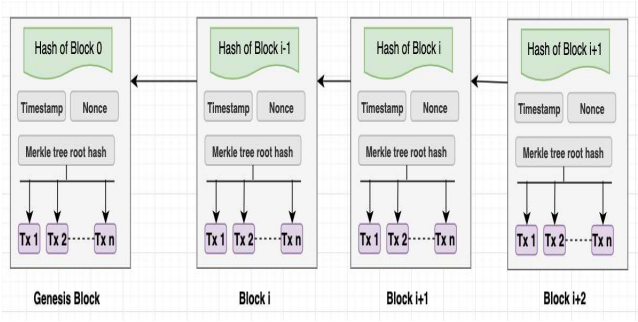


FIGURE 2. Block structure.

The block body is composed of a transaction counter and transactions. The transaction counter refers to how many transactions follow, and transactions represent the list of recorded transactions in the block. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions. A digital signature based on asymmetric cryptography is used in an untrustworthy environment such as the blockchain network. In this process, each participant in the network owns a private key and public key pair. The private key is used for signing or encrypting the transaction while the public key is distributed throughout the network and is visible to everyone, which helps to decrypt the following transaction.

C. CHARACTERISTICS OF BLOCKCHAIN

1) DECENTRALIZATION

In conventional centralized transaction systems, each transaction needs to be validated through the central trusted agency (e.g., the central bank). Therefore, decentralization requires trust, which is the main issue, along with lift resilience, availability and fail over, where the decentralized peer-to-peer blockchain architecture could be a better solution. Unlike a centralized system, a transaction in the blockchain network can be conducted between any two peers (P2P) without the authentication by the central agency. In this manner, blockchain can reduce the trust concern by using various consensus procedures. Moreover, it can reduce the server costs (including the development cost and the operation cost) and mitigate the performance bottlenecks at the central server. In contrast, in many cases, blockchain has some trade-offs. For example, PoW cases such as Bitcoin and Ethereum, the server and energy cost are orders of magnitude higher, while the performance are also several orders of magnitude lower.

2) PERSISTENCY

Blockchain provides the infrastructure by which truth can be measured [42] and enables the producers as well as consumers to prove their data are authentic and not altered. For example, if a Blockchain consists of 10 blocks, then block no. 10 contains the hash of the previous subsequent block, and to create a new block, the information of the current block is used. Therefore, all the blocks are linked and connected with each other in the existing chain. Even the transactions are related to the prior transaction. Now, a simple update on any transaction will significantly change the hash of the block. If someone wants to modify any information, he has to change all the previous block's hash data which is considered an astronomically difficult task considering the amount of work that needs to be done. In addition, after generating a block by a miner, it is confirmed by other users in the network. Hence, any manipulation or falsification of data will be detected by the network. For this reason, blockchain is almost tamper proof and considered as an immutable distributed ledger.

3) ANONYMITY

It is possible to interact with the blockchain network with a randomly generated address [43]. A user can have many addresses within a Blockchain network to avoid the exposure of his identity. As it is a decentralized system, no central authority is monitoring or recording users' private information. Blockchain provides a certain amount of anonymity through its trustless environment.

4) AUDITABILITY

All the transactions that occur in a blockchain network are recorded by a digital distributed ledger and validated by a digital timestamp. As a result, it is possible to audit and trace

previous records by accessing any node in the network [44]. For example, all the transactions could be traced iteratively in Bitcoin which facilitates auditability and transparency of the data state in the blockchain. However, by tumbling money through many accounts, it becomes very hard to trace the money to its origin.

D. TAXONOMY OF BLOCKCHAIN SYSTEMS

There are three types of blockchain: public, private and consortium [45]. These systems can be compared using different perspective as described below.

1) CONSENSUS DETERMINATION

All the nodes can participate in the consensus process in the public blockchain such as Bitcoin, while only a few selected set of nodes are being responsible for confirming a block in the consortium blockchain. In the private blockchain, a central authority will decide the delegates who could determine the validated block.

2) READ PERMISSION

Public blockchain allows read permission to the users, where the private and consortium can make restricted access to the distributed ledger. Therefore, the organization or consortium can decide whether the stored information needs to be kept public for all or not.

3) IMMUTABILITY

In the decentralized blockchain network, transactions are stored in a distributed ledger and validated by all the peers, which makes it nearly impossible to modify in the public Blockchain. In contrast, the consortium and private Blockchain ledger can be tampered by the desire of the dominant authority.

4) EFFICIENCY

In the public blockchain, any node can join or leave the network which makes it highly scalable. However, with the increasing complexity for the mining process and the flexible access of new nodes to the network, it results in limited throughput and higher latency. However, with fewer validators and elective consensus protocols, private and consortium blockchain can facilitate better performance and energy efficiency [46].

5) CENTRALIZED

The significant difference among these three types of Blockchain is that the public blockchain is decentralized, while the consortium is partially centralized and private blockchain is controlled by a centralized authority.

Since public blockchain is open to the world, it can attract many users. Communities are also very active. Many public blockchains emerge day-by-day. For the consortium blockchain, it could be applied to many business applications. Currently, Hyperledger is developing business consortium blockchain frameworks. Ethereum has also has provided tools for building consortium blockchains. For the private blockchain, there are still many companies implementing it for efficiency and auditability.

TABLE 2. Comparison among different blockchain infrastructure.

	Category of Blockchain		
Properties	Public	Consortium	Private
Nature	Open and Decentralized	Controlled and Restricted	Controlled and Restricted
Participants	Anonymous and resilient	Identified and Trusted	Identified and Trusted
Consensus Procedures	PoW, PoS, DPoS	PBFT	PBFT, RAFT
Read/Write Permission	Permissionless	Permissioned	Permissioned
Immutability	Infeasible to tamper	Could be tampered	Controlled and Could be tampered
Efficiency	Low	High	High
Scalability	High	Low	High
Transaction approval frequency	Long (10 minutes or more)	Short	Short
Energy Consumption	High	Low	Low
Transparency	Low	High	High
Observation	Disruptive in terms of disintermediation	Cost effective due to less data redundancy and higher transactions times	Cost effective due to less data redundancy and higher transactions times
Example	Bitcoin, Ethereum, Litecoin, Factom, Blockstream, Dash	Ripple, R3, Hyperledger	Multichain, Blockstack, Bankchain

III. CONSENSUS PROCEDURES

In blockchain, how to reach consensus among the untrustworthy nodes is a transformation of the Byzantine Generals (BG) Problem [47]. In the BG problem, a group of generals who command a portion of a Byzantine army circle the city. The attack would fail if only part of the generals attack the city. Generals need to communicate to reach an agreement on whether to attack or not. However, there might be traitors within the generals. The traitor could send different decisions to different generals. This is a trustless environment. How to reach a consensus in such an environment is a challenge. It is also a challenge for blockchain as the blockchain network is distributed. In blockchain, there is no central node that ensures ledgers on distributed nodes are all the same. Nodes need not trust other nodes. Thus, some protocols are needed to ensure that ledgers in different nodes are consistent. We next present several common approaches to reach consensus in the blockchain.

A. PROOF OF WORK (POW)

Proof-of-work (PoW) is a proof-based consensus algorithm. The basic concept of the consensus technique is to identify and determine the node that will obtain the right to append a new block to the existing chain by providing the sufficient

proof of its effort [15]. This consensus procedure was used in the Bitcoin network. As a matter of fact, confusion will arise if every node tries to broadcast their blocks containing similar verified transactions. For instance, if a transaction which is verified by many nodes, then the question will arise regarding who will put it into the block. Moreover, the ledger will be meaningless if transactions are duplicated in different blocks. For this reason, it is important to reach a consensus between all the nodes in the network about the newly created block. PoW tries to solve this issue as nodes need to solve a difficult puzzle with adjusted difficulty to obtain the opportunity of appending the new block to the current chain [48]. The nodes that will participate in this process are called miners, while the process is called mining. Miners are responsible for selecting verified transactions to form a block, along with some other information such as previous hash and timestamp. Then, the SHA-256 hash function will be used to convert all the information inside a block header to create a hash value.

In the decentralized network, all participants have to calculate the hash value continuously by using different secret values, called nonce, until the target is reached. A nonce is an arbitrary number that can be used just once in a single transaction that serves to modify the output of a function [1]. Because the output values of hashing algorithms can not be easily predicted from input values, this makes finding an acceptable nonce difficult and random. Miners have to use brute force to find the nonce by running different nonce values through the algorithm until an appropriate output value is found. The consensus requires that the output must be equal to or smaller than a given threshold, which is defined by the difficulty [49]. If that happens, then the nonce will be accepted and the miner can claim the block. Otherwise, the miner needs to follow the process irrelatively until reaching towards the target output. Once obtaining the appropriate nonce, the miner will broadcast the block to the network and all the nodes will verify the solution using the same nonce. When it is approved by all other miners in the network, the newly created block will be appended to the current chain. As the nodes need to put efforts into guessing the correct value, the work is called proof-of-work.

Despite that many miners might be involved for verifying transactions and creating a block, only the first who solves the puzzle will become the winner. As the miner puts considerable computing resources into publishing a block, he will receive a block creation reward of 12.5 BTC [50]. These new Bitcoin can only be used after the blockchain moves ahead a certain number of blocks. In addition to the block reward, the miner is also entitled to transaction fees. In this way, new Bitcoins will come into circulation, and the blockchain stays healthy. The block rewards is halved every 210,000 blocks and reduces to zero after the total Bitcoins created reach 21 million [51]. At this point, the miners will get only transaction fees. Figure 3 represents a block creation process in PoW consensus algorithm.

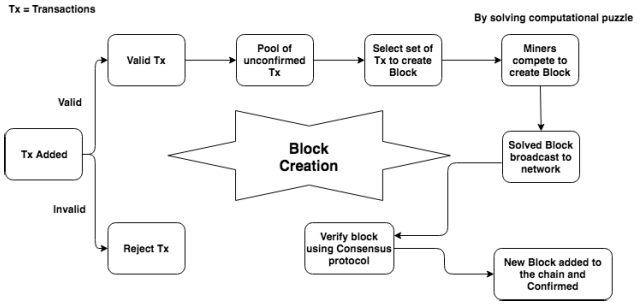


FIGURE 3. Block creation process in PoW procedure.

It is possible to envision a scenario where more than one miner finds the suitable nonce for the puzzle, almost at the same time [52]. Now, all these miners will try to broadcast their block in the network along with the nonce. In such circumstances, the miners might have a divided opinion about which block to receive and append to the current chain because those who verify the first coming block will ignore the later ones. That might create a forking problem where branches or forks are generated, as depicted in Figure 4. The original founder of Bitcoin proposed that although the miners will keep mining new blocks on their branches, eventually the longest fork will be considered the authentic one and other miners will join it [53]. From Figure 4, it can be observed that how PoW solves the forking problem by utilizing the longest chain rule. Two validated blocks X1 and Y1 are created simultaneously from block B. Once a new block X2 is appended to the block X1, the miners working on the fork Y1-Y2 will switch to X2, leaving the previous fork orphaned. In general, when six consecutive blocks are generated in a single fork (X1, X2, X3, X4, X5 and X6), it is considered to be the successful chain. Although the block intervals depends on various parameter settings, a Bitcoin block is generated in every 10 minutes while an Ethereum block is generated about every 17 seconds [9].

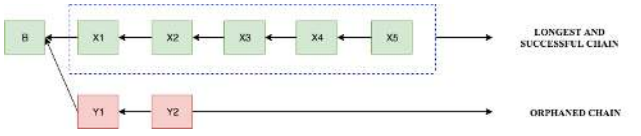


FIGURE 4. Blockchain forking.

The main concern regarding PoW approach is that miners need to spend high computational resources for solving the puzzle in order to create a block. Moreover, only one miner will be successful at the end which explains this process is not sustainable. To mitigate the loss, some PoW protocols in which works could have some side applications have been designed. For example, Primecoin searches for special prime number chains which can be used for mathematical research [54]. Instead of burning electricity for mining the PoW block, proof of burn asks miners to send their coins to addresses where they cannot be redeemed [55]. By burning

coins, miners get chances for mining blocks and they do not need powerful hardwares as PoW.

B. PROOF OF STAKE (POS)

In comparison with PoW, proof-of-stake (PoS) can be an energy efficient alternative. In this consensus method, the miner does not need to waste a huge amount of computing resource in order to solve the mathematical puzzle. Instead, it relies on having an adequate stake in the system to participate in the block creation process [56]. The chance of getting the opportunity to validate a block entirely depends on the stake or wealth of the participating node. It is believed that a sufficient stake will deter the possibility of a malicious attack on the network [57]. As the validator is chosen based on the stake it owns in the network, it eliminates the competition among the peers. Hence, a validator uses its stake and places a bet on a block. If the block is approved, the validator collects the fees from the transactions included in the block. As a result, PoS can be more sustainable than PoW, as it saves more energy as well as provides better latency and throughput [58]. However, this consensus procedure has some drawbacks. Since the selection of the validator is based on stakes, the wealthiest node may receive more chances to validate a block and becomes more dominant in the network, which may lead to unfair distribution or centralization. PoS can be more prone to malicious attacks as the mining cost and effort is much lower compared to PoW. A recently discovered limitation of this consensus algorithm is called the Nothing-at-stake problem [59]. This problem is a ramification of not relying on a physical reality to secure a coordination point for consensus.

To address these challenges, recent PoS protocols, e.g., Ethereum's Casper, are actively trying to penalize the validator for malicious behavior [60]. Many solutions are emerging with the combination of the stake size to determine the validator that will obtain the chance to forge the next block. For example, King et al., proposed Peercoin, an age-based selection of the stake where older and larger sets of coins have more priority for mining a block [61]. Vasin et al., introduced Blackcoin which uses randomization to select the next generator of the block and looks for the lowest hash value along with the size of the stake [62]. In addition, some consensus algorithms are employing some concepts of both PoS and PoW, but often with some additional feature. For instance, Bentov et al., proposed Proof-of-Activity (PoA), composed of features of PoW and PoS to ensure validators are being chosen in a pseudorandom yet uniform fashion [63]. In PoA, a block can be validated only if it is approved by N miners. In contrast, the stake can be other things instead of wealth. In Proof of Capacity (PoC), the miners allocate their hard drive space to validate a block. There are other slightly different approaches such as Proof of Importance (PoI), Proof of Storage (PoSt) and Proof of Deposit (PoD), which use tokens, storage and deposits as the stakes for a mining opportunity, respectively [64]–[66].

C. DELEGATED PROOF OF STAKE (DPOS)

Delegated proof-of-stake (DPoS) is an elective consensus procedure where each node with a stake in the network can delegate the validation of transactions to another node by the process of voting [67]. While PoS follows a direct democratic approach, DPoS is a representative democratic method. The delegates are being elected by the stakeholders to generate and validate a block and are known as witnesses [68]. These elected nodes then form a set that proposes blocks and validate data states. They take turns on voting for blocks on behalf of their stakeholders and validate previous blocks authenticity. Generally, most implementations employ a replacement pool with a standby validator to address node failures. Unlike PoS, there are significantly fewer participants for block validation, which facilitates faster block generation and confirms transactions quickly [69]. It is also possible to tune the parameters of the network, such as block size and block intervals, to ensure efficiency. The main limitation of this consensus mechanism can be its centralization tendency. The high stakes participants can vote themselves and manipulate others to vote into becoming validators. However, dishonest witnesses can be voted out by the stakeholders upon showing any malicious behavior. Bitshare is an example platform that used the DPoS consensus algorithm.

D. PRACTICAL BYZANTINE FAULT TOLERANCE (PBFT)

Byzantine fault tolerance (BFT) refers to reaching a consensus between two nodes communicating safely across a distributed network in the presence of malicious or misleading nodes [70]. Practical Byzantine fault tolerance (PBFT) is one of the examples of BFT, a replication algorithm capable of tolerating Byzantine faults. PBFT assumes that certain nodes are dishonest or faulty and was designed to be a high-performance consensus algorithm that can rely on a set of trusted nodes in the network [71]. The nodes in PBFT are ordered in a sequential manner with one being the leader and the other nodes acting as backups [72]. When the leader node gets a request, it informs the backups about it and then processes the request. The request originator is informed about the results by the leader node, who then awaits replies from other nodes with the exact same result. That means decisions are made through the majority votes, where each node communicates with other nodes, to prove the origin of the signed message as well as the integrity of the message. A new block is determined in each round, and a leader node is selected based on some rules and is responsible for ordering a transaction. The overall process is divided into three phases, preprepared, prepared and commit. One similarity among these phases is that a node would enter the next phase, if it has the support or votes from over 2/3 of all nodes. Therefore, PBFT can work efficiently with the presence of 1/3 malicious Byzantine replicas. Hyperledger fabric, a blockchain-based platform, provides different business solutions by leveraging PBFT consensus protocol [73]. Mazieres et al., proposed Stellar consensus protocol (SCP), which is also based on

TABLE 3. Comparison among different consensus algorithms.

Property	PoW	PoS	PFBT	DPoS	Tendermint
Identity Management of Node	Open	Open	Permissioned	Open	Permissioned
Energy Consumption	High	Low	Very Low	Very Low	Very Low
Adversary Tolerance	$\leq 25\%$	$< 51\%$	$\leq 33.3\%$	$< 51\%$	$\leq 33.3\%$
Scalability	Strong	Strong	Weak	Strong	Strong
Performance (transactions per second)	<20	<20	<1000	<500	<10000
Forking	While two nodes identify the suitable nonce at the same time	Very difficult	Probably	Consistent, if less than one third nodes are byzantine.	Highly unlikely
Consensus confirmation time	High	High	Low	Medium	Low
Block Creation speed	Slow	Fast	Fast	Depends on variant	Fast
Example	Bitcoin, Ethereum	Peercoin, Nextcoin	Hyperledger Fabric	Bitshares	Tendermint

Byzantine consensus protocol [74]. In SCP, the nodes have the right to choose which set of other participants to believe, while in PBFT, all the nodes need to query each other. Antshares has implemented their own version of blockchain based on PBFT, which is known as Delegated Byzantine fault tolerance (DBFT) [75]. In DBFT, some professional nodes are being elected by a voting process to record and verify transactions instead of all nodes.

E. TENDERMINT

Kwon et al., proposed Tendermint, which is based on the Byzantine consensus algorithm [76]. A new block is determined in each round. A proposer would be selected to broadcast an unconfirmed block in this round. Therefore, all nodes need to be known for proposer selection. The block can be divided into three steps: prevote step, precommit step and commit step. In the prevote step, validators choose whether to broadcast a prevote for the proposed block. In the precommit step, if the node has received more than 2/3 of prevotes on the proposed block, it broadcasts a precommit for that block. If the node has received over 2/3 of precommits, it enters the commit step. The node validates the block and broadcasts a commit for that block in the final step. If the node has received 2/3 of the commits, it accepts the block. The process is quite similar to PBFT, but Tendermint nodes have to lock their coins to become validators. Once a validator is found to be dishonest, it would be punished.

F. COMPARISONS AMONG DIFFERENT CONSENSUS ALGORITHMS

Different consensus algorithms have different advantages and disadvantages. Table 3, Illustrates a comparison between different consensus algorithms. Vukoli et al., use the following properties to differentiate various consensus procedures [77].

1) NODE IDENTITY MANAGEMENT

The process of identifying validators on the network. In PBFT, the identity of each node must be known to select leaders and followers, while Tendermint selects a proposer in each round by having the knowledge of its validators. For others, such as PoW and PoS, nodes can join and leave the network as they wish.

2) ENERGY SAVING

PoW consumes a huge amount of electricity while finding the nonce to reach the target value. In contrast, PoS and DPoS do not require any computation puzzle to solve to find the validators who will append a new block to the chain. Therefore, these solutions are more energy efficient. For Byzantine protocols, such as PBFT, Ripple and Tendermint, they do not need any mining in the consensus procedure. As a result, they can save electricity to a great extent.

3) TOLERATED POWER OF THE ADVERSARY

To gain control over a blockchain network, 51% of hash power is regarded as the required threshold. However, Eyal et al., proposed that by using selfish mining in PoW systems, the miners can achieve more revenue by acquiring only 25% of the hashing power [84]. PBFT is designed to work with 1/3 of dishonest nodes.

Bitcoin is based on PoW while Peercoin is a new peer-to-peer PoS cryptocurrency. Further, Hyperledger Fabric utilizes PBFT to reach consensus. Bitshares, a smart contract platform, adopts DPOS as their consensus algorithm. Ripple implements the Ripple protocol while Tendermint devises the Tendermint protocol. PBFT and Tendermint are permissioned protocols. Node identities are expected to be known to the whole network, so they might be used in a commercial mode rather than in a public mode. PoW and PoS are suitable for the public Blockchain. Consortium or private blockchain might have preference for PBFT, Tendermint, DPOS and Ripple. Table 3. illustrates the comparison among different consensus algorithms.

IV. BLOCKCHAIN APPLICATIONS

Blockchain technology can be used in diverse sets of applications. It is important to understand that bitcoin is not equal to blockchain; instead, it is one of the most successful applications of blockchain technology [78]. Bitcoin is a cryptographic digital currency, which is transacted over

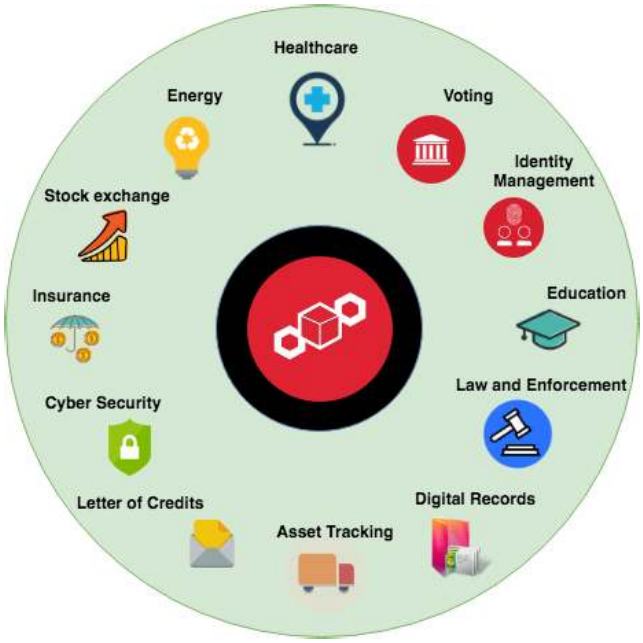


FIGURE 5. Application domains of Blockchain technology.

an open, public and anonymous blockchain network. However, experts claim that, this technology can be implemented for finding solutions for different domains, such as healthcare, voting, identity management, governance, supply chain, energy resources and so on. Furthermore, some visionaries also predict that blockchain might influence the digital realm similar to the internet [79]. When the internet first came along, we had no idea how it would forever change our lives. From smart phones and text messages to streaming movies and video conferences with loved ones, as well as for attending meeting or interviews, no one knew the ways the world would change with the invention of the Internet. We are currently in the early phases of blockchain and there is much potential yet to be unlocked. Fig. 5 represents some of the application domains of the blockchain proposed by various experts. In this section, we have discussed some use case areas of blockchain suggested by researchers around the globe.

A. HEALTHCARE

Distributed ledger technology possesses the potential to transform health services [80]. Blockchain can be used for the traceability of drugs and patient data management. Drug counterfeiting is a major problem in the pharmaceutical industry. Reports from the Health Research Funding organization revealed that 10% to 30% of the drugs sold in developing countries involves counterfeit [81]. It is estimated by the WHO that 16% of counterfeit drugs have the wrong ingredients, while 17% contain an imprecise level of essential ingredients. Therefore, these drugs can put a patient's life in danger as they will not treat the diseases, rather can trigger secondary effects that can lead to death. From an economic point of view, drug counterfeiting is responsible for an annual loss of 10.2 billion euros for European pharmaceutical organizations [82]. Blockchain can be a solution to address this issue because all the transactions added to the distributed ledger are immutable and digitally timestamped, which makes it possible to track a product and make the information tamper-proof.

Managing patient data integrity is one of the major concerns for the healthcare industry [83]. Each patient has unique physical variability, therefore a treatment strategy for a common disease varies depending upon circumstances. Hence, for providing personalized treatment, it is necessary to access the complete medical history of an individual patient. However, medical data are sensitive and requires a secured sharing platform. The existing system of bookkeeping medical records is lacking privacy as well as interoperability. Currently, blockchain can offer an infrastructure for the integration of medical records among different healthcare facilities as well as data integrity features through its immutable ledger technology. Blockchain is capable of establishing a robust and secure transparent framework of storing digital medical records that brings quality services for the patients as well as reducing treatment cost. B Shen et al., have proposed a permissioned blockchain based framework named MedChain, which is built upon Hyperledger Fabric that provides the patients full control over their own medical records [84]. The patients have the ability to share access to their health information to doctors or health centers using this distributed storage platform. Deloitte also published a paper (2016) on the opportunities for health care through blockchain based solutions [85]. This paper describes how interoperability in the health care system can be achieved by using smart contracts as well as by eliminating intermediaries to reduce additional costs and make the system more robust.

B. ENERGY INDUSTRY

One of the main uses of blockchain in energy related applications is in microgrids. A microgrid is a localized set of electric power sources and loads integrated and managed with the objective of enhancing energy production and consumption efficiencies and reliabilities [86]. The electric power sources can be distributed power generators, renewable energy stations, and energy storage components in facilities created and owned by different organizations or energy providers. One of the main advantages of the microgrid technology is that it does not only allow residents and other electric power consumers such as factories to have access to the needed energy, but they can also produce and sell excess energy to the grid. Blockchain can be used to facilitate, record, and validate power selling and buying transactions in microgrids [87].

In a similar way, blockchain can be used at larger scales to enable energy trading in smart grids. In smart grids equipped with bidirectional communication flow, blockchain can be used to support secure and privacy maintained consumption monitoring and energy trading without a need for a central intermediary [88].Smart contracts can be used to

ensure the programmatic descriptions of anticipated power flexibility degrees, the validation and tractability of demand response agreements, and the balance between power needs and generation. Furthermore, blockchain can be used to enable energy trading in the Industrial Internet of Things (IIoT) [89].Generally, utilizing blockchain for energy-related applications has the potential to reduce energy costs as well as increase resiliency.

C. STOCK MARKET

Blockchain technology could solve the issues for fragmented market systems, such as interoperability, trust, and transparency [90]. Due to the role of intermediaries, the regulatory process and operational trade clearance, it takes more than 3 days to complete and finalize all transactions. As a result, the stock market participants, for example, traders, regulators, brokers and the stock exchange, are going through a cumbersome process. Blockchain may be the solution in this regard. It can make the stock exchange more optimal through decentralization and automation [91]. By eliminating intermediaries and speeding up transaction settlements, blockchain can help reduce cost. Furthermore, the technology can provide viable use in transaction clearing and settlement while easing the monotonous paperwork of the trade and legal ownership transfer along with the secured post-trade process. By introducing smart contracts, blockchain is mitigating the need of a third party regulator by acting as a regulator for all transactions.

D. VOTING

Blockchain can be utilized in different fields as a solution to the problems that a standard database might have. One such problem can be seen in voting. Recently, it was revealed that a major U.S. voting machine manufacturer had installed remote access software on some systems [92]. This software allowed for the alteration of votes when counting the total. Instances such as this create a lack of trust in America's voting system, as seen in a recent poll: ''Exclusive poll: Majority expects foreign meddling in midterms''. This poll suggests that only approximately a quarter of Americans feel confident that their vote is being counted. Blockchain would solve this issue by providing a distributed ledger that would ensure votes are counted since the ledger a voter owns is the same as the one counting the total.

E. INSURANCE

Blockchain can be used to support the insurance marketplace transactions between different clients, policyholders, and insurance companies. Blockchain can be used to negotiate, buy and register insurance policies, submit and process claims, and support reinsurance activities among insurance companies. Different insurance policies can be automated using smart contracts, which can significantly reduce administration costs [93]. For example, there is a high administration cost associated with processing insurance claims. In many cases, the administration of claims can be very complex processes due to disagreements and misinterpretations of the terms. Smart contracts can evade these problems by structuring insurance policies in more precise if-then relationships. These policies allows for the automation of executing the terms by digital protocols that exactly implement the agreed upon insurance policies, thus reducing the effort needed and the costs of execution. With this reduction, insurance companies can also reduce the cost of their insurance products and be more competitive to attract more customers. At the same time, it allows insurance companies to launch new automated insurance products for their clients without worrying too much about their administrative overhead and costs. Furthermore, blockchain enables insurance companies to be expanded globally.

F. IDENTITY MANAGEMENT

In the real world, personal identity can be verified using identity documents such as a driver's license, national ID card, and passport. However, there is hardly any effective equivalent system for securing online identities. Blockchain may render an approach to circumvent this concern. This technology can be used to create a platform to protect an individual's identity from being theft or reduces fraudulent activities. Blockchain may allow individuals to create an encrypted identity, that does not require any username or password while offering more security features and control over accessing their personal information. By comprising identity verification with that decentralized blockchain principle, a digital ID can be generated. This ID can be assigned to every online transaction similar to a watermark. Hence, it will aid organizations to detect and eliminate the possibility of fraud by checking identity on every real-time transaction. Blockchain-based solutions on identity management could enable the consumer to access and verify online payments by simply using an app for authentication instead of using a username and password or biometric methods [94]. Paul Dunphy et al., proposed a scheme for identity management, leveraging distributed ledger technology to enhance decentralization, transparency and user control [95]. Djuri Baars et al., suggested an innovative architecture of self-sovereign decentralized identity management using blockchain technology [96]. An individual identity that is fully controlled by an individual is called self-sovereign identity. The author believes that deploying blockchain with self-sovereign identity management eliminates the issue of identity theft to be a great extent as no central authority or third party can be inferred without the user's consent.

G. TRADE FINANCE

Banks facilitate trade finance process using a letter of credit (LC) as a payment settlement method, which has been proven effective for risk mitigation [97]. However, due to the process complexities, high cost and contractual delays, it still does not account for less than one-fifth of international trade. With the increased time and cost for issuing LC, it becomes less attractive to the trading parties regarding

low-value transactions. This incident disintermediates banks as well as contribute to the rise of open trade. Blockchain may possess the potential of addressing these issues by automating LC that will provide reduced transaction costs and operational complexity. Blockchain's smart contract can be modeled in compliance with all specified conditions mentioned in LC between the supplier and client, which can guarantee payment once the trade merchandise is delivered to the buyer. This solution may mitigate the contractual ambiguities and discrepancies of information that leads to reduced time and cost of LC amendments [98]. Although the ICC survey showed that approximately 80% of respondents expressed their concern regarding traditional trade finance, in that it might not see any growth or decline in the near future, blockchain can become the solution to speed up the documentation process ensuring the security.

V. TRADEOFFS AND CHALLENGES OF BLOCKCHAIN TECHNOLOGY

Blockchain has become one of the biggest buzzwords in both business and technology today. It is considered as the technology that will revolutionize the finance sector with its ability to function without any central authority or intermediaries. Additionally, it is also believed that blockchain will be beneficial for other industries because of its capability of storing tamper-proof data and managing a huge trail of records in an efficient way. However, similar to other emerging technologies, blockchain has its limitations and is not feasible for many all types of business model.

This section describes the issues and challenges of blockchain technology as the following: performance & scalability in Section V-A, privacy in Section V-B, interoperability in Section V-C, energy consumptions in Section V-D, selfish mining in Section V-E and current regulation problems in Section V-F.

A. PERFORMANCE & SCALABILITY

Cryptocurrency and blockchain-based solutions for different business models are gaining popularity. However, there is a concern regarding whether it could meet up with the increasing demand coming from different business and government based sectors, especially regarding performance and scalability. Recently, researchers are working to address the scalability issues regarding the number of replicas in the network as well the performance concern, such as throughput (number of transactions per second) and latency (required time for adding a block of transactions in the blockchain) [99]. Increasing the number of replicas can have a detrimental effect on the throughput and latency because the network needs to deal with the increased amount of message exchange and processing. Although protocols such as PoW can ensure scalability, it is suffering from low throughput and high latency. This bottleneck occurs due to the resource wasted for solving the cryptographic puzzle to publish a block and append it to the chain. For example, Bitcoin is a PoW-based protocol that can scale a large number of replicas. In contrast, it provides low throughput considering only 6-10 transactions per second (may be less than that depending the complexity of the network) and is capable of generating a block with an average of 10 minutes. Another drawback of this consensus procedure, is that it is CPU intensive and hence, causes high consumption of electricity.

Ethereum also uses PoW in a different manner to prevent ASIC-enhanced mining, which is a hardware similar to a central processing unit (CPU) or graphics processing unit (GPU) that helps to mine faster but is very expensive and energy consuming. However, it can not eliminate the drawbacks of Bitcoin. There is also the risk of multiple branching in PoW protocol that can lead toward the double spending problem [100]. Therefore, clients need to wait for 60 minutes or six blocks confirmation to ensure that the transaction is finalized in the longest chain. That makes the transaction duration quite lengthy and might not be feasible for adopting it in real life applications.

The PBFT protocol is capable of achieving consensus in the presence of malicious replicas with few rounds of exchanging messages. PBFT generally uses a single replica as a primary that will propose a block, and if consensus is achieved by two-thirds of the all network peers, the block is added to the chain. Moreover, PBFT does not allow forking during the consensus process. This approach is sustainable in terms of energy efficiency, yet it lacks sustainability. PBFT has quadratic message complexity that requires nxn broadcast for n replicas. Although this overhead ensures that consensus will be reached having malicious replicas or Byzantine failures, it creates scalability issues. Any mainstream platform needs to process hundreds and thousands of transactions per second. Otherwise, the economy could not keep moving on without massive delays for consumers and businesses, which proves that scalability and performance is an important concern for this emerging technology.

Meanwhile, as the capacity of blocks is very small, many small transactions might be delayed since miners prefer those transactions with a high transaction fee. The size of the blocks are limited, for example, a Bitcoin block size is 1 MB. Although this approach was designed to make the platform more secure, it makes the transaction process much slower compared with other existing systems. The limited block size can not process many transactions at once. The DCS (decentralized, consistent and scalable) theorem, proposed by Slepak et el., had also emphasized on issues related to scalability, such as blocksize [101]. By using the DCS triangle, they showed that decentralized blockchain system can not have all the properties of DCS simultaneously. Blockchain can meet 2 requirements of the DCS framework. However, it provides low throughput and high latency, e.g., low volume and slow transaction speed. Fig. 7 represents the DCS triangle.

B. PRIVACY

Blockchain is considered to provide safety and privacy to the sensitive personal data as users can make transactions

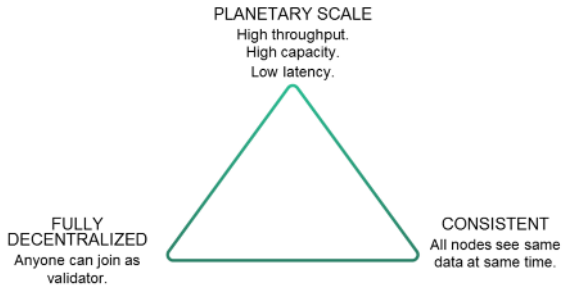


FIGURE 6. DCS triangle [101].

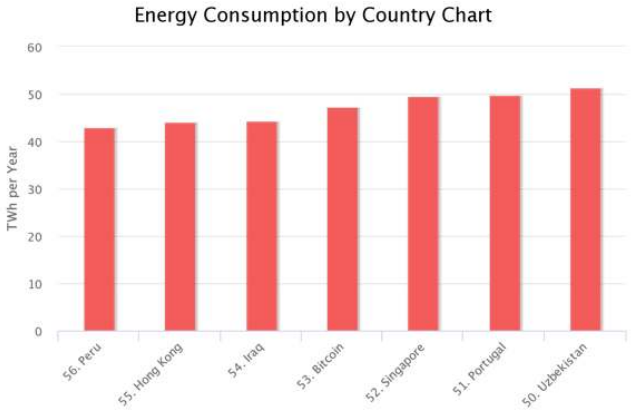


FIGURE 7. Energy consumption by country chart [106].

with generated addresses instead of using a real identity. However, some researchers suggested that Blockchain might be vulnerable in terms of transactional privacy as the public key for initiating a transaction is visible to the network peers [102]. Although it is claimed that a peer can be anonymous in the Blockchain network, some recent studies on the Bitcoin platform have shown that the transaction history can be linked to reveal member's true identity [103]. In addition, Biryukov et al. proposed a method to link peers pseudonyms to IP addresses while they are behind the firewalls or network address translation (NAT) [104]. He also mentioned that peers can be uniquely identified through its connected set of nodes. The main reason behind blockchain's vulnerability to information leakage is because the details and balances of all public keys are visible to everyone in the network. Therefore, the privacy and security requirements should be defined at the initial stage of Blockchain applications.

C. INTEROPERABILITY

From Deloitte's 2018 report, it can be observed that many industries are currently interested in adopting blockchain technology. However, there is no standard protocol that will allow them to collaborate and integrate with each other. This situation is called a lack of interoperability and has a detrimental impact on the growth of the blockchain industry. For this reason, instead of offering different practical solutions to a variety of business models, cryptocurrency is still the main platform for blockchain technology. Although, the lack of interoperability grants freedom to the blockchain developers to code in different programming platforms, all these networks are isolated and can not interact with each other. For example, GitHub has more than 6500 active blockchain projects using different platforms as well as diverse programming languages, consensus mechanisms, protocols and privacy features. Therefore, standardization is required for collaboration of enterprises on application development to share blockchain-based solutions as well as integrate with existing systems.

D. ENERGY CONSUMPTION

The proof-of-work (PoW) algorithm has enabled bitcoin to perform transactions among peers in a trustless distributed decentralized environment. However, while doing this work, miner computers are consuming a huge amount of electrical energy [25]. To provide insights about this highly unsustainable nature of the PoW algorithm, the bitcoin energy consumption index was created. The incentive mechanism motivates people around the world to mine Bitcoin. The mining process provides a solid stream of revenue that attracts individuals to run power-hungry devices to gain a chunk of it. As a result, the total energy consumption rate of the Bitcoin network reached a new high along with the value of the cryptocurrency. Based on a report published by the International Energy Agency, the overall consumption of the Bitcoin network is higher than a number of countries [105]. If Bitcoin was a country, it would rank as shown in Fig.7.

Bitcoin is not only responsible for consumption of a massive amount of energy but also contributes to an extreme carbon footprint. The coal-fired power plants in China are providing fuel for the bitcoin's network. Nature Climate Change (October 2018) even suggested that Bitcoin mining alone could push global warning above 2 °C within less than three decades.

According to Bitcoin energy consumption index [106]:

- Bitcoin's current estimated annual electricity consumption: 51.92 TWh
- Annualized estimated global mining costs: $2,595,834,583
- Bitcoin's electricity consumption as a percentage of the world's electricity consumption: 0.23%
- Carbon footprint per transaction: 274.29 kg of CO2

Another way to demonstrate the unsustainable nature of blockchain application is to compare its energy consumption with other payment systems such as VISA. This company has consumed 674,922 Gigajoules of energy for processing 111.2 billion transactions in 2017. Approximately 17,000 US households could use this amount of energy. However, a blockchain application such as bitcoin is more energy-intensive per transaction than VISA, which is shown in Fig. 8. It is possible to argue that blockchain has eliminated the need of intermediary cost; however, the cost is too high to bear. The solution for this issue might be redesigning the infrastructure of blockchain or simply using an alternative

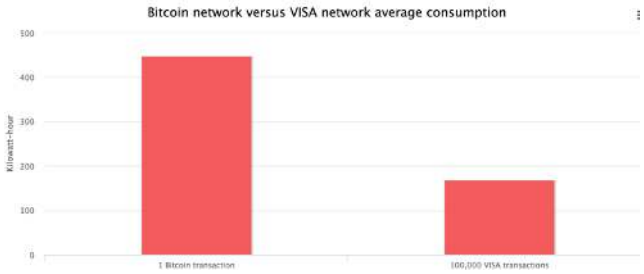


FIGURE 8. Bitcoin vs Visa network average consumption [106].

consensus algorithm such as PoS, where selected miners will verify the block without any competition. Hence, it will consume less energy.

E. FAIRNESS AND SECURITY

Given the immaturity of the technology, there are vulnerabilities that expose users to cybercrime. 51% attacks are one of the most recognized blockchain security issues. In a 51% attack, one, or several, malicious entities gain majority control of a blockchain's hashrate. With the majority hashrate, they can reverse transactions to perform double-spends and prevent other miners from confirming blocks.

Selfish Mining is another unfair method of mining pools to increase block rewards [107] that diminishes the integrity of a blockchain network. Although, it is considered that malicious nodes that are over 51% of computing power can take control of the blockchain network, Eyal et al., proposed a blockchain network that can still be vulnerable if someone wants to cheat with a small portion of hashing power [108]. In a selfish mining process, an individual miner as well as a pool of miners can initiate this process by not broadcasting the validated blocks to the rest of the network. Then, they continue the mining process for the next block to maintain the lead. The solved blocks are only revealed to the public upon satisfying some requirements. Hence, the chain of the selfish miner becomes longer and difficult, which leads the network to adopt their solutions while other miners are wasting their resources on a useless branch. Finally, the selfish miners claim more revenue. That attracts the rational miners to join the longer chain which might cause the selfish pool to exceed 51% power.

Many other mining strategies have been proposed based on selfish mining that proves the blockchain is not so secure. Nayak et al., proposed a stubborn mining strategy that can result in 13% gains in comparison with selfish mining [109]. Their strategy showed how a miner can further amplify its gain by non-trivially composing mining attacks with network-level eclipse attacks. The research of Sapirshtein et al., revealed that even with less than 25% of the computational resources, the attackers can gain from selfish mining [110]. However, Heilman et al., presented a unique approach for honest miners to choose a branch to fix the selfish mining problem [17]. Another approach (ZeroBlock) from Solat et al. was introduced in 2016, where selfish miners cannot achieve more than their expected results [111]. In this scheme, there is a maximum time interval for generating and accepting a new block.

Many of the big-name blockchain platforms have proven their resilience to attacks and that they have very few serious bugs. However, the applications (e.g., smart contracts) built on top of them are still susceptible to bugs that can have serious consequences. Until these security threats are fixed, potential users will continue to exercise caution and mass adoption will be delayed.

F. CURRENT REGULATION PROBLEMS

Blockchain platforms such as cryptocurrencies are facing regularity issues. The reason behind that is that the features of this decentralized system weaken the central banks' ability to dominate the economic policy, which makes the government prudent towards blockchain technologies [112]. For example, many governments threatened or even made cryptocurrencies illegal in their territories. Bitcoin is banned in countries such as Pakistan, Iran, Ecuador, Morocco and more, while some bitcoin owners were arrested in Bangladesh. Fig. 9 shows the global legality of bitcoin. Peter yeoh et. al., showed the challenges regarding regulatory issues that have an adverse impact on innovative distributed technologies, especially in the EU and the USA [113].

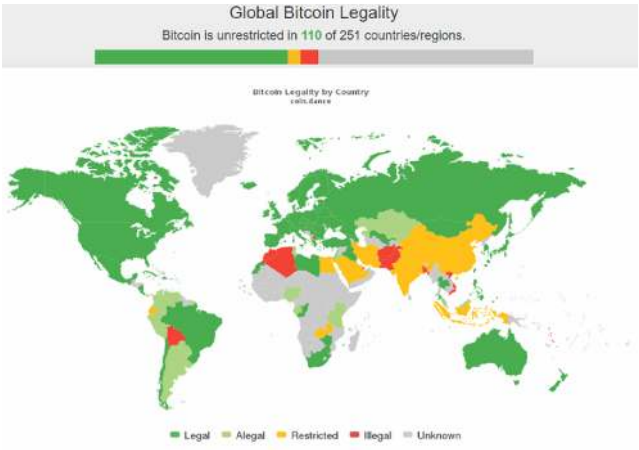


FIGURE 9. Global legality of Bitcoin [114].

Despite the emergence of such positive uses, the wider applications of block chain technology are challenged by some misgivings over its close identification to bitcoins amongst policymakers and regulators because of suspected bitcoin associations with money laundering activities. For instance, the Financial Action Task Force reported in 2015 on how the founders of Liberty Reserve were able to launder hundreds of millions of US dollars for six years to criminal organizations. Blockchain's wider and deeper applications are potentially constrained by limitations posed by technical/scalability challenges, business model challenges, scandals and public perception, government rules and privacy

challenges for personal records. Specifically, for the financial services sector, blockchain needs to overcome ten key hurdles before becoming a reality in the sector. These include matters concerning with its costs and benefits, cost mutualization, incentives alignment, evolving standards, scalability, governance, legal risks, security, simplification and regulatory interventions. Laws and regulations could impact how far and how fast the technology could develop. Therefore, regulatory approaches would need to be cleverly balanced against its innovative spirits while recognizing the possibility of the technology to unintentionally contribute to systemic risks in the financial system.

VI. FUTURE SCOPE OF BLOCKCHAIN TECHNOLOGY

The researchers believe that Blockchain has immense potential in both academia and industry. In this section, we have briefly discussed different future scopes for the Blockchain technology including standardization, asset protection, big data, and smart contract.

Blockchain performance to lure investors by promising a huge profit. It is compulsory to know whether this technology fits the requirements before adopting it into a business solution. Hence, there should be a standard testing mechanism for blockchain-based solutions to determine its importance as well as the tradeoffs. This process could be categorized into two phases; standardization and testing phase. The first phase will verify the claims of developers regarding their blockchain solutions based on some specific criteria. The testing phase is to determine the performance of the blockchain-based solution. For instance, the owner of an online retail business cares about the performance of the blockchain-based solution. Therefore, there should be some testing and standardizing methods to test the throughput, capacity, and latency of the acquired solution platform.

Blockchain technology allows companies to create a digital trail of records of their innovations and can generate a certificate upon registering the new inventions, proof-of-concepts and designs that could prove the integrity, existence, and ownership of any IP asset. By using the unique cryptographic layer, all notarized data such as trade secrets or copyright claims could remain private and secured.

It is also believed that big data analytics could be well combined with blockchain, especially in data management and data analytics. For data management, blockchain could be utilized to store data in a secured and distributed manner. Moreover, the immutability feature of blockchain could ensure the authenticity of the data. For instance, patient health records stored in the distributed ledger would be difficult to tamper and no one can steal that information without the consent of the owner. Transactions on blockchain could be used for data analytics. In this process, it is possible to determine the potential partners' trading patterns and behaviors in the blockchain network.

Another emerging scope of blockchain is smart contract. According to Szabo et al., a smart contract refers to a digital transaction protocol that executes the rules and policy of a contract [115]. This protocol a piece of code that is deployed in the blockchain node. Execution of a smart contract is initiated by a message embedded in the transaction. Recently, various smart contract developing platforms are emerging. A smart contract in blockchain could be used in different application areas, such as IoT-based platforms and banking services. The research on smart contracts can be separated into two types; development and evaluation. Smart contract platform development could be performed under development. Ethereum is providing the infrastructure to deploy many smart-contract based solutions, such as car auctions, online trading, and so on. Evaluation refers to performance and code analysis. It has been proven that even a small bug in developing smart contracts could cause a disastrous impact. The precise example could be the DAO attack, where over 60 million dollars were stolen due to the recursive call bug. Therefore, it is very important to analyze the attacks on the smart contract. On the other hand, the performance of the smart contract could become an important research topic. As the blockchain technology is acquiring immense attention from public and private sectors, more smart contract-based applications would be put into use.

VII. CONCLUSION

In this paper, the possibilities and benefits of the blockchain along with its tradeoffs are discussed through a comparative survey study. In addition, the transaction process, system architecture, application areas and consensus mechanisms of blockchain are also explained. There are still many open issues that need to be further researched and analyzed to create more workable and effective industrial applications that can fully benefit from the use of blockchain and achieve the intended goals. Examples of these open issues include security, privacy, scalability, energy issues, and integration with other systems and, more specifically, with regulatory issues. Future work in this field is required to address these issues and close the gaps for more efficient, scalable and secure blockchain industrial applications. This survey is expected to serve as an efficient guideline for further understanding about the tradeoffs regarding different blockchain consensus mechanisms and application areas for exploring potential research directions that may lead to exciting outcomes in related areas.

REFERENCES

[1] T. Aste, P. Tasca, and T. D. Matteo, "Blockchain technologies: The foreseeable impact on society and industry," *Computer*, vol. 50, no. 9, pp. 18–28, Jan. 2017.
[2] S. Nakamoto *et al.*, *Bitcoin: A Peer-to-Peer Electronic Cash System*. Citeseer, 2008. [Online]. Available: http://bitcoin.org/bitcoin.pdf
[3] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019.
[4] A. Litke, D. Anagnostopoulos, and T. Varvarigou, "Blockchains for supply chain management: Architectural elements and challenges towards a global scale deployment," *Logistics*, vol. 3, no. 1, p. 5, Jan. 2019.
[5] M. Kouhizadeh and J. Sarkis, "Blockchain practices, potentials, and perspectives in greening supply chains," *Sustainability*, vol. 10, no. 10, p. 3652, Oct. 2018.

[6] G. Peters, E. Panayi, and A. Chapelle, "Trends in cryptocurrencies and blockchain technologies: A monetary theory and regulation perspective," *J. Financial Perspect.*, vol. 3, no. 3, pp. 1–25, Nov. 2015.

[7] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," *IEEE Access*, vol. 7, pp. 36500–36515, 2019.

[8] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics Inform.*, vol. 36, pp. 55–81, Mar. 2019.

[9] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2016.

[10] S. Bano, M. Al-Bassam, and G. Danezis, "The road to scalable blockchain designs," *USENIX, Login, Mag.*, Dec. 2017, pp. 1–6.

[11] A. Gervais, G. O. Karame, and K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 3–16.

[12] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, "Is bitcoin a decentralized currency?" *IEEE Security Privacy*, vol. 12, no. 3, pp. 54–60, May/Jun. 2014.

[13] A. Blundell-Wignall, *The Bitcoin Question*, no. 37. OECD iLibrary, 2014. doi: 10.1787/5jz2pwjd9t20-en.

[14] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin P2P network," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2014, pp. 15–29.

[15] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019.

[16] S. King and S. Nadal, "PPCoin: Peer-to-peer crypto-currency with proof-of-stake," vol. 19, Aug. 2012. [Online]. Available: http://www.peercoin.net/

[17] E. Heilman, "One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2014, pp. 161–162.

[18] T. I. Kiviat, "Beyond bitcoin: Issues in regulating blockchain tranactions," *Duke Law J.*, vol. 65, p. 569, 2015.

[19] G. Karame, E. Androulaki, and S. Capkun, "Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin," *IACR Cryptol. ePrint Arch.*, vol. 2012, no. 248, Oct. 2012.

[20] J. A. Kroll, I. C. Davey, and E. W. Felten, "The economics of bitcoin mining, or bitcoin in the presence of adversaries," in *Proc. WEIS*, Jun. 2013, p. 11.

[21] M. del Castillo. (2017). *Chain is Now Working on Six 'Citi-Sized' Blockchain Networks*. [Online]. Available: https://www.coindesk.com/chainnow-working-six-citi-sized-blockchain-networks

[22] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2084–2123, 3rd Quart., 2016.

[23] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Jun. 2017, pp. 557–564.

[24] F. Glaser, "Pervasive decentralisation of digital infrastructures: A framework for blockchain enabled system and use case analysis," in *Proc. 50th Hawaii Int. Conf. Syst. Sci.*, 2017, pp. 1–10.

[25] K. J. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," in *Proc. 25th IET Irish Signals Syst. Conf.*, Jun. 2014, pp. 280–285.

[26] A. Manimuthu, R. V. Sreedharan, R. G, and D. Marwaha, "A literature review on bitcoin: Transformation of crypto currency into a global phenomenon," *IEEE Eng. Manage. Rev.*, vol. 47, no. 1, pp. 28–35, 1st Quart., 2019.

[27] G. O. Karame and E. Androulaki, *Bitcoin Blockchain Security*. Norwood, MA, USA: Artech House, 2016.

[28] Y. Yuan and F.-Y. Wang, "Blockchain and cryptocurrencies: Model, techniques, and applications," *IEEE Trans. Syst. Man, Cybern., Syst.*, vol. 48, no. 9, pp. 1421–1428, Sep. 2018.

[29] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2016, pp. 839–858.

[30] L. J. Valdivia, C. Del-Valle-Soto, J. Rodriguez, and M. Alcaraz, "Decentralization: The failed promise of cryptocurrencies," *IT Prof.*, vol. 21, no. 2, pp. 33–40, Mar./Apr. 2019.

[31] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *Proc. IEEE P2P Proc.*, Sep. 2013, pp. 1–10.

[32] S. Delgado-Segura and C. Pérez-Sola, G. Navarro-Arribas, and J. Herrera-Joancomartí, "Analysis of the bitcoin UTXO set," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2018, pp. 78–91.

[33] O. Schrijvers, J. Bonneau, D. Boneh, and T. Roughgarden, "Incentive compatibility of bitcoin mining pool reward functions," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2016, pp. 477–498.

[34] S. Ahamad, M. Nair, and B. Varghese, "A survey on crypto currencies," in *Proc. 4th Int. Conf. Adv. Comput. Sci.*, May 2013, pp. 42–48.

[35] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, Apr. 2014.

[36] D. Vujičić, D. Jagodić, and S. Randić, "Blockchain technology, bitcoin, and Ethereum: A brief overview," in *Proc. 17th Int. Symp. INFOTEH-JAHORINA (INFOTEH)*, Mar. 2018, pp. 1–6.

[37] D. Macrinici, C. Cartofeanu, and S. Gao, "Smart contract applications within blockchain technology: A systematic mapping study," *Telematics Inform.*, vol. 35, no. 8, pp. 2337–2354, Dec. 2018.

[38] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (SoK)," in *Proc. Int. Conf. Princ. Secur. Trust*. Berlin, Germany: Springer, Mar. 2017, pp. 164–186.

[39] B. K. Mohanta, S. S. Panda, and D. Jena, "An overview of smart contract and use cases in blockchain technology," in *Proc. 9th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2018, pp. 1–4.

[40] F. Ritz and A. Zugenmaier, "The impact of uncle rewards on selfish mining in ethereum," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS PW)*, Apr. 2018, pp. 50–57.

[41] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *Proc. 17th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput. (CCGRID)*, May 2017, pp. 468–477.

[42] D. Shrier, W. Wu, and A. Pentland, "Blockchain & infrastructure (identity, data security)," Massachusetts Inst. Technol., Cambridge, MA, USA, 2016, vol. 1, no. 3.

[43] Q. Wang, X. Li, and Y. Yu, "Anonymity for bitcoin from secure escrow address," *IEEE Access*, vol. 6, pp. 12336–12341, 2018.

[44] H. Yu, Z. Yang, and R. O. Sinnott, "Decentralized big data auditing for smart city environments leveraging blockchain technology," *IEEE Access*, vol. 7, pp. 6288–6296, 2019.

[45] J. Wang, P. Wu, X. Wang, and W. Shou, "The outlook of blockchain technology for construction engineering management," *Frontiers Eng. Manage.*, vol. 4, no. 1, pp. 67–75, 2017.

[46] M. Alharby and A. van Moorsel, "Blockchain-based smart contracts: A systematic mapping study," 2017, *arXiv:1710.06372*. [Online]. Available: https://arxiv.org/abs/1710.06372

[47] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, Jul. 1982.

[48] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," 2018, *arXiv:1805.02707*. [Online]. Available: https://arxiv.org/abs/1805.02707

[49] M. Pilkington, "11 blockchain technology: Principles and applications," in *Research Handbook on Digital Transformations*, vol. 225. 2016.

[50] M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems," 2011, *arXiv:1112.49800*. [Online]. Available: https://arxiv.org/abs/1112.4980

[51] *Controlled Supply—Bitcoin Wiki*. Accessed: May 21, 2019. [Online]. Available: https://en.bitcoin.it/wiki/Controlled_supply

[52] R. A. Memon, J. P. Li, and J. Ahmed, "Simulation model for blockchain systems using queuing theory," *Electronics*, vol. 8, no. 2, p. 234, Feb. 2019.

[53] C. G. Akcora, Y. R. Gel, and M. Kantarcioglu, "Blockchain: A graph primer," 2017, *arXiv:1708.08749*. [Online]. Available: https://arxiv.org/abs/1708.08749

[54] S. King, "Primecoin: Cryptocurrency with prime number proof-of-work," Jul. 2013, p. 6. [Online]. Available: http://primecoin.io/bin/primecoin-paper.pdf

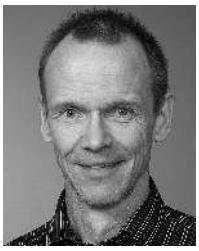
[55] A. Baliga, "The blockchain landscape," *Persistent Syst.*, 2016.

[56] F. Saleh, "Blockchain without waste: Proof-of-stake," Tech. Rep., 2018.

[57] A. Kiayias, I. Konstantinou, A. Russell, B. David, and R. Oliynykov, "A provably secure proof-of-stake blockchain protocol," *IACR Cryptol. ePrint Arch.*, vol. 2016, p. 889, Sep. 2016.
[58] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *Proc. 41st Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, May 2018, pp. 1545–1550.
[59] W. Li, S. Andreina, J.-M. Bohli, and G. Karame, "Securing proof-of-stake blockchain protocols," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Cham, Switzerland: Springer, 2017, pp. 297–315.
[60] V. Buterin and V. Griffith, "Casper the friendly finality gadget," 2017, *arXiv:1710.09437*. [Online]. Available: https://arxiv.org/abs/1710.09437
[61] S. King and S. Nadal. (2017). *Ppcoin: Peer-to-Peer Crypto-Currency With Proof-of-Stake (2012)*. [Online]. Available: https://peercoin.net/assets/paper/peercoin-paper.pdf
[62] P. Vasin. (2014). *Blackcoin's Proof-of-Stake Protocol v2*. [Online]. Available: https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf
[63] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake," *IACR Cryptol. ePrint Arch.*, vol. 2014, p. 452, 2014.
[64] N. Bozic, G. Pujolle, and S. Secci, "A tutorial on blockchain and applications to secure network control-planes," in *Proc. 3rd Smart Cloud Netw. Syst. (SCNS)*, Dec. 2016, pp. 1–8.
[65] S. Wilkinson, J. Lowry, and T. Boshevski, "Metadisk a blockchain-based decentralized file storage application," Storj Labs Inc., Atlanta, USA, Tech. Rep., 2014, pp. 1–11.
[66] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market," *Appl. Energy*, vol. 195, pp. 234–246, Jun. 2017.
[67] D. Larimer, "Delegated proof-of-stake (dpos)," Bitshare, White Paper, 2014.
[68] *Delegated Proof-of-Stake Consensus|Bitshares 3.0*. Accessed: May 21, 2019. [Online]. Available: https://bitshares.org/technology/delegated-proof-of-stake-consensus/
[69] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain," *J. Inf. Process. Syst.*, vol. 14, no. 1, pp. 101–128, Jan. 2018.
[70] X. Wang, J. WeiLi, and J. Chai, "The research on the incentive method of consortium blockchain based on practical byzantine fault tolerant," in *Proc. 11th Int. Symp. Comput. Intell. Design (ISCID)*, vol. 2, Dec. 2019, pp. 154–156.
[71] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Proc. Workshop Distrib. Cryptocurrencies Consensus Ledgers*, vol. 310, 2016, p. 4.
[72] K. Zheng, Y. Liu, C. Dai, Y. Duan, and X. Huang, "Model checking PBFT consensus mechanism in healthcare blockchain network," in *Proc. 9th Int. Conf. Inf. Technol. Med. Educ. (ITME)*, Oct. 2018, pp. 877–881.
[73] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, C. Ferris, C. Ferris, S. Muralidharan, C. Murthy, B. Nguyen, B. Nguyen, B. Nguyen, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, Apr. 2018, p. 30.
[74] D. Mazieres, "The stellar consensus protocol: A federated model for internet-level consensus," Stellar Develop. Found., Tech. Rep., 2015.
[75] *Antshares (Ans) Statistics—Price, Blocks Count, Difficulty, Hashrate, Value*. Accessed: May 21, 2019. [Online]. Available: https://bitinfocharts.com/antshares/
[76] E. Buchman, "Tendermint: Byzantine fault tolerance in the age of blockchains," Ph.D. dissertation, School Eng., 2016.
[77] M. Vukolić, "Quorum systems: With applications to storage and consensus," *Synthesis Lectures on Distributed Computing Theory*, vol. 3, no. 1. 2012, pp. 1–146.
[78] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Appl. Innov.*, vol. 2, nos. 6–10, p. 71, 2016.
[79] R. L. Twesige, "A simple explanation of bitcoin and blockchain technology," Tech. Rep., 2015.
[80] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 135, pp. 62–75, Jun. 2019.
[81] B. D. Glass, "Counterfeit drugs and medical devices in developing countries," *Res. Rep. Tropical Med.*, vol. 2014, pp. 11–22, 2014.
[82] *Counterfeit of Medicines Causes 37, 000 Job Losses in Eu Pharma Industry—ECA Academy*. Accessed: May 21, 2019. [Online]. Available: https://www.gmp-compliance.org/gmp-news/counterfeit-of-medicines-causes-37000-job-losses-in-eu-pharma-industry
[83] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30.
[84] B. Shen, J. Guo, and Y. Yang, "MedChain: Efficient healthcare data sharing via blockchain," *Appl. Sci.*, vol. 9, no. 6, p. 1207, Dec. 2018.
[85] M. Pilkington, "Can blockchain improve healthcare management? consumer medical electronics and the IoMT," Tech. Rep., 2017.
[86] R. H. Lasseter and P. Piagi, "Microgrid: A conceptual solution," in *Proc. IEEE 35th Annual Power Electron. Spec. Conf.*, vol. 6, Jun. 2004, pp. 4285–4291.
[87] A. Cohn, T. West, and C. Parker, "Smart after all: Blockchain, smart contracts, parametric insurance, and smart energy grids," *Georgetown Law Technol. Rev.*, vol. 1, no. 2, pp. 273–304, 2017.
[88] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep./Oct. 2018.
[89] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.
[90] L. Lee, "New kids on the blockchain: How bitcoin's technology could reinvent the stock market," *Hastings Bus. Law J.*, vol. 12, no. 2, p. 81, 2015.
[91] D. Tapscott and A. Tapscott, "How blockchain will change organizations," *MIT Sloan Manage. Rev.*, vol. 58, no. 2, p. 10, 2017.
[92] *Fair Fight Donate Via Actblue*. Accessed: May 21, 2019. [Online]. Available: https://secure.actblue.com/donate/fair-fight-reproductive-rights
[93] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría, "Blockchain and smart contracts for insurance: Is the technology mature enough?" *Future Internet*, vol. 10, no. 2, p. 20, Feb. 2018.
[94] O. Jacobovitz, "Blockchain for identity management," Dept. Comput. Sci., Ben-Gurion Univ., Beersheba, Israel, Tech. Rep., 2016.
[95] P. Dunphy and F. A. P. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Security Privacy*, vol. 16, no. 4, pp. 20–29, Jul./Aug. 2018.
[96] D. Baars, "Towards self-sovereign identity using blockchain technology," M.S. thesis, Univ. Twente, Enschede, The Netherlands, 2016.
[97] H. Harfield, "Identity crises in letter of credit law," *Ariz. L. Rev.*, vol. 24, p. 239, 1982.
[98] G. Fridgen, S. Radszuwill, N. Urbach, and L. Utz, "Cross-organizational workflow management using blockchain technology-towards applicability, auditability, and automation," Tech. Rep., 2018.
[99] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Proc. Int. Workshop Open Problems Netw. Secur.* Cham, Switzerland: Springer, 2015, pp. 112–125.
[100] G. O. Karame, E. Androulaki, M. Roeschlin, A. Gervais, and S. Čapkun, "Misbehavior in bitcoin: A study of double-spending and accountability," *ACM Trans. Inf. Syst. Secur.*, vol. 18, no. 1, p. 2, May 2015.
[101] G. Slepak and A. Petrova, "The DCS theorem," 2018, *arXiv:1801.04335*. [Online]. Available: https://arxiv.org/abs/1801.04335
[102] R. Henry, A. Herzberg, and A. Kate, "Blockchain access privacy: Challenges and directions," *IEEE Security Privacy*, vol. 16, no. 4, pp. 38–45, Jul./Aug. 2018.
[103] S. M. Smith and D. Khovratovich, "Identity system essentials," Tech. Rep., 2016.
[104] A. Biryukov and I. Pustogarov, "Bitcoin over tor isn't a good idea," in *Proc. IEEE Symp. Secur. Privacy*, May 2015, pp. 122–134.
[105] H. Vranken, "Sustainability of bitcoin and blockchains," *Current Opinion Environ. Sustainability*, vol. 28, pp. 1–9, Oct. 2017.
[106] *Bitcoin Energy Consumption Index—Digiconomist*. Accessed: May 21, 2019. [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption
[107] J. Göbel, H. P. Keeler, A. E. Krzesinski, and P. G. Taylor, "Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay," *Perform. Eval.*, vol. 104, pp. 23–41, Oct. 2016.
[108] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Commun. ACM*, vol. 61, no. 7, pp. 95–102, 2018.
[109] K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS P)*, Mar. 2016, pp. 305–320.

[110] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2016, pp. 515–532.
[111] S. Solat and M. Potop-Butucaru, "Zeroblock: Timestamp-free prevention of block-withholding attack in bitcoin," 2016, *arXiv:1605.02435*. [Online]. Available: https://arxiv.org/abs/1605.02435
[112] H. Kakavand, N. Kost De Sevres, and B. Chilton, "The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies," Tech. Rep., Jan. 2017.
[113] P. Yeoh, "Regulatory issues in blockchain technology," *J. Financial Regulation Compliance*, vol. 25, no. 2, pp. 196–208, 2017.
[114] *Countries Where Bitcoin is Banned or Legal in 2019*. Accessed: May 21, 2019. [Online]. Available: https://cryptonews.com/guides/countries-in-which-bitcoin-is-banned-or-legal.htm
[115] N. Szabo, "Micropayments and mental transaction costs," in *Proc. 2nd Berlin Internet Econ. Workshop*, May 1999, pp. 1–14.

AHMED AFIF MONRAT received the M.Sc. degree in computer science and technology from the Erasmus Mundus Master Scholarship Program PERCCOM (Pervasive Computing & Communications for sustainable development). He is currently pursuing the Ph.D. degree with the Lulea University of Technology (LTU), Skelleftea, Sweden. His research area for Ph.D. is mainly focused on sustainable blockchain technology. His research interests include expert systems, artificial intelligence, machine learning, distributed computing, and cloud computing technologies.



OLOV SCHELÉN received the Ph.D. degree in computer networking from the Lulea University of Technology. Thereafter, he has more than 20 years of experience from industry and academia. He is currently an Associate Professor with the Lulea University of Technology, and also the CEO of Xarepo AB. His research interests include mobile and distributed systems, software orchestration, computer networking, artificial intelligence, and blockchain.

KARL ANDERSSON received the M.Sc. degree in computer science and technology from the Royal Institute of Technology, Stockholm, Sweden, and the Ph.D. degree in mobile systems from the Lulea University of Technology, Sweden. After being a Postdoctoral Research Fellow at the Internet Real-time Laboratory, Columbia University, New York, NY, USA, and a JSPS Fellow with the National Institute of Information and Communications Technology, Tokyo, Japan, he is currently an Associate Professor of pervasive and mobile computing with the Lulea University of Technology. His research interests include mobile computing, the Internet of Things, cloud technologies, and information security.