Everything you Wanted to Know about the Blockchain

By Deepak Puthal, Nisha Malik, Saraju P. Mohanty, Elias Kougianos, and Gautam Das

In 2008, the emergence of the blockchain as the foundation of the first ever decentralized cryptocurrency not only revolutionized the financial industry but proved a boon for peer-to-peer information exchange in the most secure, efficient, and transparent manner. The blockchain is a public ledger which works like a log by keeping a record of all transactions in a chronological order, secured by an appropriate consensus mechanism and providing an immutable record. Its exceptional characteristics include immutability, irreversibility, decentralization, persistence and anonymity. With these advantages, it has found applications in almost all fields requiring data sharing among multiple parties but with secure authentication, anonymity and permanence. Some of the applications are finance, real-estate, and IoT. Despite having numerous benefits, the blockchain suffers from various disadvantages, particularly reaching consensus in a vast network quickly, energy consumption in computation, and requiring storage of the entire chain for verification. This paper discusses the ins and outs of the blockchain fundamentals, its working, different consensus mechanisms, applications, challenges and current trends. This paper is an extension of our previous instalment about the basics of blockchain [1].

1. INTRODUCTION

Throughout time, the information and communication technology has undergone numerous transformations for facilitating easier, quicker, efficient and secure sharing and exchange of data, information, and funds in assorted ways. With the emergence of the Internet, digital communications emerged, empowering all forms of data and information interchange through online transactions, such as financial transactions for making payments and receiving funds. The entire transactional and communication system goes through a trusted intermediary which not only guarantees safe and secure delivery, but in case of financial transactions, ensures accurate changes being reflected in multiple accounts. This trusted party is questionable in case of any failures in updating data, delays in delivery or fraud [2]. But with just a single network controller multiple questions arise:

1. What if this trusted party becomes rogue and cannot be trusted?
2. What if it is hacked and an attacker gets hold of all the data? This intermediary here acts as a single point of failure.
3. Each time an intermediary is used, additional delay in communication occur. Why not communicate peer-to-peer?
4. The authenticity and validation of each transaction is very important, but can the intermediary be trusted?

The solution to all the above problems is provided by the blockchain, the underlying technology invented by Satoshi Nakamoto (considered a pseudonym) in introducing the first ever decentralised cryptocurrency called as 'Bitcoin' [3], [4], [5]. Bitcoin exchange and transfer occur by means of a shared distributed ledger, which records the details of every transaction occurred among the network participants without involving any trusted centralized party. The single copy of the ledger resides in synchronization with all the involved parties, thus reducing the risk of a single point of failure. Bitcoin works on Public Key Infrastructure (PKI) in the blockchain for authenticating anonymous users and controlling access. For source authentication and identification, each transaction is digitally signed by the owner with the private key. To keep a track of transactions occurring simultaneously, multiple transactions are grouped together in a structure called a 'block' uniquely identified by its hash and timestamp. Validation of transactions and the block, among potentially distrusted users is done using a consensus mechanism, which means the state of the shared ledger is updated by the

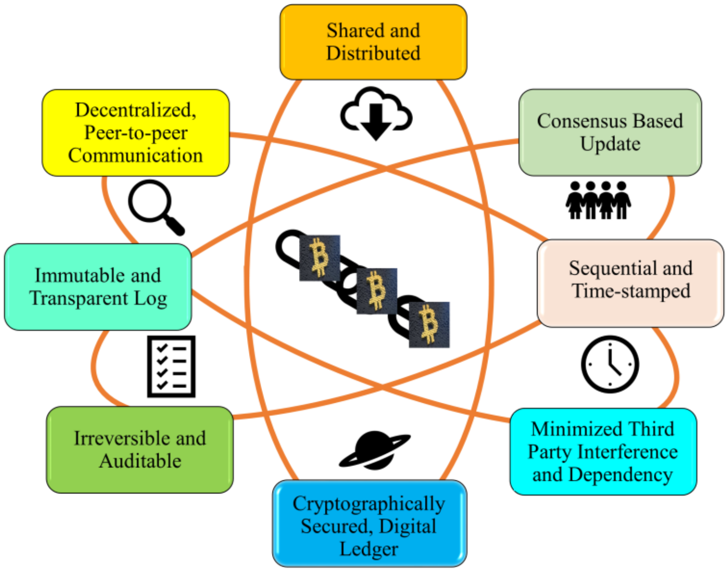
Shared and Distributed
Consensus Based Update
Sequential and Time-stamped
Minimized Third Party Interference and Dependency
Cryptographically Secured, Digital Ledger
Irreversible and Auditable
Immutable and Transparent Log
Decentralized, Peer-to-peer Communication

FIGURE 1. Vital blockchain characteristics.

agreement/consensus of the majority of nodes. This updating in case of bitcoin employs the proof-of-work consensus algorithm, whereby miners strive to find a special value to achieve the block's hash, less than a target value, which is usually set to avoid any conflicts and establish trust. This target value is set in such a way that miners compete to find a nonce (a unique, one-time number) in around 10 mins, hence the block generation time is 10 mins. This process by which nodes perform rigorous computations, thus devoting their resources (such as CPU, electricity, etc.) to find the nonce is called *mining* and the nodes doing so are called as *miners*. Through mining, nodes compute the proof-of-work which is a form of achieving consensus among the distrusted modes. The blockchain characteristics are depicted in Figure 1 [6], [7]. With the above characteristics, the blockchain has found applicability in other sectors as well, and not just cryptocurrencies. A broad overview of blockchain technology is presented in Figure 2.

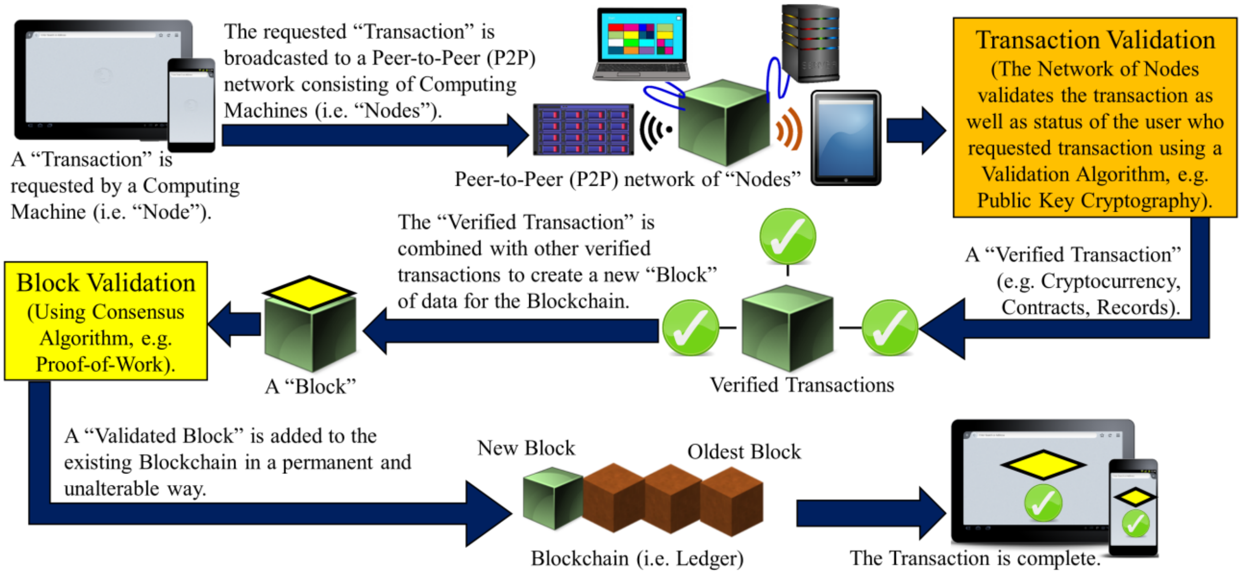
The requested "Transaction" is broadcasted to a Peer-to-Peer (P2P) network consisting of Computing Machines (i.e. "Nodes").
A "Transaction" is requested by a Computing Machine (i.e. "Node").
Peer-to-Peer (P2P) network of "Nodes"
Transaction Validation
(The Network of Nodes validates the transaction as well as status of the user who requested transaction using a Validation Algorithm, e.g. Public Key Cryptography).
The "Verified Transaction" is combined with other verified transactions to create a new "Block" of data for the Blockchain.
A "Verified Transaction" (e.g. Cryptocurrency, Contracts, Records).
Block Validation
(Using Consensus Algorithm, e.g. Proof-of-Work).
A "Block"
Verified Transactions
A "Validated Block" is added to the existing Blockchain in a permanent and unalterable way.
New Block
Oldest Block
Blockchain (i.e. Ledger)
The Transaction is complete.

FIGURE 2. Overview of blockchain.

2. WORKING MODEL

In this section, we explain the core components comprising the blockchain network setup and their importance. Then we discuss the different phases of blockchain functionality, where these components collaborate in performing secure communication among distrusted nodes by publishing a distributed log of the committed transactions, using a consensus mechanism. Next, we give an overview of the stepwise network operation. We have taken the bitcoin blockchain as an example here to illustrate most of the blockchain functioning.

2.1 Core Components

The blockchain setup and network operations are built upon the core components shown in Figure 3.

2.1.1. Asymmetric key Cryptography: The blockchain network utilizes the capabilities of public key cryptography for secure operation of the blockchain. To perform any exchange, other than being on the same platform, the users need to possess a digital wallet (functioning like a bank account) secured with the user's private key, and accessible with appropriate signatures generated using that private key. This wallet's public key serves as the bitcoin address known to everyone, which is advised to change with each transaction for maintaining privacy and anonymity of users. Private keys are used to digitally sign transactions and are kept secret by the user.

2.1.2. Transactions: The Blockchain enables the sharing and exchange of information among nodes on a peer-to-peer basis. This exchange takes place by means of files containing transfer information from one node to the other, generated by a source node and broadcasted to the entire network for validation. The current state of blockchain is represented by these transactions, which are continuously generated by the nodes, and then congregated in blocks. In the case of bitcoin, each transaction represents the transfer of currency from one node to the other. All nodes are aware of the current balance at each address and maintain a copy of the existing blockchain, which is the log containing the history of previous transactions. The state of the blockchain changes after each transaction [8]. With a huge number of transactions generated each second, it is very important to validate and verify the genuine ones and discard the fake.

2.1.3. Consensus Mechanism: When nodes begin data sharing and exchanging via a blockchain platform, they don’t have a centralized party to regulate and resolve disputes or safeguard against security violations and a mechanism to keep track of the flow of funds and ensure an unassailable exchange to avoid fraud, such as double spending attacks [9], [10] is needed. All nodes should agree on a common content updating protocol for this ledger, to maintain a consistent state and blocks should not simply be accepted to be a part of the blockchain, without majority consent. This is called a consensus mechanism, by which blocks are created and added to the existing ledger for future use. In the case of bitcoin the recipients, after signature verification, might redeem outputs multiple times for use in subsequent transactions as they would seem valid by individual recipients. Thus, solely for avoiding the double spending, Satoshi was the first one to propose a consensus based decentralized cryptocurrency among non-trusted nodes. This consensus is an agreement amongst the nodes, which involves block mining, wherein miners compete to find the next valid block by computing a cryptographic block hash. Nodes finding the solution are rewarded with some bitcoins, thereby generating new currency. This hash value is called ‘the proof of work’ and if all transactions and proof-of-work are valid, the nodes accept it by updating their copy.

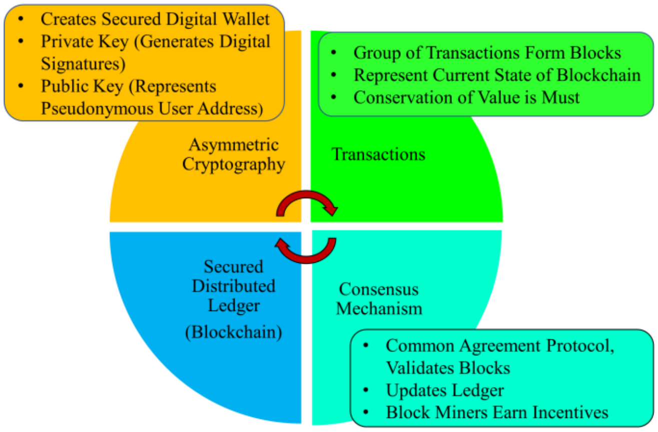
• Creates Secured Digital Wallet
• Private Key (Generates Digital Signatures)
• Public Key (Represents Pseudonymous User Address)
• Group of Transactions Form Blocks
• Represent Current State of Blockchain
• Conservation of Value is Must
Asymmetric Cryptography
Transactions
Secured Distributed Ledger
(Blockchain)
Consensus Mechanism
• Common Agreement Protocol, Validates Blocks
• Updates Ledger
• Block Miners Earn Incentives

FIGURE 3. Core components of blockchain.

2.2. Phases of Operation

We split the complete block formation process in the blockchain into two phases: 1) Transaction generation and verification, and 2) Consensus execution and block validation.

2.2.1. ***Transaction Generation and Validation:***

A. Contents

Users connected within the same network have knowledge of each other’s address before they begin any transfer. When a new transaction is initiated, it includes input transactions, namely the amount to be transferred and the recipient’s bitcoin address. For example, if Sheryl needs to transfer 5.0 BTC to Alice, then the transaction executing this transfer contains the following: *Input transactions*: These are the source/descendant transactions whose unused transaction outputs (UTXO), serve as an input in this transaction. In other words, it refers to the hash of the transaction which supplies the record indicating from what source Sheryl earned that 5.0 BTC in her bitcoin wallet she intends to transfer. These can be one or more transactions whose sum turns up to be 5.0 BTC. Say for example, there are 4 transfers received from multiple sources whose sum is 5.0 BTC and these have already been published in the ledger. Then there would be 4 input transactions for the next transfer. The outputs of the transaction depend upon all places she would split and send these 5.0 BTC. *Amount to be transferred*: 5.0 BTC in this case. *Public key hash of the receiver*: this is Alice’s bitcoin address where she would receive the 5.0 BTC. Transactions are uniquely identified by their transaction ID, which is the SHA-256 hash value of the input transaction and public key of the recipient. This is further encrypted with the sender’s private key, for generating digital signatures to assist recipients in uniquely identifying the source. If any content is changed, it would consequently affect the Transaction ID as well as the signatures, and in case of mismatch the transaction is discarded.

B. Confirmation of transaction

When Alice learns about Shirley’s transaction crediting funds to her bitcoin address, she needs to confirm that there is no double spending by Shirley and that the transaction has been confirmed with its existence in a valid block of the ledger. Until the time the transactions are confirmed, they are not considered trustworthy. Transactions are committed only if, upon reception of the transaction, Alice could verify the following:

a. The referenced *input’s transaction’s UTXO is valid* i.e. there is not double spending. Satoshi, to prevent double spending in bitcoin, proposed that the output of a transaction can be redeemed in following one subsequent transaction, and only after its successful verification both via signatures and ledger entry, the output could be redeemed in another transaction.

b. Since only the user authorized to access the UTXO can use it in a subsequent transaction, the recipient checks for the *valid signature* which should match the UTXO owner signature.

c. The referenced transaction must be *published in a valid block*. The existence of a transaction in a block confirms its validation.

d. *Conservation of value is a must*, which means that during the transfers, it is mandatory that the sum of input UTXOs equals the sum of output UTXOs, subtracting the amount of coin base transactions. This is called conservation of value and is most important in checking a transaction's validity. Figure 4 shows the transaction broadcast and verification among the network nodes.

C. Claiming ownership

Every transaction produces an output redeemable by the recipient nodes authorized in the public key hash of the transaction. This public key hash authenticates users by uniquely identifying them in the network while preserving their privacy. Apart from this pseudonymous identity, users need a private key to control access to their bitcoins. Only those users who can generate valid signatures with their private keys can claim ownership for redeeming transaction outputs. Thus, a public key hash and a private key are the essentials to enable users to redeem funds.

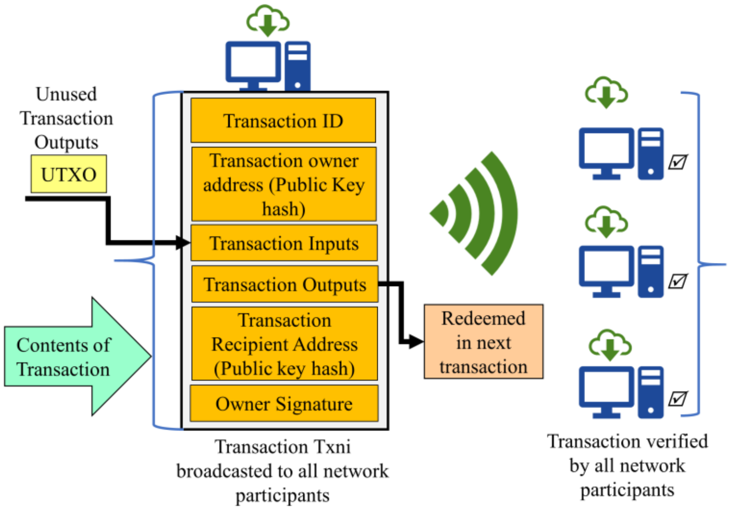
Unused Transaction Outputs
UTXO
Transaction ID
Transaction owner address (Public Key hash)
Transaction Inputs
Transaction Outputs
Transaction Recipient Address (Public key hash)
Owner Signature
Contents of Transaction
Redeemed in next transaction
Transaction Txni broadcasted to all network participants
Transaction verified by all network participants

FIGURE 4. Transaction broadcast and verification.

2.2.2 Consensus, mining and block validation

Nodes, in the absence of a trusted party follow a consensus on how to confirm or discard blocks and transactions with mutual effort so that there aren't any conflicts at a later stage. This consensus in bitcoin is achieved by 'proof-of-work' which proves how much work has been put in for validating a block. A cryptographic puzzle is to be solved for acceptance of any block and its addition in the shared ledger. This works by nodes accumulating the verified transactions in a block and putting their resources (such as computation power and electricity) to find a value that makes the SHA-256 hash value of this block less than a dynamically varying target value. The block contents include, the arbitrary nonce, hash of the previous block, Merkle root hash of the listed transactions, timestamp and block version. The term 'proof-of-work' refers to this random value which is found by the miners, by repeatedly hashing the block contents with many such random values to achieve the Cryptographic block hash. The blockchain structure is shown in Figure 5. The necessary steps for block validation are summarized as follows:

1. All the transactions contained in the current block are verified by the steps discussed in Section 2.2.1 (c). After individual verification, the transactions' chronological order conforming to their occurrences and references is confirmed.
2. The previous block's hash referenced by the current block exists and is valid. This is usually checked from the genesis block.
3. Accuracy of time stamp is verified.
4. The proof-of-work for the current block is valid.

2.3 Network Operation

The network operation steps are defined as follows by the order of their execution.

Transaction broadcast: There should be no direct transactions between source-destination; instead all transactions should be announced to the entire network for verification through broadcasting.

Transaction collection and verification: Nodes verify all transactions as per steps in Section 2.2.1(c) and accumulate them in a block, depending upon the block size, which is 1MB for bitcoin.

Running consensus protocol: To add this block to the blockchain, nodes put their resources at work and start the mining process to solve the cryptographic puzzle by finding proof-of-work. Upon solving the puzzle, the block is broadcasted to the entire network.

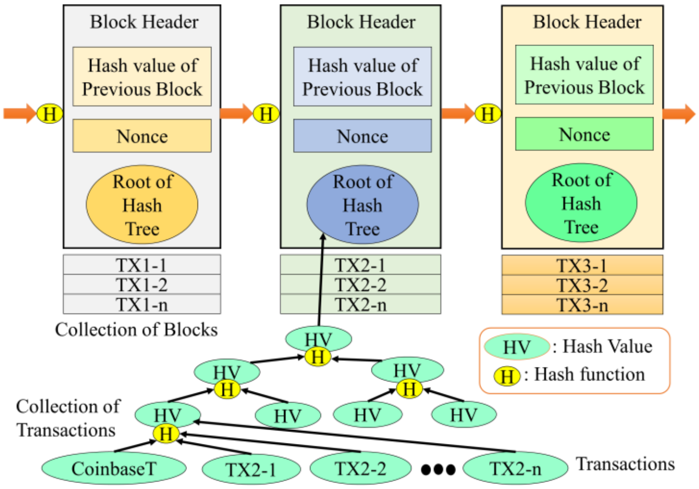

FIGURE 5. Structure of Blockchain.

Block acceptance and chain update: Upon reception of blocks by nodes, two scenarios can occur:

I. Either nodes *accept* the block, provided that all transactions contained in it are valid and the computed proof-of-work is correct. Nodes show their approval and acceptance, by adding the block to their copy of the ledger and advancing to find the next valid block, with this block as a predecessor, and taking its hash as the previous hash for the successive block. If two miners find a valid solution at the same time, only the longest blockchain is considered valid. This is how the blockchain is made tamper-proof and changes once made cannot be reversed.

II. If the transactions in this block or proof-of-work isn't valid, the block is discarded, and nodes continue to find a valid block.

Earning Incentives: Miners earn incentives upon successful acceptance of blocks. This is to keep nodes honest and make the system robust.

3. CLASSIFICATION OF BLOCKCHAIN SYSTEMS

Based upon several criteria, blockchain systems are classified as public, private and consortium, as shown in Figure 6.

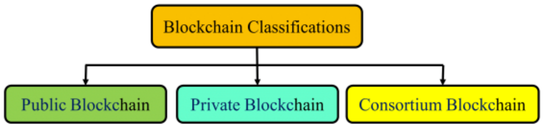

FIGURE 6. Classification of blockchains.

3.1 Public Blockchain

A public blockchain provides an open platform for people from various organizations and backgrounds to join, transact and mine. There aren't any restrictions on any of these factors. Therefore, these are also called *'permission-less'* blockchains. Every participant is given full authority to read/write transactions, perform auditing in the blockchain or review any part of the blockchain, anytime. The blockchain is open and transparent and there are no specific 'validator nodes'. All users can collect transactions and begin with the mining process to earn mining rewards. The availability of the copy of the entire blockchain synchronized with all the nodes makes it immutable. With complete decentralization, the vastness of existing networks, and an open platform for anyone to join, consensus is achieved by any of the decentralized consensus mechanisms such as proof-of-work, proof-of-stake, etc. Of course, the public availability of the ledger in a private blockchain system exposes it to attacks. The robust mechanism of proof of work combined with cryptographic validation of the entire blockchain each time a new block is added offset this shortcoming.

3.2 Private Blockchain

It is a type of blockchain system which is setup to facilitate private sharing and exchange of data among a group of individuals (in a single organization) or among multiple organizations with mining controlled by one organization or selective individuals. It is also called a permissioned blockchain since unknown users cannot get access to it, unless they receive a special invitation. Nodes' participation is decided either by a set of rules or by the network in-charge, to control access. This inclines the network more towards centralization, while derogating the elementary blockchain features of complete decentralization, and openness as defined by Satoshi. In a private blockchain system, once nodes become part of the network, they contribute in running a decentralized network, with each node maintaining a copy of the ledger, and collaborating to reach a consensus for updating, but unlike public blockchain the writes are restricted.

3.3 Consortium Blockchain

A consortium blockchain can be considered as a *partially private* and *permissioned* blockchain, where not a single organization but a set of pre-determined nodes are responsible for consensus and block validation. These nodes decide who can be part of the network and who can mine. For block validation, a multi-signature scheme is used, where a block is considered valid, only if it signed by these nodes. Thus, it is a partially centralized system, owing to the control by some selected validator nodes, unlike the private blockchain which is completely centralized, and the public blockchain which is completely decentralized. It is decided by the consortium whether read or write permissions would be public or limited to the network participants. Also, the restriction of consensus to a set of nodes doesn't guarantee immutability and irreversibility, since control of the consortium by a majority can lead to tampering of the blockchain.

4. CONSENSUS ALGORITHMS

A consensus in a decentralized and distributed network with distrusted users is the sole and imperative determinant of the next secure update of their shared state. The following subsections presents various approaches to achieve consensus in a blockchain network, as shown in Figure 7.

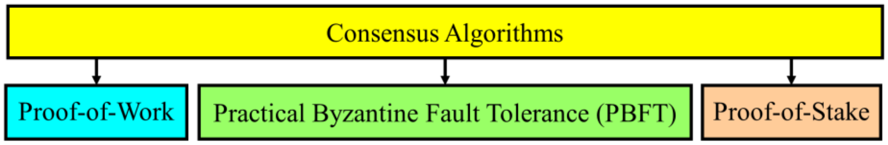

FIGURE 7. Consensus approaches in the blockchain.

4.1 Practical Byzantine Fault Tolerance Algorithm (PBFT)

The PBFT algorithm was proposed as a solution to the Byzantine Generals problem, which is about conducting a successful attack on a rival city by the Byzantine army [11], [12]. For the Byzantine army to win, all loyal generals must work on the same plan and attack simultaneously. In addition, no matter what the traitors do, the loyal generals should stick to the decided plan and a small number of traitors should ruin the plan. Similarly, in the blockchain, PBFT works to establish consensus among the participating nodes. Nodes maintain a current state, which upon reception of a new message is fed together with the message received for computations, to help the node reach a decision. This decision is then broadcast to the network. The majority of the decisions determine consensus for the network. Hyperlegder [13], which is working for developing consortium blockchain systems for businesses, utilizes PBFT as its underlying consensus mechanism. It should be pointed out that many of the new developments on blockchain stem from prior work on distributed databases. Examples of such prior work are [14], [15], [16].

4.2 Proof-of-Work (POW)

Proof-of-work was the first decentralized consensus protocol proposed by Satoshi, to achieve consistency and security in the bitcoin network. In bitcoin, currency transfer occurs in a completely decentralized fashion, thus requiring a consensus for authentication and block validation. The nodes in the bitcoin network compete to calculate the hash value of the next block, which is supposed to be less than a dynamically varying target value, determined by the consensus rule. Nodes achieving the solution, wait for mutual confirmation by other nodes, before adding the block to the existent blockchain. More than one valid block might be generated, if multiple nodes find an appropriate solution causing a temporary fork (branch) in the network. In such scenarios, all of them are acceptable and nodes closer to the miners accept the solution they receive and forward the same to other peers. The conflict at a later stage is avoided by accepting the 'Longest Version' of the chain available at any time.

4.3. Proof-of-Stake (POS)

Proof-of-stake was proposed to overcome the disadvantages of excessive power consumption by POW in bitcoin. Ethereum utilizes POS to achieve consensus. Instead of investing in resources which can perform rigorous computations for hash calculations in POW, POS proposes to buy cryptocurrency and use it as stake in the network. The stake is directly proportional to the chance of becoming the block validator. To reach consensus, the block validator is randomly selected and is not predetermined. The nodes producing valid blocks get incentives, but if their block is not included in the existing chain, they also lose some amount of their stake. Different consensus models have been differentiated based upon several factors [17]:

a. ***Type of blockchain*** – Whether the blockchain network is permissioned or permission-less.
b. ***Transaction rate*** – At what rate are transactions confirmed, which is basically decided by the consensus algorithm. In bitcoin, which employs POW, the transaction rate is only 7 transactions/sec, because POW requires significant computation time and the block generation time is 10 minutes.

c. ***Scalability:*** A blockchain system is scalable, if it can achieve consensus with the number of nodes continuously growing, especially in public blockchain systems.

d. ***Participation charges:*** For some systems, initial cost of participation is required. For example, with POS, nodes invest in the cryptocurrency, to express their interest in the consensus and block validation, whereas POW requires energy input, which isn't necessary if you simply want to be part of the network and do not wish to mine.

e. ***Trust condition:*** This determines if the nodes contributing are to be trusted and predetermined, just like in consortium and private blockchain systems or unknown like in public and POW based blockchains.

5. APPLICATIONS AND USE CASES

The blockchain has the capacity to revolutionize the security, stability and transparency of networks in need, provided applied appropriately and only if needed, because it is not a panacea for all security applications. Figure 8 shows some of the areas where blockchain finds application and is currently being used owing to its advantages.

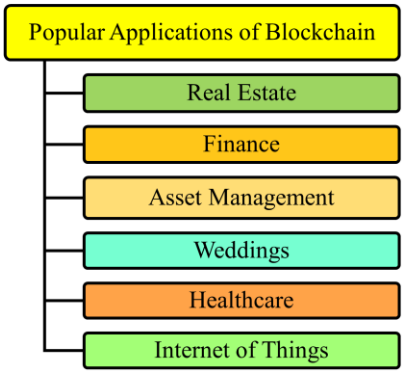

FIGURE 8. Blockchain applications.

Blockchain in Asset Management - It is all about securely transferring assets within a business network. An asset could be a physical one like a server, computer or a laptop or an intangible one like software and services. The blockchain offers shared ledger capability which means full visibility from end to end into a business network. The blockchain is employed right from serialization to being deployed on the floor and focuses only on five key events i.e. manufacturing serialization of assets to initiate the blockchain, receiving and validation of assets, asset capitalization, warranty activation and installation of the asset.

Blockchain in Real Estate – Transactions in real estate are cumbersome, opaque and expensive mainly because of the involvement of the various middlemen like brokers, government property databases, title companies, escrow companies, inspectors and appraisers, notary publics etc. The blockchain will enable every property, everywhere, to have a corresponding digital address that contains occupancy, finance, legal, building performance, and physical attributes that conveys perpetually and maintains all historical transactions.

Blockchain in Finance – A very important process, which becomes quite expensive and sluggish, due to the presence of unnecessary middlemen is cross-border payments. It takes several banks (and currencies) before the money can be collected. Services like Western Union can be used which are faster but also expensive. The blockchain can speed up and simplify this process, cutting out the unnecessary middlemen. At the same time, it makes money remittance more affordable. Until now, the costs of remittance were 5-20%. The blockchain reduces the costs to 2-3% of the total amount and provides guaranteed, real time transactions across borders.

Blockchain in the IoT - IoT solutions using blockchain can be built to maintain a continuously growing list of cryptographically secured data records protected against alteration and modification. For instance, as an IoT connected (e.g. RFID) asset with sensitive location and temperature information moves along various points in a warehouse or in a smart home [18], this information could be updated on a blockchain. This permits all involved parties to share data and status of the package as it moves among different gatherings to guarantee the terms of an agreement are met [19], [20].

Blockchain Assisting Weddings – It is possible to search for a bride or groom online and then physically meet and get to know each other and finally making commitments and involving in a marriage. Now this entire end to end process can be done online, right from finding someone to getting the monetary wedding gifts. In 2014, the first couple to do this was Joyce and David Mondrus [21].

Blockchain in Healthcare – A blockchain based management of patient's health records is proposed in [22]. The patient's medical history is stored on a decentralized system, accessible to the treating doctors, and medical insurance providers.

6. CHALLENGES

Despite its capabilities and benefits, the blockchain has a few disadvantages, the most serious being the scalability problem. The consensus and block validation require the presence of the entire blockchain, i.e. all the transactions that ever happened, thus demanding a lot of storage. The restriction of the block size contributes majorly in the scalability issue. With the limitation of 1MB block size and the delayed consensus process, only 6-7 transactions are confirmed in a second, with high transaction fees. Increasing the size of the blocks would create an additional delay by decelerating the propagation of the block. To achieve security with reduced block size, a new version of blockchain called Bitcoin-NG was proposed [23], which divides the block into two parts to reduce the propagating size. Forks in typical blockchain networks, cause further delay, while the longest version is awaited by the nodes, to confirm the correct blockchain. Another issue with blockchain is the '51% attack' problem. This problem arises if more than 51% of the nodes collude to generate fake blocks or reverse confirmed transactions. Since greater computation power leads to quicker generation of the blocks, genuine nodes would not be able to compete for a fair version of the blockchain as nodes would only believe the longest version. Another important challenge of the blockchain is the power or energy requirement [24]. It is estimated that mining of 1 bitcoin needs energy equivalent to 2 years consumption of a typical US household. It is also estimated that energy consumption for each bitcoin transaction is equivalent to 80,000X of energy consumption of a credit card processing. The above described challenges are shown in Figure 9.

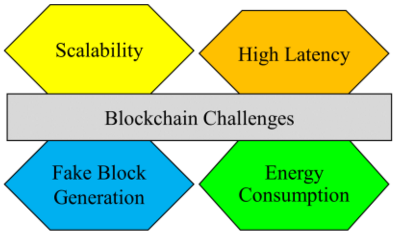

FIGURE 9. Challenges of Blockchain.

7. CONCLUSION

The blockchain is used globally for securing peer-to-peer infrastructure with decentralization. This paper presented a comprehensive review of the blockchain by highlighting the working model of blockchain and subsequently presenting the system features. Consensus algorithms are described with different applications and use cases. Finally, this paper is concluded with presenting different security challenges.

ABOUT THE AUTHORS

Deepak Puthal (deepak.puthal@uts.edu.au) is a Lecturer (Assistant Professor) in the Faculty of Engineering and IT at University of Technology Sydney (UTS), Australia. He is an author of 45+ peer reviewed research articles.

Nisha Malik (nisha.malik@student.uts.edu.au) is a Ph.D. student in the Faculty of Engineering and IT at University of Technology Sydney, Australia.

Saraju P. Mohanty (saraju.mohanty@unt.edu) is a Professor at the University of North Texas. Prof. Mohanty's research is in Smart Electronic Systems. He is an author of 250 research articles, and 3 books. He is the Editor-in-Chief of the IEEE Consumer Electronics Magazine.

Elias Kougianos (eliask@unt.edu) is Professor in Engineering Technology at the University of North Texas. He is author or co-author of over 120 peer-reviewed journal and conference publications.

Gautam Das (gdas@cse.uta.edu) is Endowed Chair Professor in Computer Science and Engineering at the University of Texas at Arlington. He is author over 250 peer-reviewed journal and conference publications.

REFERENCES

[1] D. Puthal, N. Malik, S. Mohanty, E. Kougianos, and C. Yang, "The Blockchain as A Decentralized Security Framework", *IEEE Consumer Electronics Magazine*, Vol. 7, No. 2, pp. 18--21, 2018.

[2] D. Puthal, S. Mohanty, P. Nanda, and U. Choppali, "Building Security Perimeters to Protect Network Systems against Cyber Threats", *IEEE Consumer Electronics Magazine*, Vol. 6, No. 4, pp. 24-27, 2017.

[3] R. Grinberg, "Bitcoin: An Innovative Alternative Digital Currency", *Hastings Science & Technology Law Journal*, Vol. 4, pp. 159-208, 2012.

[4] S. Barber, X. Boyen, E. Shi, and E. Uzun, "Bitter to better -- How to make bitcoin a better currency", in *Proceedings of the International Conference on Financial Cryptography and Data Security*, pp. 399-414, 2012.

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf, Last visited 11th November 2017.

[6] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A Survey on the Security of Blockchain Systems", *Future Generation Computer Systems*, 2017, doi = https://doi.org/10.1016/j.future.2017.08.020.

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

[8] A Next Generation Smart Contract & Decentralized Application Platform, https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf, Accessed 15th December 2017.

[9] G. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin", in *Proceedings of ACM conference on Computer and communications security*, pp. 906-917, 2012.

[10] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. Kroll, and E. Felten, "Sok: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies", in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 104-121, 2015.

[11] M. Castro, and B. Liskov. "Practical Byzantine fFault Tolerance", in *Proceedings of the 3rd Symposium on Operating Systems Design and Implementation*, pp. 173-186, 1999.

[12] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem", *ACM Transactions on Programming Languages and Systems*, Vol. 4, No. 3, pp. 382-401, 1982.

[13] Hyperledger project, https://www.hyperledger.org/, 2015, Last Accessed on 4th February 2018.

[14]: C. Mohan, "Blockchains and Databases: A New Era in Distributed Computing", http://www.hpts.ws/papers/2017/mohan.pdf, Last accessed on 28th Februaty 2018.

[15] Tien Tuan Anh Dinh, Rui Liu, Meihui Zhang, Gang Chen, Beng Chin Ooi, and Ji Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems", https://arxiv.org/abs/1708.05665, Last Accessed on 4th February 2018.

[16] Tien Tuan Anh Dinh, Ji Wang, Gang Chen, Rui Liu, Beng Chin Ooi, and Kian-Lee Tan, "BLOCKBENCH: A Framework for Analyzing Private Blockchains", in *Proceedings of the ACM International Conference on Management of Data*, pp. 1085-1100, 2017.

[17] A. Baliga, Understanding Blockchain Consensus Models, Technical Report, Persistent Systems Ltd, April 2017, https://www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Blockchain-Consensus-Models.pdf, Last Accessed on 4th February 2018.

[18] A. Dorri, S. Kanhere, R. Jurdak, and P. Gauravaram "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home", in *Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops*, pp. 618-623, 2017.

[19] D. Puthal, M. S. Obaidat, P. Nanda, M. Prasad, S. Mohanty, and A. Y. Zomaya, "Secure and Sustainable Load Balancing of Edge Datacenters in Fog", *IEEE Communications Magazine*, 2017, pp. in Press.

[20] S. Ray, D. Puthal, S. Sharma, S. P. Mohanty, and A. Y. Zomaya, "Building a Sustainable Internet of Things", *IEEE Consumer Electronics Magazine*, Vol. 7, No. 2, March 2018, pp. 42--49.

[21] Use the Blockchain Technology for Smart Contracts, https://cointelegraph.com/news/david-and-joyces-wedding-demonstrates-how-easy-it-is-to-use-the-blockchain-technology-for-smart-contracts, Accessed 15 December 2017.

[22] A. Ekblaw, A. Azaria, J. D. Halamka, A. Lippman, "A Case Study for Blockchain in Healthcare: "MedRec" Prototype for Electronic Health Records and Medical Research Data", Whitepaper, August 2016, http://dci.mit.edu/assets/papers/eckblaw.pdf, Last Accessed 04 Feb 2018.

[23] I. Eyal, A. Gencer, E. Sirer, and R. Renesse, "Bitcoin-NG: A Scalable Blockchain Protocol", in *Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation*, 2016, pp. 45-59.

[24] N. Popper, "There is Nothing Virtual About Bitcoin's Energy Appetite", The New York Times, 21st Jan 2018, https://www.nytimes.com/2018/01/21/technology/bitcoin-mining-energy-consumption.html, Last Accessed on 23rd January 2018.