Imminent Threat with Authentication Methods for AI Data Using Blockchain Security

Vijaya Krishna Sonthi, S. Nagarajan, M. V. B. Murali Krishna M, Koppisetti Giridhar, V. Lakshmi Lalitha, and V. Murali Mohan

Abstract Since the announcement of Satoshi Nakamoto's Bitcoin policy document in 2008, blockchain has become one of the most widely discussed techniques for implementing safety storage and processing through decentralized, approved, peer-to-peer networks. This study described peer-reviewed literature, which uses cryptocurrency for cybersecurity purposes and offers a comprehensive overview of the most commonly used application areas of blockchains. This main forward-looking study further illuminates the possible directions for science, education, and practice on blockchain and cyberprotection, such as IoT blockchain security, as well as the need for data analysis of blockchain safe data. Analyses of this data increase the value of the latest machine learning (ML) technologies. There is a logical quantity of data required by ML for correct decisions. Data reliability and sharing in ML are very critical for improving the accuracy of performance. The combination of these two technologies will yield extremely accurate results (ML and BT). In this paper, we present a detailed review of ML adoption to make mobile platforms based on BT more resilient against attacks. Examples of such support systems as support vector machines (SVM) and bagging and deep learning (DL) algorithms can be used to evaluate attacks on a blockchain network, including convolutional neural network (CNN) and long short-term memory (LSTM). Actually, various traditional ML techniques are available. Furthermore, we include the use of both technologies in a variety of smart applications, including UAV, Smart Grid (SG), healthcare, and

V. K. Sonthi (✉) · V. L. Lalitha · V. M. Mohan
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India
e-mail: svijayakrishna@kluniversity.in; vlakshmilalitha@kluniversity.in; muralimohan310@kluniversity.in

S. Nagarajan
Department of CSE, FEAT, Annamalai University, Chidambaram, Tamil Nadu, India

M. V. B. Murali Krishna M · K. Giridhar
Department of Computer Science and Engineering, Aditya College of Engineering, Surampalem, Andhra Pradesh, India

K. M. Baalamurugan et al. (eds.), *Blockchain Security in Cloud Computing*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-70501-5_14

smart towns and cities. Future technological issues and concerns are also debated. Finally, we discuss the study model with a thesis.

Keywords Blockchain · Machine learning · Smart Grid · Data security and privacy · Data analytics · Smart applications

1 Introduction

Blockchain technology, as a distributed ledger of physical and financial resources, allows for trusted payments among unauthenticated network participants. Different blockchain networks, such as Ethereum and Hyperledger Fabric, have emerged through public and private availability outside traditional digital currencies and electronic token systems since the launch of the first Bitcoin blockchain. Multiple industries trying to adapt the core principles to existing processes have recognized the importance of a trustless, decentralized ledger which really carries traditional non-repudiation. For several business fields, such as finance, logistics, the pharmaceutical industry, smart contracts, and perhaps, most notably, cybersecurity, the specific properties of blockchain technology make its use an attractive concept in the context of this paper. The drastic shifts in production and distribution, including globalization and outsourcing, are the result of the higher degree of sophistication. As a consequence, various parts of global supply chains are operated by independent companies. By using local information such as cost structures, profit margins, and estimates, each organization in the supply chain establishes operational and strategic targets to optimize its very own profit. While advances in information technology allow businesses to gather, store, and exchange information, because of competing incentives, companies may be reluctant to do so. Trying to align rewards increases the profits of companies and sustains any use of information technology. The motivation concerns with a large risk imbalance, such as capability risk, need to be fixed. The effect of resource risk is more serious for a decentralized supply chain than for a vertically integrated supply chain because of the imbalance. We recommend a blockchain-based approach to resolve the double-marginalization issue in order to solve these problems [1].

2 Prioritize Vulnerabilities: From Identification

Discounting the value of incident prevention is standard. The sheer amount of vulnerabilities in their own organizations can be underestimated by executives. Additional risks that may emerge from acquisitions of many other companies may not be considered. These individuals could get some sobering facts, especially in light of market enforcement regulations, such as with the General Data Protection

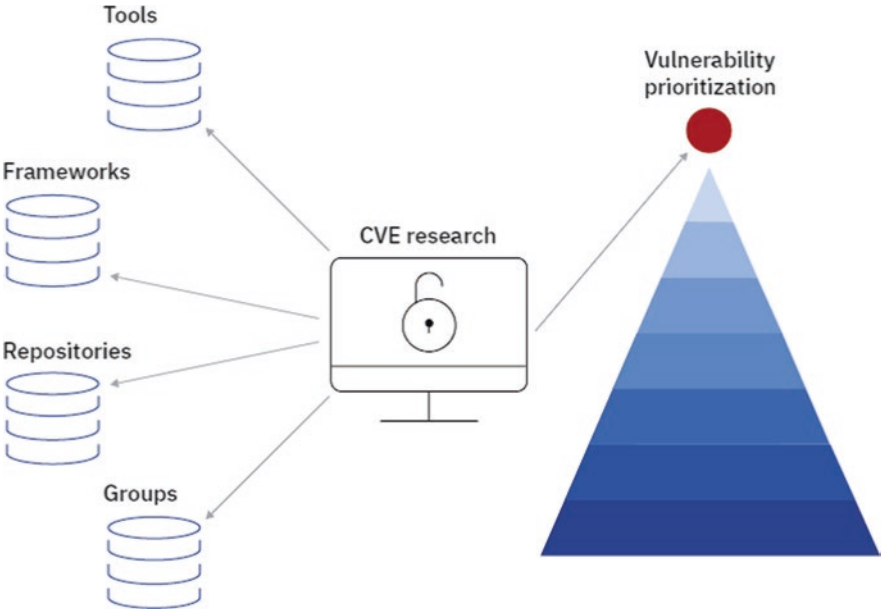


Fig. 1 An armed intruder insecurity rating approach is intended to offer a simple impression of containment

Regulation (GDPR). Personally curated data can also easily become outdated. It could take 3–5 full working days to complete the development of a database to rank vulnerabilities as shown in Fig. 1. New bugs are likely to appear by the time your spreadsheet is completed and may be ignored. Other factor to consider is indeed a lack of knowledge. Sometimes, business leaders feel that they are quick to fix when bugs are identified. As such, instead of seasoned data scientists, workers who lack updates and patch skills and training may obtain the assignments. When they are discovered, these novice workers are also not prepared to repair bugs [2].

Despite these conditions, several companies are presented with a long list of vulnerabilities that are not properly addressed. Organizations need to adopt a risk management program to further strengthen their defense capabilities [3, 4].

2.1 Identifying Flaws

Focusing on improving the most important vulnerabilities based on property value and cyberwarfare

Fixing after a manageable mitigation phase

The most risk-elevating vulnerabilities

The Popular Vulnerability Point System annotates each CVE identification using the CVSS. Based on an average, this economy standard is being used internationally to rate the seriousness and risk with CVE. A quantitative radiological rating is generated by the CVSS depending on multiple factors, along with the following:

1. Form of assault
2. Degree of access required
3. Sophistication levels [5]

3 Vulnerabilities and the Management of Remediation

Where a third-party remediation manager uses the "work increase" of hourly staff, the employees may use customer-provided or purchased vulnerability scanning from a supplier. The remedial service provider then communicates with the scanners used by ticketing or table customers. It is not likely that this strategy would yield results, as scanners might not be able to detect "not-yet-known" vulnerabilities that are not designed to defend against hacker thought and motives [6].

Companies must view vulnerability management as a multistage process, not a single process.

3.1 Scanning Efforts

A successful programmer, focused on a sheer number of existing and emerging vulnerabilities, will focus the institution's attention on the most high-risk vulnerabilities continuously.

One significant issue in remediating vulnerability is that corporations typically need not invest time and money on manufacturing [7].

Attackers could only initiate attacks on the infrastructure in a bitcoin system if an attacker controls 51% or more of the nodes. Because most nodes are run by genuine network nodes, attacks can be conducted very differently, and the block information in the blockchain is therefore credible.

Participants in the Bitcoin system pledge their privacy. By purchasing the longest working load-proof chain, participants can willfully leave or reenter the Bitcoin scheme to access transaction details while leaving the system [8].

4 Attack Model

4.1 Semi-Honest Model

Half-honest respondents in this model are also known as passive attackers. A semi-honest partner shall not withdraw from the deal nor interferes with the outcome of the protocol, in full compliance with the implementation of the contract during intra-computation. He or she is able to maintain.

Some intermediate outcomes in implementing the agreement attempt, through these intermediate outcomes, to evaluate and extract input data from other participants [9].

4.2 Malicious Model

Malicious assailants are also active model attackers. A malicious attacker can not obey the procedure of the protocol, interrupt the protocol operations, and concur with intermediate results or amend the contract with other parties as shown in Fig. 2.

5 Encryption of Authentication and Connection

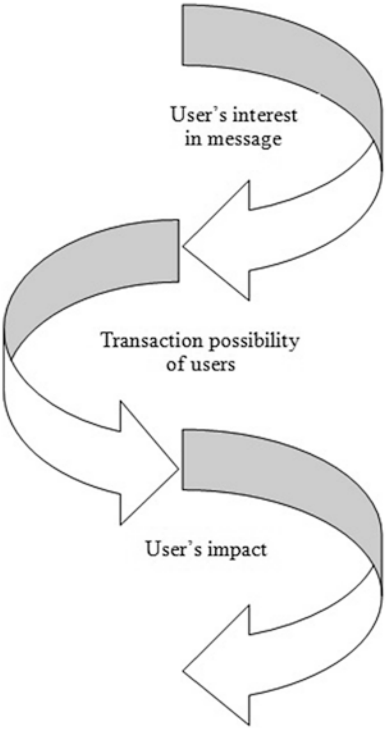
CSE is focused on the intimacy of the user. If two people have much more mutual friends in society, there is a more intimate contact for both users. Thus, we measure intimacy by measuring two follow-up users. However, in the social network world, to prevent other users from miscellaneously entering user information to identify social circles, a user on two sides may confirm their identification before the communication process. In this sense, a user would have to know the personal information of other users. Consequently, we must authenticate the user's identity in case a malicious user gets the user connection inappropriate and infer the user's wishes and desires until a client receives details from other user relationship. Encryption of authentication is shown in Fig. 3 [10].

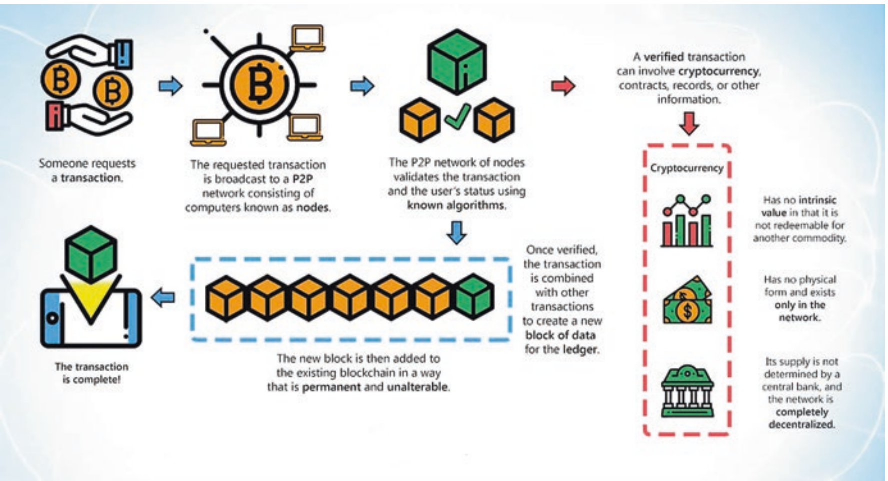
5.1 Hashing Blockchain

Since this is the first block in a sequence, it does not contain the pointer. At the same time, there is potential for a final block to exist in the blockchain database with no pointer.

Blockchain infrastructure can be useful for companies and businesses**.**

Fig. 2 Models for malicious attack




Someone requests a transaction.

The requested transaction is broadcast to a P2P network consisting of computers known as nodes.

The P2P network of nodes validates the transaction and the user's status using known algorithms.

A verified transaction can involve cryptocurrency, contracts, records, or other information.

Cryptocurrency

Has no intrinsic value in that it is not redeemable for another commodity.

Has no physical form and exists only in the network.

Its supply is not determined by a central bank, and the network is completely decentralized.

Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.

The new block is then added to the existing blockchain in a way that is permanent and unalterable.

The transaction is complete!

Fig. 3 Encryption of authentication

Reducing the cost of storing data can also be achieved by keeping data secure from cyber criminals and corrupt intentions [11].

History of Data: Inside a blockchain structure, you can check the history of any transaction at any time. A centralized database is more like a snapshot of information at a single point in time.

Data is maintained and controlled by the blockchain. Data is difficult to tamper with. Verification of records takes time since it happens in each individual network rather than in a compound mechanism (Fig. 3). That means we compromise output speed but instead have high protection and validity [12].

Blockchain systems fall into three groups.

5.2 Blockchain Technology Architecture: Public

A public blockchain design ensures data and access is open to anyone who is willing to participate (e.g., Bitcoin, Ethereum, and Litecoin blockchain systems) [13, 14].

5.3 Blockchain Architecture

In private device architecture, the user is only approved by a certain entity or has been given permission by a particular user.

5.4 Consortium Architecture

The blockchain can involve several organizations. In a consortium, procedures are regulated by the preliminary allocated users (Table 1).

Table 1 A detailed comparison among these three blockchain systems

Property	Public blockchain	Consortium blockchain	Private blockchain
Consensus determination	All miners	Designated set of nodes	Within one organization
Read permission	Public	Public or restricted	Public or restricted
Immutability level	Almost impossible to tamper	Could be tampered	Could be tampered
Efficiency (use of resources)	Short	High	High
Centralization	No	Partial	Yes
Consensus process	Agreementless	Needs agreement	Needs agreement

Each block stores a combination of digital currencies and many records. For instance, the block keeps records of the transferor, recipients, and amount of money in Bitcoin blockchain.

The same way, a hash is a unique identifier (long record consisting of some digits and letters). The algorithm generates each block hash (SHA-256). This then allows simpler recognition of each block in a blockchain structure. If a block is mined, a hash is automatically formed, while any changes made in a block result in updating the hash. Hashes help evaluate any changes made to a block [15].

This is the final element of the preceding block hash. This provides protection and helps to deter security breaches. In this way, 45 and 46 are related. The very first block is unique because all other blocks originate from this block of origin.

Any corrupt attempts will guarantee that the blocks are going to pass. Many of the next blocks contain inaccurate data and do not guarantee the stability of the entire blockchain package.

On the other hand, with the help of computer processors, it may be possible to modify all the blocks at once. There is a solution called concrete proof that addresses this concern. This makes it possible for a customer to accelerate the pace of the construction of new buildings and apartments. It takes about 10 minutes to produce proof of work that is needed to mine new coins in the BTC blockchain. Miners perform this role of computation. Miners get to retain transaction fees as a bonus of mining [16, 17].

A copy of the entire blockchain network is received by each new user (node) joining the Ethereum network. This dataset has been sent to increase node inside the blockchain system after each block is created. Then, each node tests the information and finds that it is valid. If all goes well, each block is connected to the local blockchain.

A unanimous choice is reached by all the nodes in the blockchain system. When using the blockchain system, participation at all levels of the system is guaranteed due to the fact that people willingly abide by its laws.

Blockchain could solve the data protection issues on AI networks in modern computing world (e.g., IoT). AI and its implementations have become significant instruments for monitoring and processing [18, 19].

In order to ensure sufficient analytics in resolving security issues, the gathered data must be accounted for. Artificial intelligence (AI) is efficient and can be used in distributed computing if data entered into it is not manipulated or truthful.

Third-party blockchain, with contradicting input, can be used in different areas of cyberspace. Therefore, blockchain may have a great impact to decentralized systems.

Ensure authenticity, accuracy, and credibility of details. If information has credibility and is accurate, AI can do better. The possible course of study for this is to study the blockchain.

Businesses should ensure data security under B2B and M2M style setting.

5.5 Blockchain Development of Networks

When an individual, or a few, decide to embrace a blockchain technology, a network is built. This can be perceived as high-tech culture within these enterprises.

To give a clearer picture, let's use diamonds as an example. There are risks and difficulties involved with processing and selling the diamonds. Consumers would like to be sure they are acquiring diamonds from reputable and responsible businesses. Government agencies need the taxes to be collected and controlled. That framework of the blockchain will eradicate these potential risks.

In this network, the parties concerned include:

(a) Diamond manufacturers
(b) Institutions of the government
(c) Transporters with gems
(d) The sellers of diamonds

The same entities are assembled by blockchain solutions into a peer-to-peer network, which help to remove all the risks that had been listed and help to create a transparent system. All will be able to obtain the decentralized data of an immutable ledger and to track the flow of diamond from production to the final customer. In the public blockchain, all operations such as diamond mining, refining, and delivery are organized in sequence.

Under these blockchain networks, everybody has a complete copy (called peers). Also, there is ordering service to outline stuff that happened at the same time. Both those involved in the process have an oversight of the transactions (Fig. 4). There is

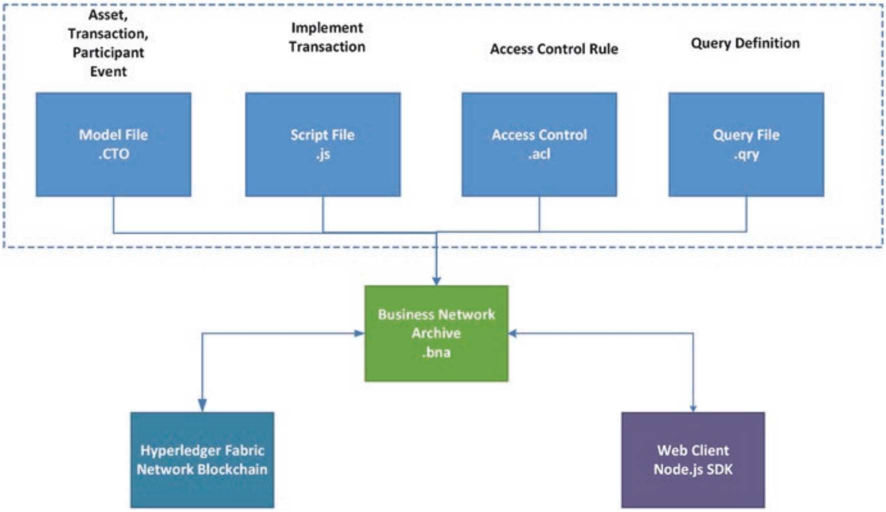


Fig. 4 Hyperledger composer

a member management system (MMS) for multiple users, which allows access to unique users within the network.

All transactions go through the general ledger during this phase (e.g., data with diamond photos, place of extraction, color, serial number, place where it was cut, purified, sold, etc.). This knowledge is reliable and true [20].

5.6 Key Characteristics of Blockchain Architecture

The blockchain architecture has many benefits for businesses. There are some attributes here.

Blockchain transactions are encrypted and checked because of their complex mathematical computations.

Immutability is permanent because records made cannot be altered or erased.

Provenance means that transactions can be trusted because they can be monitored online for a long time.

The entire various places are accessible by each member of the decentralized system. The consensus algorithm promotes network security.

Each user in the blockchain system is a generated address, not really a user identity. This will protect the privacy of users in a shared blockchain system.

Transparency cannot be manipulated by human. It is unlikely to happen because it takes too much computing power to rewrite the entire blockchain network.

Depending on how it is accessed and how the access permissions are issued, blockchain can be categorized into public, permissioned, and consortium blockchain [21, 22] (Fig. 5).

5.7 Key Features of a Blockchain Network

5.7.1 Public Blockchain

A public blockchain is a blockchain that anyone can access (often, anonymously). There are no limits on who can enter and, whether the transactions are mathematically legitimate, what transaction they can publish. Even though participants can secretly join the network (revealing only).

Any transaction they make is accessible to all (the public), which can be carefully analyzed in order to identify the users. The most popular example of decentralized blockchains is Bitcoin [3].

In such a network, there is usually an opportunity for participants to adopt an intensive consensus protocol for a computing resource (e.g., validate a block using proof of work).

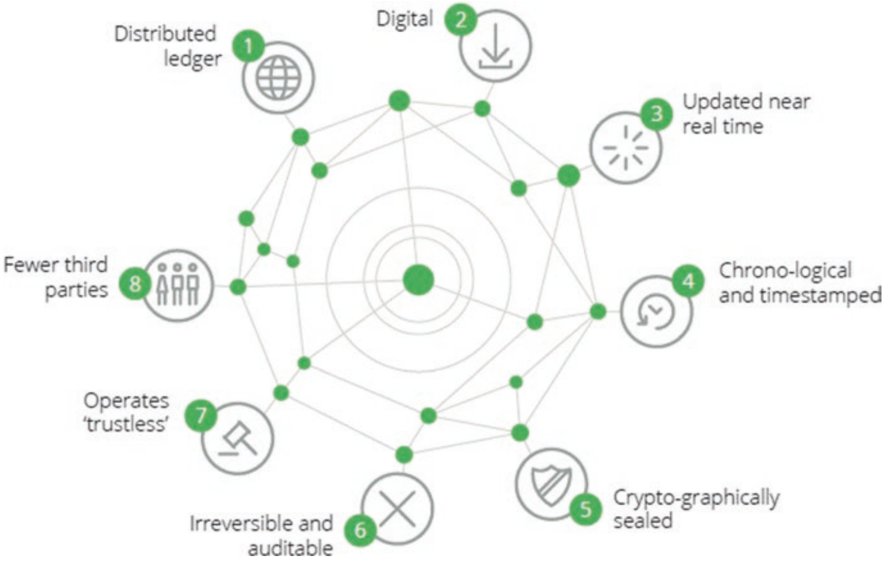


Fig. 5 Distributed domain feature of blockchain

5.7.2 Permissioned Blockchain

A permissioned blockchain is one in which the company's contact is limited to users who have access rights given by the owner of the network. Non-anonymous validation of blocks or contact with the blockchain is not allowed on such a network. To control access to such a network, a certificate authority (CA) is usually used. A platform running its network as an approved network by blockchain would decide who can be validators and what rights are provided to the users. One of the most famous examples of a permissioned blockchain system is Hyperledger Fabric [23–[25].

5.7.3 Consortium Blockchain

It is conceivable that the consortium blockchain (centralized) will be maintained by a single (originating) entity and offers predefined access rights to interacting parties. Usually, such a network suits government or regulatory bodies that have legal competence over other members.

In several cases, machine learning systems are used and have received great success, as shown below.

These types of patterns can be discovered by reviewing vast databases, such as stored medical records or credit history information. Machine learning techniques are used in places where we cannot get good results with conventional (deterministic) algorithms.

Several subjects require adaptable growth, for example, controlling manufacturing processes as per customer demand and adapting to readers' varied reading interests:

(i) In numerical data, supervised algorithms use statistical models in order to correctly identify the result. Regression and decision trees are the most commonly used algorithms in artificial intelligence.

(ii) ML does not contain label data. Here, the data points are grouped according to their statistical proximity or distance. K stands for algorithms for clustering and association rules. Supervised ML is a form of semi-supervised learning.

(iii) This project requires integrating both supervised and unsupervised machine learning. Unsupervised learning is implemented after which the most likely decisions are expected. It affects the data that lead [26–[28].

The model is then used as training data when constructing a new model.

Considering that more than half of the recorded cybersecurity blockchain applications were dealing with IoT devices, opportunities to optimize IoT security are obvious. There is a connection between IoT, military, and healthcare in Singapore (Fig. 6). The announcements of security breaches and attacks on IoT will create the market for approaches to IoT security threats.

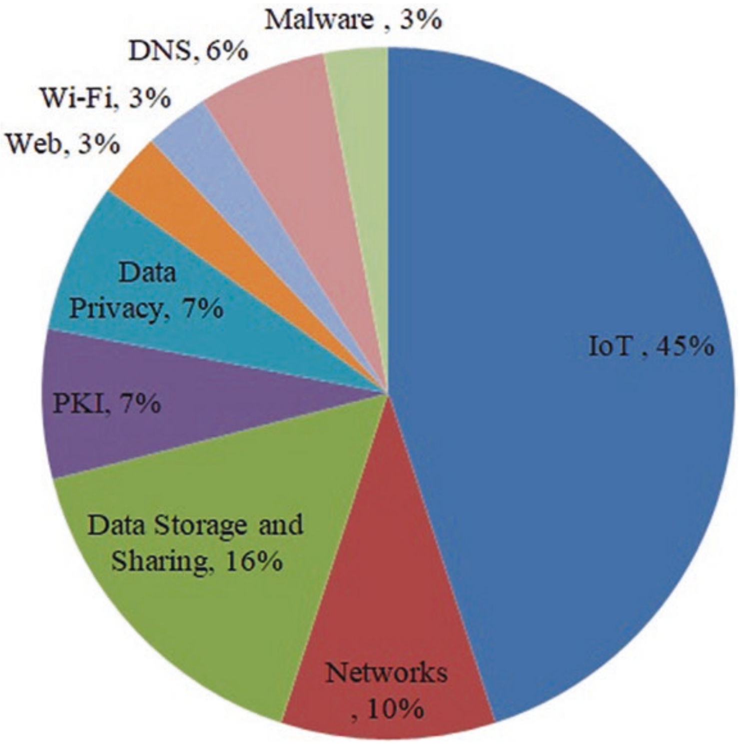


Fig. 6 Chart of themes of primary studies

Blockchain could solve the data protection issues on AI networks in modern computing world (e.g., IoT). Artificial intelligence (AI) and its applications are used in order to apply the security technique. The problem with big data is that if an AI's data is manipulated or misused by malicious third party, misleading analysis is the outcome. Blockchain can be used in different areas of cyberspace. Thanks to its decentralized and immutable features, blockchain guarantees data consistency, reliability, and honesty as well as reduces possibility of financial exploitation. If information has credibility and is accurate, AI can do better. Some blockchain research could include the implementation of AI data security in B2B (business-to-business) and M2M (machine-to-machine) environments [29, 30].

There are also questions about the validation and tamper resistance of main chains. We expect a distributed multi-blockchain infrastructure in the foreseeable future (Fig. 7).

This research sheds light on possibilities for research in cybersecurity other than IoT to be conducted. With the rising amount of users in the network using HTTPS encryption, cryptography needs to be safe and sound to ensure continued secure communications. Prospective research goal 1 in blockchain applications is to investigate the "Internet of Things" protection using Blockchain. Such data is unknown and hard to calculate for the purpose of this article. Future studies will include an in-depth evaluation of wireless network security, power consumption, and latency [31]–[34].

IoT (Internet of Things) networks and data packets would need to be monitored and handled in order to enhance processes.

You can seek ways to overcome by exploring ideas and solutions using Ethereum and smart contracts. Researchers will want to explore how disruptive cybertechnology can be used in combination with blockchains.

Conclusion leads that, in the future, researchers could concentrate on developing decentralized applications and frameworks to protect the blockchain. However, decentralized cryptocurrencies such as Bitcoin have longer and more reliable

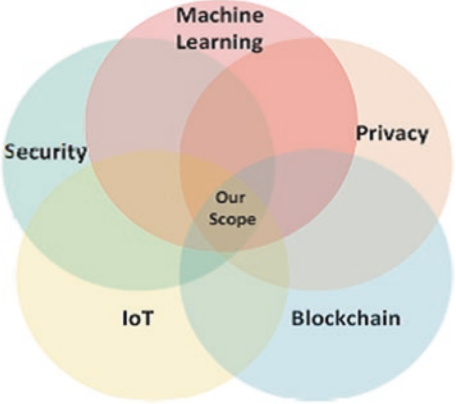


Fig. 7 Distribution status for the latest technology

blockchain (than decentralized cryptocurrencies such as Bitcoin) (e.g., ransomware and terrorism financing).

It is noted that permissionless blockchain systems typically take minutes to reach consensus, such as Bitcoin and Ethereum. For applications that are latency-sensitive including the Internet of Battlefield Things (IoBT), latency sensitivity may not be sufficient. Therefore, in combination with hardware-based approaches that have minimum latency, a future development objective is to design blockchain-based solutions [35].

Data has a significant role in training an ML model. We can use historical data of patients to predict how someone will respond with any new disease or medication. However, patients are hesitant to reveal their test results because of privacy concerns. Researches have worked to fix these issues. The researchers have developed a service called eDiag in order to collect user information and store them in a safe and supervised process. The previous study used quantitative reasoning methods that were not appropriate for online diagnosis. It was discovered that they achieved 94% accuracy without compromising data privacy. Likewise, the study examined the privacy issues as a question of learning privacy and model privacy, respectively (Tables 1 and 2).

Table 2 Objectives of the survey on data privacy

Objectives of survey	Merits	Demerits
To present the use of blockchain in intrusion detection	Scope of application of blockchain was discussed	Discusses only data sharing and trust management issues of collaborative intrusion detection
To discuss various security and privacy issues in Bitcoin	A comprehensive review of possible attacks on Bitcoin and provided countermeasures	Blockchain issues are not high-lighted
Survey on ML security solutions for Bitcoin	In-depth and wide classification of major threats and extensive explanation of the role of ML	Other applications of blockchain are missing
To study ML techniques for malware analysis	Time and space complexity for various methodologies has been described in detail	Lacks discussion on the uses of these techniques in a blockchain environment
Discuss applications, platforms, and protocols in blockchain specifically for AI	The decentralization feature of blockchain is explained with a specific view of AI	Discussion on privacy is not covered in detail
Review blockchain-based applications and identify open issues	Prerequisites for blockchain applications are thoroughly discussed	Focused on applications, not the open issues
To survey how ML can be used in blockchain-based smart applications	Discusses architecture and technology at a fundamental level and bridges the gap between the two technologies	–

6 Existing Solutions Using Blockchain Technology

The blockchain (BC) is a stable, fault-tolerant, open, verifiable, and auditable mesh network. Decentralized, P2P, open, confidence, and eternal are the commonly used keywords to explain BC benefits. These characteristics make a BC more trustworthy than an untrusted one.

Model for central client-server. The smart contract is a BC programming protocol that ensures that a scheduled operation is carried out. The blockchain, therefore, guarantees data integrity and authenticity, making it an effective solution for the protection of IoT devices against information theft.

Efforts to provide protection. Several supply chain, access control, application security, and IoT BC-based solutions have been suggested. However, the latest solutions do not comply with the time delay either, and cannot be extended to resource-restricted IoT devices [36, 37].

Some research, for example, focused only on the improvement of an IoT device's time response rather than its confidentiality and support. By breaking their BC architecture into three levels, i.e., IoT, fog, and cloud, they provided data integrity for cyber-physical systems (CPS) [38].

Using the Trustful Space-Time Protocol (TSTP), which is centered on confirmation, the IoT devices in the very same environment regain relationships with each other (PoT). Proof of luck (PoL) was used during the fog level to create responsibility to fix IoT information that generates a cryptographic digest for a data audit. SHA-256 was used to hash the data generated from the first level and saved temporarily. The data was permanently stored at the third level of the cloud, which is a public ledger, after acknowledgment and agreement had been achieved. Other than data integrity, key management utilizing time synchronization and node position was also provided by the report. HECOPS was used via multilateration to estimate the node's position, and clock synchronization was provided by TSTP. The paper suggested the use of several consensus points, such as PoT and PoL, but did not discuss any question of user privacy. The idea of securing data obtained from the drone using public BC was provided in another paper that provided data integrity. There were four modules presented by DroneChain; drones, management system, cloud server, and BC network. The control system managed the drone, and the software was encrypted and processed on a decentralized BC using a cloud server. The resulting system was trustworthy or accountable, provided immediate integrity of information, and had a resilient infrastructure. The study used PoW, however, which was not the best alternative for a real-time IoT application such as drones. In comparison, data provenance nor user/data protection was not provided by the network [39–41].

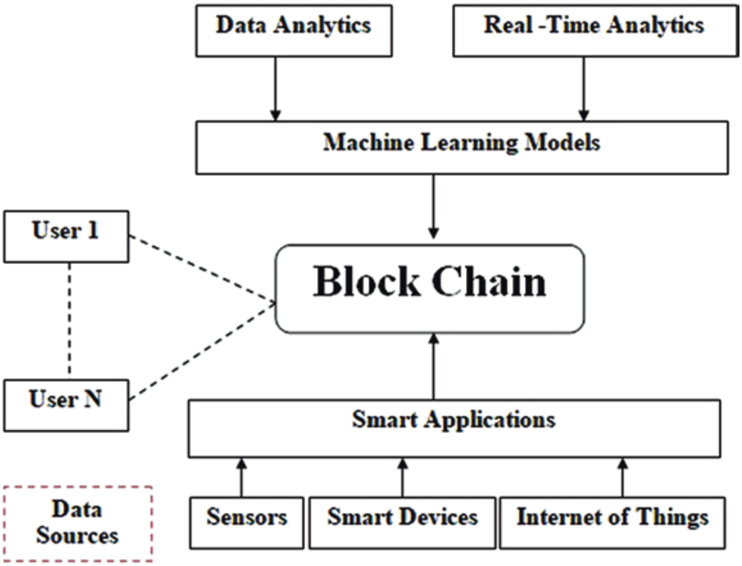


Fig. 8 Architectural diagram for data source with AI model

7 DeepChain Suggested a Value-Driven Reward System Based on BC to Solve Security Problems

For the model training process, DeepChain ensures data protection and auditability. Using the threshold Paillier method that offers an additive homomorphic property, confidentiality is used. Utilizing CNN algorithms and the MNIST dataset, DeepChain showed that even more parties were interested in the process.

The lower the preparation accuracy, the more collaborative training. To practice, ML classifiers require databases. Due to many privacy issues, such as data leakage, data integrity, and possession, these datasets are obtained from various entities that are typically unwilling to share their data. Users do not know how and when it is possible to use their knowledge [42] (Fig. 8).

8 Challenges to ML and BC

We assume that in providing maximum security and privacy for IoT networks, a single technology or tool, such as BC or ML, will not suffice. The research group is therefore in desperate need of time to investigate the provision of IoT security and privacy with the merger of BC and ML, which has the following challenges:

Storage: ML algorithms work better with bigger datasets, as described in Sect. 4. The growth of data on BC platforms, however, will degrade its performance.

To find a compromise, which would be perfect for IoT applications, open a research issue.

Latency challenges: An IoT network will produce a large amount of latency, depending on the scenario.

The volumes of information are more beneficial for deep learning. The overall speed of the ML system will accelerate. Both ML and BC have difficulty in terms of usability since both are computationally intensive.

Costs of response. Many machine learning algorithms use more power. It is normal in major IoT networks to anticipate increasing costs for wire access, routers, and switches. Similarly, when more users enter in a device, efficiency slows. On average, in the Ethereum, BC transactions are conducted at a rate too slow for a cryptocurrency. IoT software is where billions of transactions occur every second.

Vulnerability: The combination of ML and BC will dramatically increase security. There are some legal dilemmas as well.

The rise in the number of threats, particularly. Malicious and potentially malicious code increases in complexity with every passing day.

Real-time IoT networks. While it is possible, the training stage of ML would take a long time. This form of defense is only feasible when an eligible safety is on offer.

Blockchain technology. Information immutability can also be assured, and its adjustments can be specified. Moreover, there is considerable issue with the data on the blockchain. Besides that, it is not difficult to confirm whether equipment or sensors are malfunctioning prior to the problem. The device has been tried. Besides the above issues, BC is vulnerable to the risk of privacy disclosure. Methods are applied online and are available for all readers without cost [43].

Using third-person pronouns. As the data shows, there are also several opportunities raised in BC. The quantity of storage required for ML is extremely high. This move theoretically improves the average output (latency) of conventional models [44, 45].

Processing speed: It is difficult to identify vast volumes of data, because ML and BC are comparatively more data-consuming.

Communication costs. Many ML algorithms need extra processing and communication with increasing quantity of data transmitted that will lead to an increase of money expenses.

Often, the BC. As the number of users and nodes increase, congestion becomes more serious. On average, 90%, an Ethereum BC handles just 12 transactions per second, which is not possible in a conventional payment system.

Networks, where millions of transactions are taking place every second of the day. The combination of MBD and BB may have a major impact on economic and financial decisions. There are a few issues surrounding privacy in the present period. There is a rise in frightening circumstances. Malicious software and malware problem is difficult to identify and avoid. These are very useful in real-time IoT networks [46, 47].Although it is possible for most to go through the preparation, it could take a long time. Detection of malicious traffic is only possible with qualified models on the blockchain technology. It is possible to guarantee data immutability and to be able to define its transformations. However, because of the incorrect data, this problem is occurring. Moreover, these early defects cannot be expected before anything happens suddenly.

The tests were completed and still have several things that are vulnerable to privacy evasion. The data is freely accessible for anyone to read it and analyze.

Getting private. BC is a solution to these problems but still restricted access in a way. There are abundant data available for ML to carry out its work [48, 49].

9 Conclusion

Blockchain and ML's recent developments have made them route developments. With the foundation of numerous intelligent applications such as smart cities, UAV, SG, and data trading, the distributed ledger has the potential to operate. We have provided extensive details on BT and ML in this paper, along with their uses in smart applications, and proposed an architecture based on ML-BT. An ML-BT-based data analysis framework can be developed and implemented using this architecture. It provides a discussion and comparison of various current surveys. Then, we implemented the taxonomy of the ML-BT solution, concentrating on objective-oriented, layer-oriented, countermeasures, and smart application dimensions. In each dimension, a comparative study of available methodologies and methods is presented. Then, during ML adoption in BT-based systems, we have listed several research challenges faced that require solutions. We also stressed a range of research opportunities that could serve as a future, such as the availability of infrastructure, quantum resilience, and privacy concerns.

References

1. S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system. Available online: https://bitcoin.org/en/bitcoin-paper (accessed on 29 June 2017)
2. N. Bozic, P. Guy, S. Stefano, A tutorial on blockchain and applications to secure network control-planes. SCNS IEEE 2016. [CrossRef]
3. D. Bradbury, The problem with bitcoin. Comput Fraud Secur. **11**, 5–8 (2013) [CrossRef]
4. G. Paul, P. Sarkar, S. Mukherjee, Towards a more democratic mining in bitcoins. In *Proceedings of the International Conference on Information Systems Security*, Hyderabad, India, 16–20 December 2014; Springer International Publishing: Cham, Switzerland, 2014
5. T. Bamert, C. Decker, R. Wattenhofer, S. Welten, BlueWallet: the secure BitcoinWallet, in *Security and Trust Management*, ed. by S. Mauw, C. Jensen, (Springer International Publishing, Cham, Switzerland, 2014), pp. 65–80
6. E. Anceaume, T. Lajoie-Mazenc, R. Ludinard, B. Sericola. Safety analysis of Bitcoin improvement proposals. In *Proceedings of the 2016 IEEE 15th International Symposium on Network Computing and Applications (NCA)*, Cambridge, MA, USA, 31 October–2 November 2016
7. R. Upadhyaya, A. Jain, Cyber ethics and cybercrime: a deep dwelved study into legality, ransomware, underground web and bitcoin wallet. In *Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA)*, Noida, India, 29–30 April 2016

8. S. Haber, W.S. Stornetta, How to time-stamp a digital document. In *Proceedings of the Conference on the Theory and Application of Cryptography*, Sydney, NSW, Australia, 8–11 January 1990; Springer: Berlin/Heidelberg, Germany, 1990
9. I. Eyal, G.S. Emin, Majority is not enough: Bitcoin mining is vulnerable. In *Proceedings of the International Conference on Financial Cryptography and Data Security*, Christ Church, Barbados, 3–7 March 2014; Springer: Berlin/Heidelberg, Germany, 2014
10. K. Petersen, R. Feldt, S. Mujtaba, M. Mattsson, Systematic Mapping Studies in Software Engineering. In *Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering (EASE)*, Bari, Italy, 26–27 June 2008
11. C. Mann, D. Loebenberger, Two-factor authentication for the Bitcoin protocol. In *International Workshop on Security and Trust Management*; Springer International Publishing: Cham, Switzerland, 2015
12. Y. Yuan, F.-Y. Wang, Towards blockchain-based intelligent transportation systems. In *Proceedings of the 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, Rio de Janeiro, Brazil, 1–4 November 2016
13. E.K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, B. Ford, École Polytechnique Fédérale de Lausanne (EPFL). Enhancing bitcoin security and performance with strong consistency via collective signing. In *Proceedings of the 25th USENIX Security Symposium (USENIX Security 16)*, Austin, TX, USA, 10–12 August 2016
14. M. Vasek, M. Thornton, T. Moore, Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem. In *Proceedings of the International Conference on Financial Cryptography and Data Security*, Christ Church, Barbados, 3–7 March 2014; Springer: Berlin/Heidelberg, Germany, 2014
15. M. Bastiaan, Preventing the 51%-attack: A stochastic analysis of two phase proof of work in bitcoin. Available online. http://referaat.cs.utwente.nl/conference/22/paper/7473/preventingthe-51-attack-astochastic-analysis-of-two-phase-proof-of-work-in-bitcoin.pdf (accessed on 29 June 2017
16. M.H.U. Rehman, E. Ahmed, I. Yaqoob, I.A.T. Hashem, M. Imran, S. Ahmad, Big data analytics in industrial IoT using a concentric computing model. IEEE Commun. Mag. **56**(2), 37–43 (2018)
17. P.K. Sharma, J.H. Ryu, K.Y. Park, J.H. Park, J.H. Park, Li-Fi based on security cloud framework for future IT environment. HCIS **8**(1), 1–13 (2018)
18. W. Yu, F. Liang, X. He, W.G. Hatcher, C. Lu, J. Lin, X. Yang, A survey on the edge computing for the internet of things. IEEE Access **6**, 6900–6919 (2018)
19. M. Chiang, S. Ha, C.-L.I.F. Risso, T. Zhang, Clarifying fog computing and networking: 10 questions and answers. IEEE Commun. Mag. **55**(4), 18–20 (2017)
20. O. Novo, Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet Things J. **5**(2), 1184–1195 (2018)
21. K. Kalkan, S. Zeadally, Securing internet of things with software defined networking. IEEE Commun. Mag. **56**(9), 186–192 (2018)
22. B.B. Zarpelão, R.S. Miani, C.T. Kawakani, S.C. de Alvarenga, A survey of intrusion detection in internet of things. J. Netw. Comput. Appl. **84**, 25–37 (2017)
23. I. Butun, B. Kantarci, M. Erol-Kantarci, Anomaly detection and privacy preservation in cloud-centric internet of things. In *Proc. IEEE International Conference on Communication Workshop (ICCW)*, Jun 2015, pp. 2610-2615
24. S.R. Kumar, N. Gayathri, Trust based data transmission mechanism in manet using solsr. In *Annual Convention of the Computer Society of India* (pp. 169–180). Springer, Singapore., S. R., & Gayathri, N. (2016, December). Trust based data transmission mechanism in MANET using sOLSR. In *Annual Convention of the Computer Society of India* (pp. 169–180). Springer, Singapore
25. S.R. Kumar, N. Gayathri, B. Balusamy, Enhancing network lifetime through power-aware routing in MANET. Int. J. Internet Technol. Secur. Trans. **9**(1–2), 96–111 (2019)

26. HIMSS Blockchain Work Group. (2017, Oct. 23). Part 1: Navigating the blockchain landscape—Opportunities in digital health. [Online]. Available: http://www.himss.org/news/part-1-navigatingblockchain-landscape-opportunities-digital-health
27. D. Houlding, H. Flannery. (2018, Feb. 1). Part 2: Healthcare blockchain—A path to success in 2018. [Online]. Available: http://www.himss.org/news/part-2-healthcare-blockchain-path-success-2018
28. R. Rahim, R. Patan, R. Manikandan, S.R. Kumar, Introduction to blockchain and big data, in *Blockchain, Big Data and Machine Learning*, (CRC Press, 2020), pp. 1–23
29. HIMSS 2018 conference session. (2018, Mar. 6). Blockchain reset: Seeing through the hype and starting down the path. [Online]. Available: http://www.himssconference.org/session/blockchainreset-seeing-through-hype-and-starting-down-path
30. R. Chandran, S.R. Kumar, N. Gayathri, Designing a locating scams for mobile transaction with the aid of operational activity analysis in cloud. Wirel. Pers. Commun., **117**, 1–14 (2020)
31. The Linux Foundation. (2017). About Hyperledger. [Online]. Available: https://www.hyperledger.org/about Ethereum Foundation. (2018). Ethereum: Blockchain app platform. [Online]. Available: https://www.ethereum.org/
32. A. Azaria, A. Ekblaw, T. Vieira, A. Lippman. (2016, Aug. 22–24). MedRec: using blockchain for medical data access and permission management, presented at the Int. Conf. Open and Big Data, Vienna, Austria. [Online]. Available: http://ieeexplore.ieee.org/document/7573685/
33. A.K. Show, A. Kumar, A. Singhal, N. Gayathri, K. Vengatesan, Future blockchain technology for autonomous applications/autonomous vehicle, in *Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles*, (IGI Global), United States of America pp. 165–177
34. N. Kumar, N. Gayathri, M. A. Rahman, B. Balamurugan (eds.), *Blockchain, Big Data and Machine Learning: Trends and Applications*, United States of America (CRC Press, 2020)
35. C. McFarlane, M. Beer, J. Brown, N. Prendergast. (2017, May). Patientory: a healthcare peer-to-peer EMR storage network v1.1. [Online]. Available: https://patientory.com/patientory_whitepaper.pd.
36. S.K. Sharma, R.K. Modanval, N. Gayathri, S.R. Kumar, C. Ramesh, Impact of application of big data on cryptocurrency. Cryptocurrencies and Blockchain Technology Applications, Scrivener Publishing LLC, Beverly, Massachusetts. 181–195 (2020)
37. A. Pandey, A. Kumar, A. Singha, N. Gayathri, S.R. Kumar, 4 Blockchain Databases 2. *Blockchain, Big Data and Machine Learning: Trends and Applications*, 97 (2020)
38. R. Chandran, S.R. Kumar, N. Gayathri, Genetic algorithm-based tabu search for optimal energy-aware allocation of data center resources. Soft. Comput. **24**(21), 16705–16718 (2020). https://doi.org/10.1007/s00500-020-05240-9
39. L. Dong, W. Jinwu, Block chain technology principle, application field and challenge [J]. Telecomm. Sci. **32**(12), 19–25 (2016)
40. Y. Yong, W. Feiyue, Development status and Prospect of block chain technology [J]. Acta Automat. Sin. **42**(4), 481–494 (2016)
41. G. Nagasubramanian, R.K. Sakthivel, R. Patan, A.H. Gandomi, M. Sankayya, B. Balusamy, Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Comput. & Applic. **32**(3), 639–647 (2020)
42. C. Gao, T. Liang, L.I. Huixing, et al., Development and Application of open automated demand response [J]. Power Syst. Technol. **93**(3), 12–12 (2013)
43. R.K. Sakthivel, G. Nagasubramanian, F. Al-Turjman, M. Sankayya, Core-level cybersecurity assurance using cloud-based adaptive machine learning techniques for manufacturing industry. Trans. Emerg. Telecommun. Technol., e3947 (2020)
44. W. Beibei, S. Yujun, L. Yang, Application of uncertain demand response modeling in power integral incentive decision [J]. Automat. Electr. Power Syst. 2015(10). R.M. Parizi, On the gamification of human-centric traceability tasks in software testing and coding. In: *2016 IEEE 14th International Conference on Software Engineering Research, Management and Applications (SERA)*, Towson, MD, 2016, pp. 193–200

45. A. Back, et al., Enabling blockchain innovations with pegged sidechains [Online]. Available: http://www.blockstream.com/sidechains.pdf, 2014
46. P. Robinson, Requirements for Ethereum Private Sidechains, arXiv Prepr. arXiv1806.09834, 2018
47. Q. Zhang, R.M. Parizi, K.K.R. Choo, A pentagon of considerations towards more secure Blockchains. IEEE Blockchain Tech. Briefs. pp. 1–30 (2018)
48. Bitcoin-abe, https://github.com/bitcoin-abe/bitcoin-abe
49. T.T.A. Dinh, J. Wang, G. Chen, R. Liu, B.C. Ooi, K.-L. Tan, BLOCKBENCH: a framework for analyzing private blockchains. In: *Proceedings of the 2017 ACM International Conference on Management of Data*, 2017, p. 10851100