

# Blockchain and Its Applications: A Systematic Review

**Basundhara Chakrabarty**  
Customer Experience, Security  
Cisco Systems, Inc  
Bangalore, India

**Harish Krishnamoorthy**  
Customer Experience, Service Provider  
Cisco Systems, Inc  
Bangalore, India

**Karan Shahani**  
Deputy Category Manager  
BulkMRO  
Mumbai, India

**Abstract** -Blockchain has crept into all facets of technology and have brought about an upheaval in existing systems. This work provides a systematic review of blockchain technology and its applications, elaborating on the benefits and shortcomings of each. It details on the salient features of blockchain, the current themes, trends, and emerging areas of research in blockchain, and highlights how it revolutionizes the financial, industrial, political, and socio-economic sectors. Based on a thorough analysis of prevailing research, we classify blockchain-based applications across various spheres like Smart Industries, Governance, Healthcare, Supply Chain, etc. The paper, thus, juxtaposes the major highlights and the research gaps in the field of blockchain technology.

**Keywords**-Blockchain, Decentralization, Industry, Commerce.

## I. INTRODUCTION

Blockchain technology came to the limelight when in 2008, the pseudonym Satoshi Nakamoto proposed a peer-to-peer cryptographic currency called 'bitcoin' [1]. Bitcoin employed distributed ledger technology [2] with transactions being stored within 'blocks'. Each block in a bitcoin contains the hash of the previous block. Thus, an attempt to tamper with a block requires a re-calculation of all the subsequent blocks of the chain, a process that is computationally infeasible. Furthermore, Nakamoto believed that 'the only way to confirm the absence of a transaction is to be aware of all the other transactions'. Hence, the bitcoin ledger is publicly available to all the participants, and addition of new blocks to the chain requires the consensus of a majority of participants.

He propounded a 'proof of work' consensus mechanism where each participant must solve a complex computation and calculate the appropriate 'nonce' value to add the block to the chain. Nakamoto's paper caused a remarkable stir in the world of cryptocurrencies. Blockchains soon emerged beyond the confines of cryptocurrency and found its way into industrial, commercial, health care and financial sectors. In this paper, we perform a review of the primary features of blockchains and their applications in various sectors.

## II. SALIENT FEATURES OF BLOCKCHAIN

A blockchain can be thought of as a growing list of transaction records. Each block in a blockchain has a block header and a block body, and points to the previous block via a reference which is the cryptographic hash of the previous block. The first block in the blockchain is referred to as a 'genesis' block, which is the absolute

parent of all subsequent blocks. Each following block contains a block header and a block body. The block header comprises the block version, the parent block's hash, the nonce and a Merkle tree root hash [3] of all transactions in the block. The block body maintains a list of transactions and a transaction counter. The block size and the size of each individual transaction determines the capacity of the blockchain.

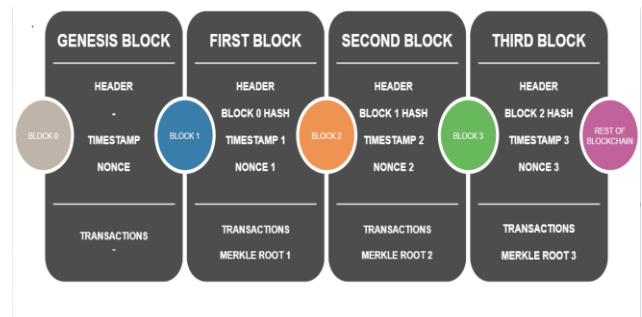


Fig.1. A diagrammatic representation of blockchain.

Blockchains employ public key cryptography [4] to validate transactions. For eg., if A wants to attest a transaction, he signs the hash of the transaction with his private key and sends it across to B. B can then decrypt the hash value by using A's public key and verify whether the decrypted hash matches the hash value encoded in the received transaction. This validation of transactions by nodes makes falsification of information very difficult. The following are the primary features of blockchain:

**1. Decentralization:** Traditional banking systems require transactions to be validated and monitored by a centralized server (eg., the bank). This system not only adds to maintenance costs, but also causes frequent bottlenecks at the centralized servers. In contrast, blockchains present a peer-to-peer transaction mechanism wherein two parties can exchange information sans the

intervention of a centralized server. Blockchains, hence eliminate a single point of failure by virtue of decentralization.

**2. Immutability:** Since each block stores the hash of the previous block, blockchains are almost impossible to tamper with. Any attempt to add or change a block would require a re-calculation of all the preceding hash values, lest the blockchain be rendered invalid. The most popular cryptographic hashing algorithms employed to preserve immutability in blockchains are elliptical-curve algorithms [5].

**3. Consensus and Mining:** Consensus mechanisms dictate how nodes in a blockchain elect and confirm the authenticity of the blocks to be added. Nakamoto described a permissionless consensus mechanism called 'Proof-of-work' based on a cryptographic block-racing game. In particular, PoW requires nodes to recursively query a hash function for a partial preimage generated from a participating block. The nodes participating in the block racing-game are called 'miners' and the PoW process is called 'mining'.

To maintain security, bitcoin generates roughly one 1 MB block every 10 minutes (often known as the block frequency), causing hours of waiting to confirm each transaction. This leads to a substantial reduction in the throughput, potentially resulting in high transaction fees and subpar user experience. There are several research endeavors to improve the speed of PoW-based transactions. Conflux, for example, is a fast blockchain framework that can process thousands of transactions in a matter of seconds, thus speeding up the verification process [6]. Proof of stake (PoS) is an energy-efficient alternative to Proof of Work. PoS randomly elects a block and delegates to it the authority to contribute to the blockchain. Unlike PoW, PoS doesn't offer any explicit reward or incentive to members to participate in a computational arms race, however, a block reward is conferred to a validator for updating the blockchain.

Since a tremendous amount of computational resources are required for mining, miners often cooperate with one another to form a mining pool. Qin's further work analyzes the comparative risks incurred by miners for different pool selection strategies in [7]. The exploits of mining are distributed between the members of the mining pool following a sharing mechanism like proportional mechanism, pay-per-share mechanism or pay-per-last-N-shared. These reward mechanisms are explored in depth by Qin in [8].

**4. Access:** The landscape of blockchain technology evolved and gave rise to three distinct types of blockchains based on access: public, private and permissioned. Public blockchains allow anyone to join in as a new node or miner. Some of the biggest examples of

a public blockchain are bitcoins and Ethereum. Ethereum is an open-source platform which offers a build-in Turing-complete programming language that allows users to write applications called 'smart contracts' [9]. These smart contracts are written in languages like Solidity and executed by Ethereum Virtual Machines codes [10]. Maintaining privacy and trust within public blockchains is a consistent area of research as a substantial amount of sensitive data is available and accessible to the public.

Atzei introduces the various security pitfalls smart contracts are vulnerable to in [11]. In [12], Yuan designed ShadowEth, a framework that allows a secure platform for storage of private contracts within the trusted execution environment of public blockchains. The vulnerability of public blockchains to DDos and other attacks have also remained a significant area of research. In particular, Sybil attacks have been addressed by frameworks like TrustChain, which provides Sybil-resistance via an algorithm called Netflow and ascertains the credibility of participating agents in an online transfer [13].

Property	Proof of Work	Proof of Stake	PBFT	Proof of Activity	Proof of Burn
Access Type	Public	Public	Permissioned	Permissioned	Permissioned
Adversary Power	<25% of computing power	<51% of stake	<33.3% of faulty replicas	<25% computing power	<51% of stake
Energy requirements	High	Medium	Low	High	High
Examples	Bitcoin	Peercoin	Hyperledger Fabric	Decred	Slimcoin

Fig.2. Table of comparison of consensus protocols.

Private and Federated blockchains, on the other hand, restrict access to a whitelist of users. This allows organizations to group individuals and implement granular access control. Private blockchain frameworks like Ripple and Hyperledger, follow a comparatively more centralized approach, as less members are involved in a transaction.

Hyperledger fabric is an open-source, enterprise-grade consortium blockchain introduced by IBM. It is a sub-project derived from the Hyperledger project founded by Linux Foundation[14]. Hyperledger Fabric doesn't utilize any cryptocurrency, in stark contrast to Bitcoins or Ethereum. Instead, chaincodes are used in Hyperledger for designing applications to interact with the network.

### III. METHODOLOGY

To provide a structured review of blockchain-based applications, the following research method was used:

#### 1. Locating literature

A systematic search was carried out in high impact and using the referenced works of these articles, additional searches were also conducted (Snowball Effect).

#### 2. Study Assessment and Selection

To assess the eligibility of literature, the title, abstract and introduction were analyzed. Articles deemed irrelevant or unsatisfactory were discarded. A full text review was done on the qualifying articles, the experimental methodology was studied, and the salient features were highlighted.

#### IV. APPLICATIONS

A lion's share of existing research classifies blockchain applications into financial and non-financial ones since cryptocurrencies constitute a considerable number of blockchain networks. In this paper, however, we use an application-oriented classification. In the following subsections, we review on the blockchain-enabled applications in various sectors:

##### 1. Healthcare

Healthcare is a data-intensive domain where a gigantic amount of data is created, shared and retrieved. When a patient undergoes a test, the scans, results, etc., are stored at the hospital, and might need to be accessed later by a medical practitioner or insurance company. Electronic Health Records fulfill the given purpose by storing data forming a holistic picture of the patients' health, including his medical history, lab tests and clinical trials, immunization dates, allergies and surgeries. EHRs also promote interoperability by facilitating the sharing of healthcare data among different groups.

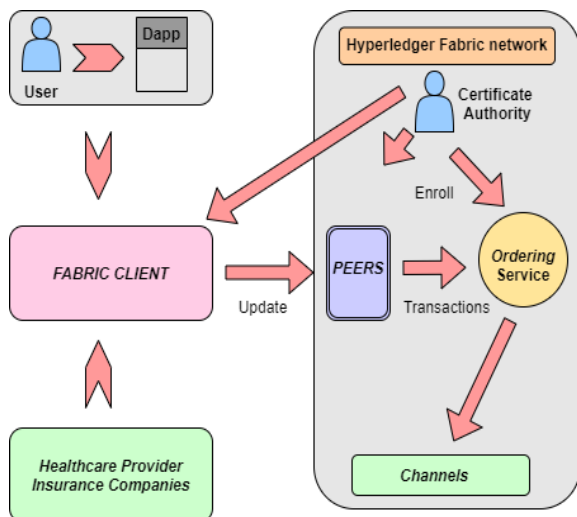


Fig.3. Representation of blockchain-based health network.

The diagram above shows a typical implementation of a blockchain based EHR record system. Users can register to the cloud to synchronize the data collected from their wearables, apps, etc. The health data is gleaned from a variety of devices, hence a Merkle-tree based approach is used to maintain integrity. The Merkle root is binded to a blockchain transaction and the data records are anchored

to Fabric channels. The user can now share this data with healthcare providers to seek their services, or with insurance companies to obtain a quote. Every such request is recorded as a block and validated by the other blocks in the chain.

Access control is implemented by utilizing a membership framework on Hyperledger Fabric. A designated Certificate Authority issues certificates to participants, and access control lists are configured for all subsequent operations. Channels are formed for each user, the data carrying a unique user ID, to maintain isolation between different users. Healthcare specialists and insurance agencies can also communicate with the server to request or update data, and shall be allowed into a channel as permitted by the user [15].

In multi-tier healthcare blockchain networks, miners are incentivized for utilizing their computational resources. Medrec, for examples, provides access to anonymized, cumulative medical data as mining rewards. Care providers are required to attach a bounty query to any transaction they send in the contract [16]. This bounty query can be programmed to return the average iron levels in blood tests performed by the provider for all patients in the past week. The provider can redeem this query when the block containing the transaction is mined. Blockchain based electronic health record networks require a huge degree of interoperability. There are numerous challenges in obtaining interoperability, as significant collaboration is required between participating institutions.

There has to be a uniform consensus between these parties about the patient matching algorithms and procedures, and the governance rules invoked while exchanging health records. Zhang introduces metrics for measuring the extent of interoperability in the decentralized apps or Dapps that interact with blockchain based cloud healthcare records in [17]. The security and privacy of healthcare networks is being constantly worked upon in various research endeavors. Badr presents a pseudonym based encryption with different authorities (PBE-DA) approach which removes the logic for key generation and authentication from IoT nodes to corresponding Gateways, thus removing computational burden from the IoT devices [18].

He elucidates on a tiered system of authorities for key generation to prevent overcrowding. Another constant challenge faced by blockchain-based healthcare networks is optimization of the patient data size on the ledger, as medical scans/images are often heavy files. Furthermore, regulations like GDPR for the EU shall soon allow patients the right to erase their healthcare records at their will, which goes against the very foundations of a blockchain network.

## 2. Supply Chain

Supply chains are turning into increasingly complex networks, spanned across different geographical locations. The advent of globalization, legislation and cultural behaviour makes it very difficult to maintain transparency and security in these intricate networks, leading to fraud, counterfeit, pilferage, and poor performance [19].

Traceability is perhaps the foremost concern while designing sustainable supply chain networks. Customers rely only on the vendor's credibility while purchasing a product, they don't have much information at their disposal about the real provenance of the food item they are purchasing. Such a system has seen misconduct scandals like the Salmonella outbreak due to Maradol papayas from Mexico, afflicting more than 200 peoples in the US. Although the origin of the papayas was traced to a farm in Mexico, it wasn't possible to trace where the shipments went, due to which a complete recall of shipped papayas couldn't be performed. These food crises necessitate better provenance records within the supply chain, as today's customers demand to know the exact nature of the product's origin. Being a decentralized, immutable ledger, blockchain is perfect for the purpose.

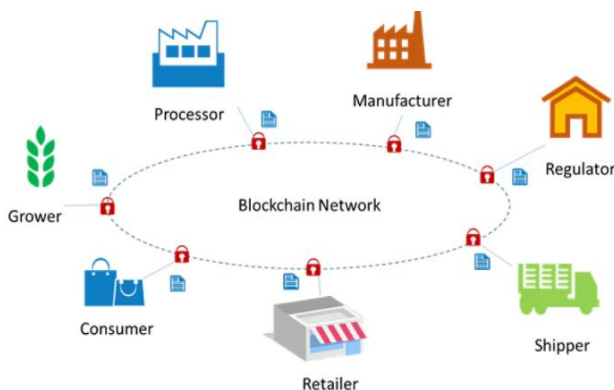


Fig.4. Blockchain-enabled supply chain network.

Certification mechanisms can be implemented in a similar way. After visiting factories for inspection, the certifier or standard organization can digitally sign the actors or products' profile. This framework guarantees transparency and prevents certificate fraud [20].

Counterfeiting is another major problem in supply chain that blockchain aims to solve. Since an astounding number of deaths occur every year in developing countries due to drug counterfeiting, many healthcare organizations emphasize on drug traceability. Once a drug is manufactured and sold to the vendor, the corresponding data is recorded on a permissioned blockchain. A similar process is followed by diamonds or high valued jewels, bags, etc. This makes it much more difficult to tamper with products or to add products of an illegal origin [21].

The merits of blockchain in bringing about traceability, are often reset by the complexity of the supply chain network. For example, a network consisting of a single source of a food item is relatively much simpler than a multinational conglomerate that gleans raw materials from various sources [22]. In the latter case, several actors contribute to the complexity of the blockchain network: raw material suppliers, distributors, retailers, and consumers.

An important issue to address for blockchain-based supply chain networks is that of the participant's privacy. A manufacturer or supplier in the supply chain may be the competitor of another and can hence gain unfair data from the blockchain. Moreover, current industries still use legacy hardware and it's a challenge to integrate blockchain technology into such antiquated systems.

## 3. Voting

Elections are the cornerstone of a democracy and it is highly imperative to ensure secure and non-fraudulent elections. Ballot-voting and Electronic Voting Machines (EVMs) are among the notable methods used in voting, however these methods do not allow the required transparency to voters. This leads to a remarkable decline in voter confidence [23]. E-voting has been widely adopted in several countries, like Estonia [24]. Since 2005, Estonia has been using their e-voting system, 'i-Voting', in governance, allowing voters to cast their vote from any computer connected to the internet.

During the voting period, the voter logs into the system using an identification number and casts his/her ballot. When the ballot reaches the National Electoral Commission for counting, this unique ID is removed to preserve anonymity. This is a simple, elegant method and has saved more than 11,000 working days for Estonia per voting cycle. Eventually, similar approaches were legalized in Switzerland, Norway, the Netherlands, etc [25]. These systems, are however, highly susceptible to DDos attacks and vulnerability breaches [26]. A major drawback of the online voting system is lack of transparency, as the voting database is controlled by a central authority, and the same can be tampered at will. The solution is to make the database public, a requirement where blockchain comes in. Blockchain technology allows each voters' vote to be recorded as a transaction that can be verified and added into the chain, and the resultant database can maintain an open audit trail [27].

A typical blockchain-based e-voting system looks like the diagram below. A permissioned blockchain is mostly used where each participating district can be represented by a district node. Trusted administrators may be enrolled to manage the life cycle of an election, assign nodes and register votes. In the pre-election period, voters are required to register, and the administrator pulls out a list

of eligible voters after identity verification. When the administrator creates an election, a smart contract is deployed onto the district node. When a voter casts her vote, the vote data is verified by a majority of district nodes and every validated vote is added to the blockchain. The transaction ID of this casted vote may be shared with voters, who can subsequently locate their transaction on the blockchain using a blockchain explorer. This ensures voter confidence by allowing voters to track where their vote went. Hjálmarsson implements this framework by using smart contracts and the Proof of Authority consensus mechanism on Go-Ethereum [28].

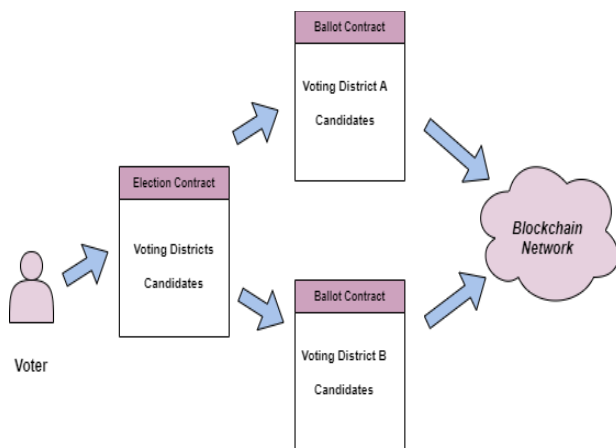


Fig.5. Blockchain-based voting system.

Privacy concerns of blockchain-based voting solutions are a constant area of research. Wang describes the process of voting as a five-stage process (Setup, Register, Vote, Valid, Append, Publish, VerifyVote). His work using the DPOS consensus mechanism to increase the transaction speed for public blockchains [29]. He propounds the use of un-linkable signatures and ring signatures, to preserve anonymity of both the sender and receiver of the transaction. Another mechanism to improve privacy by using homomorphic encryption techniques is BroncoVote [30]. Bartolucci's work focuses on efficient broadcast and counting of votes while protecting voters' privacy and anonymity. The work uses the SHARVOT protocol, a secret share-based voting system, and Shamir's Secret sharing to allow on-chain vote submission and candidate victory [31].

#### 4. Industry

Many smart factories utilize a cloud-based manufacturing architecture, in which users can access the shared pool of manufacturing resources on demand, and resource management is carried out with little third-party interaction. In this architecture, however, if the central node is damaged, all services are suspended. Using a decentralized blockchain-based system instead of a centralized one resolves the issue of availability. The term 'Industry 4.0' was coined by Germans in 2011, to describe highly automated, dynamic production

networks driven by Industrial IoT, human-machine interaction, blockchain, artificial intelligence and open source software [80]. The boom of Industry 4.0 led to the development of Industrial IoT, which integrates wireless sensor networks and communication protocols to facilitate intelligent industry operations in monitoring, analysis, and management. Industrial IoT consists of three layers: physical, communication and application. The physical layer consists of sensors/actuators, the communication layer is built of WSNs/5G and connects the devices in the physical layer. IIoT has crept its way into several industries including manufacturing, power grids, agriculture, healthcare, etc., and in each, blockchain serves a unique purpose.

In the power industry for instance, blockchain facilitates global energy transformation by reducing transaction costs and allowing the power grid to operate in a more efficient manner. It achieves this by enabling smart contracts and pushing buyers to become 'prosumers' (ones who consume as well as produce) by empowering them to utilize their power by safe record of data. Zhong proposes a reserve-sharing mechanism between interconnected power grids using the Shapley value method to calculate the value of the shared reserve capacity. Probabilistic forecasting is used to depict wind and solar generation, and unserved demand and reserve shortage are factored in the system operation cost [81]. Qin introduces a point-to-point encryption method for power system communication data based on blockchain technology. His model shows that the larger the amount of encrypted data, the more secure and stable the communication is [82].

In the manufacturing sector, factories often publish manuals of their products, which are then distributed amongst other departments. Blockchain can store these technical publications, saving on tons of paperwork. In the automobile manufacturing industry, for example, tracking of spare parts is vital, and blockchain resolves this issue by updating relevant information of the spare parts on the ledger that is available to all parties involved. Kim describes a firmware management architecture using blockchain and Interplanetary file System (IPFS).

IPFS is a peer-to-peer distribution system like BitTorrent, that uses version management through Merkle DAG and supports self-certified names. IoT devices are provided with firmware information and updated through blockchain networks to ensure file integrity [83]. Huang proposes B-IoT, a blockchain based IoT system that uses a credit-based PoW consensus mechanism that enhances security and improves transaction efficiency. The system is based on a directed acyclic graph (DAG) blockchain, which is reportedly more efficient than the Nakamoto-styled blockchain. Blockchain-based approaches to industrial are fraught with several challenges. In the power industry for instance, energy consumptions for

blockchain-based transactions are exorbitant, affecting the scalability of such networks. In the agricultural and manufacturing sectors, blockchain-based deployments majorly use data collected by IoT sensors. In addition to paying for subscribing to blockchain, parties have to pay for IoT deployments as well, which deters them for choosing a complex blockchain deployment unless the return on investment is high.

## V. CONCLUSION

In this paper, we presented a brief introduction of blockchain technology, discussed its architecture its primary features. We surveyed the evolution of research and the latest research work done on blockchain consensus, mining, access, and the application of blockchain in various spheres. We followed an application-oriented approach while detailing on the network structure applied to healthcare, supply chain, industry, and governance, talked about their challenges and the prevailing research that seek to solve these challenges. Based on a deep scrutiny of said research, we conclude that blockchain deployments shall be more interoperable and customizable if further work is directed to address the challenges of data protection, privacy, adoption cost, scalability, and ease of government regulations.

## ACKNOWLEDGMENT

We would like to thank the Cisco community for introducing us to blockchain and consequently allowing us to build our concepts in the same via conferences and events. This is an independent research stud and has been carried out sans any grants/sponsorship.

## REFERENCES

- [1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System
- [2] Mills, David C. and Wang, Kathy and Malone, Brendan and Ravi, Anjana and Marquardt, Jeffrey and Badev, Anton I. and Brezinski, Timothy and Fahy, Linda and Liao, Kimberley and Kargenian, Vanessa and Ellithorpe, Max and Ng, Wendy and Baird, Maria, Distributed Ledger Technology in Payments, Clearing, and Settlement (2016-12). FEDS Working Paper No. 2016-095
- [3] Szydlo M. (2004) Merkle Tree Traversal in Log Space and Time. In: Cachin C., Camenisch J.L. (eds) Advances in Cryptology - EUROCRYPT 2004. EUROCRYPT 2004. Lecture Notes in Computer Science, vol 3027. Springer, Berlin, Heidelberg. [https://doi.org/10.1007/978-3-540-24676-3\\_32](https://doi.org/10.1007/978-3-540-24676-3_32)
- [4] Salomaa, A. (2013). Public-Key Cryptography. Springer Verlag-Berlin
- [5] Valsorda, F. (2014). Exploiting ECDSA failures in the bitcoin blockchain. Hack In The Box (HITB)
- [6] Li, C., Li, P., Zhou, D., Xu, W., Long, F., & Yao, A. (2018). Scaling nakamoto consensus to thousands of transactions per second. arXiv preprint arXiv:1805.03870
- [7] Qin, R., Yuan, Y., & Wang, F. Y. (2018). Research on the selection strategies of blockchain mining pools. *IEEE Transactions on Computational Social Systems*, 5(3), 748-757.
- [8] Qin, R., Yuan, Y., Wang, S., & Wang, F. Y. (2018, June). Economic issues in bitcoin mining and blockchain research. In 2018 IEEE Intelligent Vehicles Symposium (IV) (pp. 268-273). IEEE
- [9] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151(2014), 1-32
- [10] Hirai, Y. (2017, April). Defining the ethereum virtual machine for interactive theorem provers. In International Conference on Financial Cryptography and Data Security (pp. 520-535). Springer, Cham
- [11] Atzei, N., Bartoletti, M., & Cimoli, T. (2016). A survey of attacks on Ethereum smart contracts. *IACR Cryptol. ePrint Arch.*, 2016, 1007
- [12] Yuan, R., Xia, Y. B., Chen, H. B., Zang, B. Y., & Xie, J. (2018). Shadoweth: Private smart contract on public blockchain. *Journal of Computer Science and Technology*, 33(3), 542-556
- [13] Otte, P., de Vos, M., & Pouwelse, J. (2020). TrustChain: A Sybil-resistant scalable blockchain. *Future Generation Computer Systems*, 107, 770-780
- [14] Cachin, C. (2016, July). Architecture of the hyperledger blockchain fabric. In Workshop on distributed cryptocurrencies and consensus ledgers (Vol. 310, No. 4)
- [15] Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017, October). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC) (pp. 1-5). IEEE.
- [16] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data. In Proceedings of IEEE open & big data conference (Vol. 13, p. 13).
- [17] Zhang, P., Walker, M. A., White, J., Schmidt, D. C., & Lenz, G. (2017, October). Metrics for assessing blockchain-based healthcare decentralized apps. In 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 1-4). IEEE
- [18] Badr, S., Gomaa, I., & Abd-Elrahman, E. (2018). Multi-tier blockchain framework for IoT-EHRs systems. *Procedia Computer Science*, 141, 159-166
- [19] Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, 57(7), 2117-2135

- [20] Abeyratne, S. A., & Monfared, R. P. (2016). Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology*, 5(9), 1-10
- [21] Jamil, F., Hang, L., Kim, K., & Kim, D. (2019). A novel medical blockchain model for drug supply chain integrity management in a smart hospital. *Electronics*, 8(5), 505
- [22] Francisco, K., & Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. *Logistics*, 2(1), 2
- [23] Moura, T., & Gomes, A. (2017, June). Blockchain voting and its effects on election transparency and voter confidence. In *Proceedings of the 18th annual international conference on digital government research* (pp. 574-575)
- [24] Braun Binder, N., Krimmer, R., Wenda, G., & Fischer, D. H. (2019). *International Standards and ICT Projects in Public Administration: Introducing Electronic Voting in Norway, Estonia and Switzerland Compared*. *Halduskultuur*, 19(2), 8-22
- [25] Goede, M. (2019). E-Estonia: The e-government cases of Estonia, Singapore, and Curaçao. *Archives of Business Research*, 7(2), 225-227
- [26] Ayed, A. B. (2017). A conceptual secure blockchain-based electronic voting system. *International Journal of Network Security & Its Applications*, 9(3), 01-09
- [27] Hanifatunnisa, R., & Rahardjo, B. (2017, October). Blockchain based e-voting recording system design. In *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)* (pp. 1-6). IEEE.
- [28] Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G. (2018, July). Blockchain-based e-voting system. In *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)* (pp. 983-986). IEEE
- [29] Wang, B., Sun, J., He, Y., Pang, D., & Lu, N. (2018). Large-scale election based on blockchain. *Procedia Computer Science*, 129, 234-237
- [30] Dagher, G. G., Marella, P. B., Milojkovic, M., & Mohler, J. (2018). Broncovote: Secure voting system using ethereum's blockchain
- [31] Bartolucci, S., Bernat, P., & Joseph, D. (2018, May). SHARVOT: secret SHARe-based VOTing on the blockchain. In *Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain* (pp. 30-34)
- [32] Alladi, T., Chamola, V., Parizi, R. M., & Choo, K. K. R. (2019). Blockchain applications for industry 4.0 and industrial IoT: A review. *IEEE Access*, 7, 176935-176951
- [33] Mal, Z., Zhong, H., Wang, J., Du, E., & Xia, Q. (2018, June). The Reserve Sharing Mechanism Among Interconnected Power Grids Based on Block Chain. In *2018 15th International Conference on the European Energy Market (EEM)* (pp. 1-5). IEEE
- [34] Qin, H., Li, Z., Hu, P., Zhang, Y., & Dai, Y. (2019, October). Research on Point-To-Point Encryption Method of Power System Communication Data Based on Block Chain Technology. In *2019 12th International Conference on Intelligent Computation Technology and Automation (ICICTA)* (pp. 328-332). IEEE
- [35] Son, M., & Kim, H. (2019, February). Blockchain-based secure firmware management system in IoT environment. In *2019 21st International Conference on Advanced Communication Technology (ICACT)* (pp. 142-146). IEEE

### Author Profile



#### Basundhara Chakrabarty

Basundhara Chakrabarty is a Network Consulting Engineer at Cisco Systems, Bangalore, India. She has over two years of experience in the field of network security and works in close closely with Cisco's clients in the design, configuration and troubleshooting of network security deployments. She has presented her previous work in the field of network security in the International Conference on Computing Communication and Networking Technologies, 2020 (IIT Kharagpur), and International Virtual Conference on Industry 4.0, 2020 (VIT Chennai). She received her undergraduate BTech in Electronics and Communication Engineering from VIT Vellore in 2018.



#### Harish Krishnamoorthy

Harish Krishnamoorthy is a Network Consulting Engineer in the Service Provider team at Cisco Systems, Bangalore, India. He has been engaged in multiple projects involving network security, and has presented his previous work in the International Conference on Computing Communication and Networking Technologies, 2020 (IIT Kharagpur), and International Virtual Conference on Industry 4.0, 2020 (VIT Chennai). He received his undergraduate BTech in Electronics and Communication Engineering from VIT Vellore in 2019.



#### Karan Shahani

Karan Shahani is a Deputy Category Manager at BulkMRO and is involved in managing supply chain

networks for Fortune 500 companies. He has received his undergraduate degree in Mechanical Engineering from VIT University Vellore in 2018. Karan is an enthusiast in blockchain-powered supply chain frameworks and has done been involved in several such projects.