Internet of Things and Blockchain Integration: Use Cases and Implementation Challenges

Kelechi G. Eze(✉), Cajetan M. Akujuobi, Matthew N. O. Sadiku, Mohamed Chouikha, and Shumon Alam

The Center of Excellence for Communication Systems Technology Research (CECSTR), Systems to Enhance Cybersecurity for Universal Research Environment (SECURE), Cybersecurity Center of Excellence, Department of Electrical Engineering, Prairie View A&M University, Prairie View, TX 77446, USA
kelechigodwin9@gmail.com, {cmakujuobi,mfchouikha,shalam}@pvamu.edu, sadiku@ieee.org

Abstract. Research on blockchain (BC) and Internet of things (IoT) shows that they can be more powerful when combined or integrated together. However, the technologies are still emerging and face a lot of challenges. The paper focuses on Internet of things integration with the blockchain technology. We reviewed these technologies and identified some use cases of their combination and key issues hindering their integration. These issues are scalability, interoperability, inefficiencies, security, governance and regulation. While these issues are inherent in the current generations of blockchain such as Bitcoin and Ethereum respectively, with a well-designed architecture, the majority of these issues can be solved in the future generation. This work is inspired by the rapid growth in the number of connected devices and the volume of data produced by these devices and the need for security, efficient storage and processing.

Keywords: Blockchain · Security · Internet of Things · Smart contracts · Artificial intelligence · Cloud computing

1 Introduction

Blockchain and Internet of Things (IoT) are emerging Internet-based technologies that will have a tremendous disruptive effect in all disciplines, industries and economies [1]. Blockchain (Distributed Ledger Technology, (DLT)) is a decentralized network that constitutes of nodes or parties where all nodes in the network maintain a copy of the blockchain (i.e. have the same data, keeps a history of the transactions and receive the same transaction). The blockchain uses cryptography and consensus algorithm to make transaction secure and records immutable in a distributed fashion. Blockchain technology started with Bitcoin in 2008 which is referred to as the first generation blockchain. Today, we have

W. Abramowicz and R. Corchuelo (Eds.): BIS 2019 Workshops, LNBIP 373, pp. 287–298, 2019.
https://doi.org/10.1007/978-3-030-36691-9_25

the second generation blockchain like the Ethereum blockchain, NEO blockchain and Waves blockchain with smart contract support, a feature that makes it programmable. The property of programmability makes the second generation blockchain adaptable to a whole lot of application beyond Bitcoin, especially in the area of Internet of thing.

Applications of blockchain beyond bitcoin include IoT security, management of IoT devices and service provision in IoT, data management, data security, greater efficiency etc [2–6,9–17]. Blockchain has gained so much attention from the private and public sector, especially in the financial industry. The major attractions for the blockchain technology are its distributed nature, security (immutability) and applicability to a whole lot of domains.

While this paper is focused on IoT integration with blockchain, AI and the cloud will have a crucial role to play in this integration. While IoT devices produce enormous quantity of data, these data are usually aggregated for computation and processing in the cloud and AI applied to further turn these big data into actions and insights. Accordingly, IoT, AI, and blockchain can be considered as interconnected organic processes where IoT plays the role of sensing, AI handles reasoning and the blockchain acts as the memory [18].

Blockchain technology converged with Internet of things, artificial intelligence (AI) and cloud computing will bring solutions to problems, leading to greater trust and reliability as well as extended advantages within these technologies. Efficient and secure integration of emerging technologies and IT systems of diverse types, needed to build smart industrial, city and home applications and services, remains the greatest challenge to overcome today. This paper investigates current issues in blockchain technology with respect to its application and integration in the Internet of things, while considering AI and the cloud as a vital components of this integration.

The rest of this paper is organized as follows. Section 2 presents an overview of the technological components of blockchain and Internet of things (IoT). The Integration of blockchain and IoT, that is bringing blockchain and IoT to function together is discussed in Sect. 3. Section 4 is a summary of the use cases of integrating blockchain and IoT. The issues we found to be the major issues hindering blockchain and IoT integration are presented and analyzed in Sect. 5 and lastly our conclusion and future directions is presented in Sect. 6.

2 Overview of the Basic Concepts

In this section we give a brief overview of the basic concepts of blockchain, Internet of Things and associated technologies.

2.1 Blockchain Technology

Blockchain refers to a decentralized network of databases in the form of blocks capable of holding and transferring digital assets or data in a tamper-proof manner. Blockchain is designed with the properties of immutability, no central authority, irreversibility, time-stamping, replication and cryptography. It uses elliptic curve cryptography (ECC) and various hashing schemes like KECCAK-256 and secure hashing algorithms (e.g. SHA-256) for security, business logic and replicated ledger [14,19]. Figure 1 is a simplified structure of the blockchain. Each block in a blockchain is linked cryptographically to the previous blocks to maintain immutability as shown in Fig. 1 (i.e. the parentHash of any block must be same as the hash of the previous block). The genesis block (first block) has index of 0, timestamp of 0, parentHash of 0 and a preassigned nonce value while the second block derive most of its values computationally or cryptographically from the genesis block and so on. The nonce is a 32 bit random number taken into account during consensus process. The consensus algorithm is used to reach decision on a single version of the data to get stored in the blockchain. Transactions are events allowed to take place within the blockchain protocol such as sending and receiving data (e.g. cryptocurrency) from one node to another and are stored in blocks.

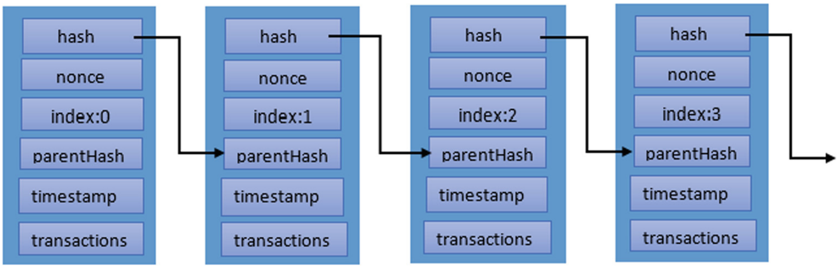
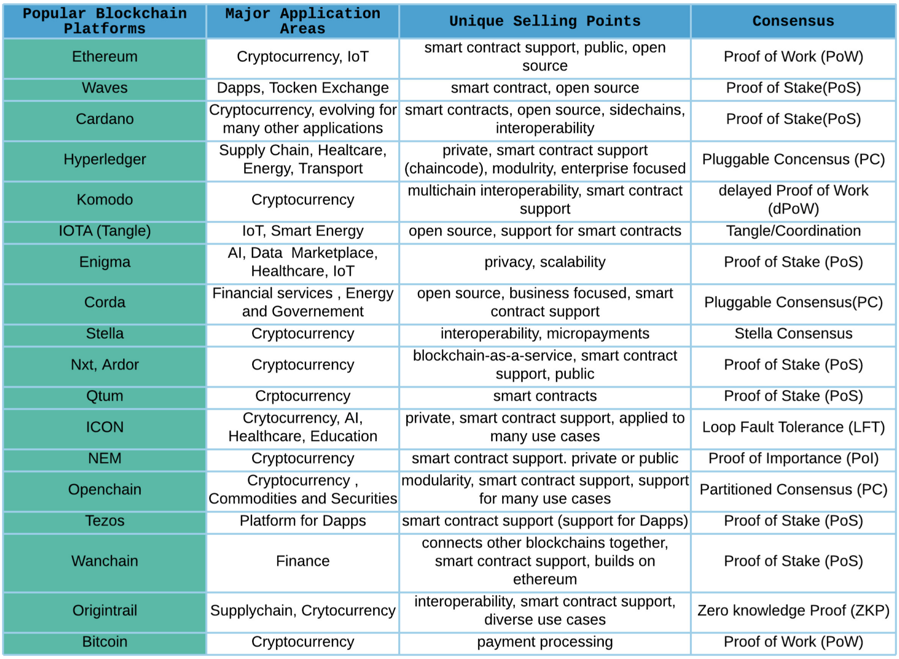


Fig. 1. Basic structure of blockchain.

Some examples of blockchain are Bitcoin, Ethereum, Corda, Hyperledger, Komodo etc. We have prepared a list of popular blockchain platforms as shown in Fig. 2. The blockchains are categorized as private or permissioned, public blockchains or unpermissioned blockchain and consortium blockchain [6]. A public blockchain are free to the public to join without restrictions but the private blockchain are restricted and can only be connected to with valid credentials. An example of permissioned blockchain are Hyperledger fabric and Ethereum is an example of permissioned blockchain.

2.2 Smart Contracts

Smart Contract is an executable code representing a set of promises or agreements that automatically runs on the blockchain and is self-enforced [20]. Just like a computer program, a smart contract is written in a smart contract language (Solidity) or general-purpose language (Java, Go or node.js), compiled and run on a blockchain. The smart contract is compiled into two separate parts, the application binary interface (ABI) and the bytecode [9]. The bytecode is the



Popular Blockchain Platforms	Major Application Areas	Unique Selling Points	Consensus
Ethereum	Cryptocurrency, IoT	smart contract support, public, open source	Proof of Work (PoW)
Waves	Dapps, Tocken Exchange	smart contract, open source	Proof of Stake(PoS)
Cardano	Cryptocurrency, evolving for many other applications	smart contracts, open source, sidechains, interoperability	Proof of Stake(PoS)
Hyperledger	Supply Chain, Healtcare, Energy, Transport	private, smart contract support (chaincode), modulrity, enterprise focused	Pluggable Concensus (PC)
Komodo	Cryptocurrency	multichain interoperability, smart contract support	delayed Proof of Work (dPoW)
IOTA (Tangle)	IoT, Smart Energy	open source, support for smart contracts	Tangle/Coordination
Enigma	AI, Data Marketplace, Healthcare, IoT	privacy, scalability	Proof of Stake (PoS)
Corda	Financial services , Energy and Governement	open source, business focused, smart contract support	Pluggable Consensus(PC)
Stella	Cryptocurrency	interoperability, micropayments	Stella Consensus
Nxt, Ardor	Cryptocurrency	blockchain-as-a-service, smart contract support, public	Proof of Stake (PoS)
Qtum	Crptocurrency	smart contracts	Proof of Stake (PoS)
ICON	Crytocurrency, AI, Healthcare, Education	private, smart contract support, applied to many use cases	Loop Fault Tolerance (LFT)
NEM	Cryptocurrency	smart contract support. private or public	Proof of Importance (PoI)
Openchain	Cryptocurrency , Commodities and Securities	modularity, smart contract support, support for many use cases	Partitioned Consensus (PC)
Tezos	Platform for Dapps	smart contract support (support for Dapps)	Proof of Stake (PoS)
Wanchain	Finance	connects other blockchains together, smart contract support, builds on ethereum	Proof of Stake (PoS)
Origintrail	Supplychain, Crytocurrency	interoperability, smart contract support, diverse use cases	Zero knowledge Proof (ZKP)
Bitcoin	Cryptocurrency	payment processing	Proof of Work (PoW)

Fig. 2. Blockchain platforms.

actual machine instructions that is made up of opcodes; whereas the ABI is data formatted in JavaScript Object Notation (JSON) that describes the various functions (methods) in the smart contract. ABI also provides a convenient way to interact with the smart contracts.

Smart contract is a feature of blockchain that makes it programmable and therefore possible to develop flexible and decentralized applications on blockchain. These applications run on blockchain when predefined conditions are met and are tamper proof, secure and transparent [20]. A typical smart contract specifies the parties involved in a transaction, what the transaction should do and the state transitions in the blockchain. Therefore, the smart contract removes the need for a trusted third party in a blockchain technology. Most blockchains supports smart contracts.

2.3 Internet of Things

Internet of things (IoT) is simply the enabling of non-traditional computing devices for Internet connectivity. IoT refers to anything (e.g cars, smart devices, objects, wearables, etc.) enabled to communicate (send and receive data) using the Internet network. Edge devices in Internet of things paradigm are often limited in memory and computational capability and thus uses specialized protocols MQTT, CoAP, ZigBee, Bluetooth, LoRaWan etc. for communication and are inherently distributed. Internet of things thus involves devices of various types, sizes and capabilities that are distributed [10].

The rapid growth of Internet of things poses serious challenge to the centralized or the client-server model which involves having these many IoT devices connected to a single server with high computational and storage resources for management and control. The centralized model is expensive and suffers from single point of failure when compromised by cybersecurity attacks (e.g. Denial of Service (DoS) and ransomware attacks) [11,14,21]. A solution to this problem is a decentralized model for IoT where nodes will share the computational power as well as the storage resources required in the network and can tolerate faults [11].

Internet of Things (IoT) are widely being adopted in industries such as manufacturing, healthcare, finance, logistics, energy etc where it helps in making automation of industrial processes a lot more efficient. The IoT also empowers flexible information and resource sharing in the industry as well as enhanced collaborations. The IoT is therefore very essential for expanding growth and productivity in Industrial sector.

3 Blockchain and IoT Integration

The centralized architecture where a central server provides services to clients on the network has downsides of high maintenance costs, poor interoperability and single point of failures from security threats [4]. A decentralized architecture on the other hand will eliminate the disadvantages of the centralized architecture. A rising decentralized management platform for IoT is blockchain. By design, the blockchain network operates in a decentralized fashion where network nodes can communicate in a peer-to-peer fashion.

Blockchain and Internet of things integration will strengthen the security of the future Internet as this integration will incorporate the security features of blockchain. Requirements for the implementation of the aforementioned integration will depend on hosting platform (cloud or fog), use case and choice of blockchain platform (such as Ethereum, Hyperledger etc.) [7]. We have shown this integration where Internet of things integrates the cloud and AI for extended advantages in Fig. 3.

The Internet of things in the block diagram (Fig. 3) contains the actors in the network such as user applications and IoT devices and communicate to the cloud network using the gateways. The cloud network aggregates sensor data in the cloud storage for computation and analytics using built-in AI capabilities. The capabilities of the cloud network and smart contracts efficiently monitors raw telemetry data (sensor data), converts it to the appropriate format and routes it to the blockchain. IoT devices are also able to receive services (e.g. secure updates) from the blockchain on a regular basis as the case may be. The block diagram also shows that the cloud network houses Application Programming Interface (APIs) or access layer that give enterprises and cloud providers access into the blockchain. Also note that from Fig. 3, the gateway functions as a node

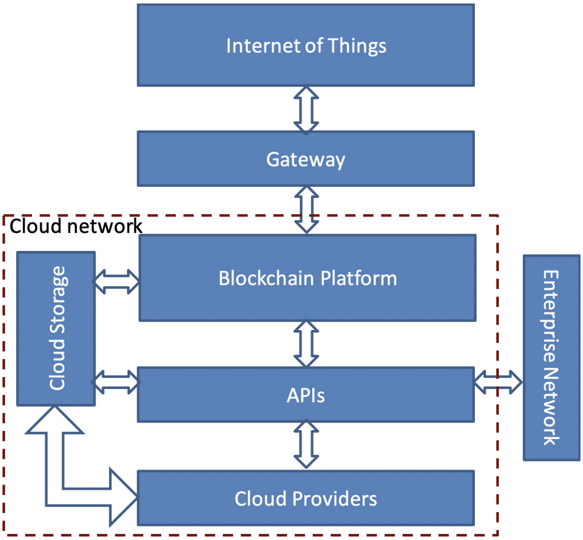


Fig. 3. Block diagram of blockchain and IoT integration.

on the blockchain (external to the cloud network but local to the IoT devices) and therefore decentralized.

4 Use Cases of Converging Blockchain and IoT

Many industries today are using blockchain to solve most IoT issues such as security and identity management. Extended advantages are also derived by combining these two technologies. The following are the use cases of combining blockchain and Internet of Things [8].

- ***Access Control and Identity Management***: Using smart contracts, features of a blockchain can be extended to adapt to a variety of use cases. A contract for access control will enforce access control of the various resources on the blockchain network and a smart contract for identity management will enhance the identity management capability of the blockchain for various IoT devices on the network [15].
- ***Secure Update of Edge Devices in IoT***: Blockchain combined with Internet of things can be used to provide firmware or software update in scenarios like the smart cities and smart homes. Here, smart contracts are used to define the update conditions and the secure nature of blockhain make them resistant to cyberattacks.
- ***Logistics and Supply Chain Management***: In IoT-enabled supply chain where vehicles and cargoes are equipped with sensors, combining blockchain and Internet of things enables near real time access to status information regarding shipment, increasing visibility and reliability within the supply chain.

- ***Automobile Industry***: Automobiles are becoming highly equipped with sensors and Internet capabilities making them part of the IoT ecosystem. Connecting smart cars to the blockchain network will enable trusted exchange of information, improved connectivity and security as well as accurate vehicle records (e.g. trip information, service, fault information etc.).
- ***Sharing Economy***: As the sharing economy is rapidly growing in adoption, blockchain can enable a decentralized application on shared economy, making the exchange of value, goods and services seamless at reduced cost.
- ***Healthcare Industry***: Blockchain by enabling transparency and traceability in pharmaceutical supply chain can drastically reduce the problem of fake medicines (one such application is mediledger project). Also patients using monitoring healthcare devices connected to the blockchain can choose who to share their data and be guaranteed that only healthcare professional responsible for their care can have access to such data.
- ***Agriculture***: Sensor data from farms stored on the blockchain can provide useful information regarding provenance of products, improved transparency in agricultural supply chain and informed decision making for farmers and customers.
- ***Micropayments***: Micropayments in IoT will involve either machine to machine or person to machine transactions using crypto currencies without involving centralized third parties like the banks. Examples are a smart connected electric vehicle making payment to a charging station and a person making payment for a product from a connected vending machine. Micropayment enables faster and cheaper payment among the parties involved.
- ***Data Integrity in IoT***: Combining IoT and Blockchain will ensure IoT data integrity automatically using the digital signature and hashing technique that are inbuilt by design on the blockchain. This is especially very useful in scenarios where multiple parties are involved like the smart energy grid to eliminate fraud and rip-offs by the participants in energy trading.

5 Major Blockchain and IoT Integration Issues

Blockchain has a number of technological limitations as well as non-technological limitations, although it is a very powerful technology. We have reviewed and identified the major problems that hinders blockchain integration with Internet of things as shown in Fig. 4. They are scalability, interoperability, inefficient consensus algorithm, security, privacy, governance and regulations.

5.1 Issue with Scalability

A major issue in the integration of blockchain with Internet of things is scalability [4]. The problem of scalability in the context of blockchain integration with Internet of things is caused mainly by ubiquitous nature of IoT [22] and the limitations inherent in a typical IoT device. An optimal blockchain solution must be scalable with the number of IoT devices or gateways (i.e. nodes on the

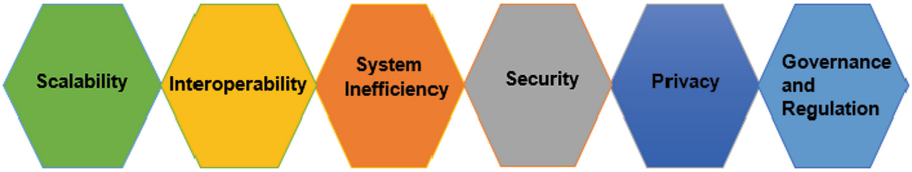


Fig. 4. Internet of things and blockchain integration challenges.

blockchain network) and be able to handle high transaction rates. The block size and block generation interval will vary with the number of IoT devices and will reach a maximum set size at a point. The transaction throughput or performance increases with the number of IoT devices up to a maximum while the block generation interval decreases as the number of IoT devices increase up to an optimal point [4]. The blockchain is initialized with the genesis block and grows according to the configuration settings for the genesis file, e.g. the gas limit, mining difficulty, etc. In bitcoin, however the block size determines the rate of growth. In each case, a high number of transactions will result in a corresponding decrease in throughput. The number of transactions per second is governed by: (i) the block generation time, (ii) the number of transaction that a block can hold, and (iii) the time it takes to reach a consensus.

"Blockchain pruning" (i.e., erasing unnecessary record to avoid holding the entire blockchain on a single node) is a possible solution to the ever-growing blockchain [23]. With the help of AI, federated learning, a new decentralized machine learning system can also be used along with other techniques such as sharding technique to make the blockchain system more efficient.

5.2 Issue with Interoperability

Interoperability is the ability to transact and share data across blockchain and non-blockchain systems. Today, interoperability is a big issue facing the integration of blockchain with other systems such as Internet of things, AI and cloud computing. Blockchain was originally designed to operate with computers with high computational powers on the Internet. Internet of things (edge devices/sensors) on the other hand has low computational powers by design. IoT and blockchain are therefore mismatch in computational powers. IoT sense and transmit enormous data in Terabytes while the blockchain is limited by design on storage capacity. This is another important bottleneck that need to be addressed.

AI and cloud computing when combined with this integration will play a huge role in solving the interoperability issue faced with Blockchain and IoT. While the AI will help reduce this data to a form that can be handled by blockchain through techniques such as data compression, data normalization, data smoothing etc. [24], cloud computing will provide a suitable computation environment for these data.

5.3 System Inefficiency

Blockchain is slow in running codes and smart contracts on traditional computing devices. This is because the process of mining in blockchain requires a lot of computational power. Therefore, miners or special hardware are required to carry out mining in a typical blockchain solution. This could lead to inefficiencies and extra investment.

Popular consensus algorithm used in a blockchains today are modified Proof of Work (PoW), Practical Byzantine Fault Tolerance and Binary consensus [11]. Major concerns about these consensuses are the high computational power consumed in the mining process and the time taken (high latency) to reach consensus [11,25]. The Proof of Work is also vulnerable to majority hash rates or the 51% attack which makes it possible for someone to reverse transaction history and prevent incoming transaction from confirmation by controlling most of the networks hash rate. Examples of where this attack has occurred are Bitcoin Gold, Verge, ZenCash, and other POW-based cryptocurrencies [5]. Other consensus protocol used in blockchain are Proof of Stake and (PoS), Proof of Burn (PoB), Proof of Activity, Proof of Capacity (PoC), Proof of Elapsed Time (PoET), Proof of Authority (PoA), Proof of Importance (PoI) [17,26]. These consensus algorithms have issues to be addressed as well.

5.4 Issue with Security

Blockchain is said to be immutable and hack resistant. In scenarios such as Decentralized Autonomous Organization (DAO) and Bitfinex [27], where extra layers of applications are involved however, security could be a major concern. This will also be the case when blockchain is integrated with other technology like the Internet of things, AI and the cloud.

The security of blockchain rests upon two one-way cryptographic technologies: cryptographic hash functions and digital signatures. Most blockchain platforms generate this digital signature using the elliptic curve public-key cryptography (ECDSA) or the large integer factorization algorithm (RSA) [27]. Unfortunately, what determines the security of these algorithm is the computational complexity of some mathematical algorithms. Unfortunately computers like the quantum computers could solve these algorithms thereby making underlying digital signature algorithm vulnerable to attack. The Grover search algorithm for example could lead to the 51% attack by enabling a quadratic speedup in calculating the reverse hash function used in blockchain.

Another security concern in blockchain is smart contracts. Smart contracts cannot access data outside of their network without the use of external third-party services. This third-party service uses what is known as oracles, a data feed or an agent that communicate real world occurrences to the blockchain. Effective implementation of an oracles come with huge security challenges because third party data sources cannot be fully reliable for trustless execution in a blockchain network. Data from oracles should therefore be properly authenticated using appropriate methods. Finally, a smart contract should be developed following best practices in software engineering to ensure code security and quality. A poorly written smart contract may contain a bug or security hole that attacker may leverage to compromise the system.

5.5 Issue with Privacy

An important feature of the blockchain is transparency where transactions can be audited, traced back and verified from the first transaction. In fact, all data in a blockchain is public by default and this means no privacy. Trust is maintained in the blockchain by keeping data transparent in this way. This situation directly raises the issue of privacy in blockchain and it becomes even more serious with the Internet of things when it involves a privacy sensitive information such as smart home devices and smart medical devices.

The current anonymity features in blockchain is not be enough to protect privacy and it is highly recommended that more efforts should be made to provide stronger pseudonyms [9] as the data in a blockchain can be accessed by anyone [30]. In order to solve the problem of privacy in blockchain, homomorphic encryption can be used on blockchain data. Homomorphic encryption is the ability to perform compute operations directly on encrypted data. Blockchain like Enigma is able to perform computation on data without exposing the raw data to the nodes of the network by encrypting data and then splitting the data in the network. Zerocash [30] improves upon user privacy by hiding user attributes such as identity, transaction activities and account balances from public access.

5.6 Issue with Governance and Regulation

Governance and Regulation is very important for blockchain standards, interoperability, integration, and architecture. Work in this area has been slow probably due to the complexity of blockchain technology and early stages of its development. According to [6], standard making bodies such as IEEE, NIST and ITU are making progress towards standardizing blockchain. Regulating blockchain is not going to be easy because of the nature of the technology as it was designed with no regulation in mind. However, some level of regulation in form of private and consortium blockchains are currently present [9].

A new set of regulations has to be made to guide the integration of blockchain with other technologies such as IoT, AI and Cloud computing. This could help set standards for the security features that these technologies must have in order to operate.

6 Conclusion

In this work, we reviewed Blockchain technology and identified its integration issues with Internet of things and the need to further extend this integration to include AI and cloud computing. We introduced current state of affairs in the blockchain space and how blockchain is being adopted in areas such as healthcare, government, supply chain management etc. with the Internet of things. We have an integration diagram for blockchain in action with IoT, AI and the cloud. The issues discussed in this paper must be solved to achieve a successful integration of Blockchain and IoT. We summarized major blockchain implementations taking the consensus algorithm used into consideration. There are significant improvements on the Proof of Work (PoW) consensus seen in early blockchains like the bitcoin and Ethereum in form of Proof of Stake (PoS), Proof of Space (PoS), Proof of Burn (PoB), Proof of Importance (PoI) etc. However, the consensus layer still remains an open research issue to be solved in the upcoming generations of blockchain. Other open issues are scalability, interoperability, security, privacy, efficiency and regulation. These issues are currently standing on the way of a successful integration of blockchain and Internet of Things and may take a while to fully resolve.

References

1. Sadiku, M.N.O.: Emerging Internet-Based Technologies. CRC Press, Boca Raton (2019)
2. Zheng, Z., et al.: An overview of blockchain technology: architecture, consensus, and future trends. In: Proceedings of the IEEE 6th International Congress on Big Data, pp. 557–564 (2017)
3. Miller, D.: Blockchain and the Internet of Things in the industrial sector. IEEE IT Prof. **20**(3), 15–18 (2018)
4. Sagirlar, G., et al.: Hybrid-IoT: hybrid blockchain architecture for Internet of Things-PoW sub-blockchains, pp. 1–10 (2018). https://arxiv.org/pdf/1804.03903.pdf
5. Dinh, T.N., Thai, M.T.: AI and blockchain: a disruptive integration. IEEE Comput. **51**(9), 48–53 (2018)
6. Salah, K., Rehman, M.H., Nizamuddin, N., Al-Fuqaha, A.: Blockchain for AI: review and open research challenges. IEEE Access **7**, 1–23 (2019)
7. Samaniego, M., Deters, R.: Blockchain as a service for IoT. IEEE International Conference on Internet of Things and Green Computing and Communications, pp. 433–436 (2016)
8. Opportunities and Use Cases for Distributed Ledger Technologies in IoT (2018). https://www.gsma.com/iot/wp-content/uploads/2018/09/Opportunities-and-Use-Cases-for-Distributed-Ledgers-in-IoT-f.pdf
9. Reyna, A., et al.: On Blockchain and Its integration with IoT. Future Gener. Comput. Syst. **88**, 173–190 (2018)
10. Novo, O.: Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet of Things J. **5**(2), 1184–1195 (2018)
11. Zoican, S., Zoican, R., Vochin, M., Galatchi, D.: Blockchain and consensus algorithms in Internet of Things. In: Proceeding of the International Symposium on Electronics and Telecommunications (ISETC), pp. 1–4 (2018)
12. Pahl, C., El Ioini, N., Helmer, S.: A decision framework for blockchain platforms for IoT and edge computing. In: International Conference on Internet of Things, Big Data and Security (2018)

13. Biswas, S., Sharif, K., Li, F., Nour, B., Wang, Y.: A scalable blockchain framework for secure transactions in IoT. IEEE Internet of Things J. 1–10 (2018)
14. Almadhoun, R., Kadadha, M., Alhemeiri, M., Alshehhi, M., Salah, K.: A user authentication scheme of IoT devices using blockchain-enabled fog nodes. In: Proceedings of the IEEE/ACS 15th International Conference on Computer Systems and Applications, Jordan, Aqaba, pp. 1–8 (2018)
15. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., Wan, J.: Smart contract-based access control for the Internet of Things. IEEE Internet of Things J. 1 (2018)
16. Ølnes, S., Ubacht, J., Janssen, M.: Blockchain in government: benefits and Implications of distributed Ledger Technology for information sharing. Gov. Inf. Q. **34**, 355–364 (2017)
17. Sadiku, M.N.O., et al.: Blockchain technology in healthcare. Int. J. Adv. Sci. Res. Eng. **4**(5), 154–159 (2018)
18. Oracle: Transformational Technologies Today How IoT, AI, and blockchain will revolutionize business. http://www.oracle.com/us/solutions/cloud/tt-technologies-white-paper-4498079.pdf
19. Cachin, C., et al.: Blockchain. Cryptography and Consensus, IBM Research (2017)
20. Sadiku, M.N.O., et al.: Smart contract: a primer. J. Sci. Eng. Res. **5**(5), 538–541 (2018)
21. Uddin, M.A., et al.: An efficient selector miner consensus protocol in blockchain oriented IoT smart monitoring (2018). https://www.researchgate.net/publication/329235620_An_Efficient_Selective_Miner_Consensus_Protocol_in_Blockchain_Oriented_IoT_Smart_Monitoring
22. Dwivedi, A.D., et al.: A decentralized privacy-preserving healthcare blockchain for IoT. Sensors **19**(2), 326 (2019)
23. Corea, F.: AI and blockchain. In: Corea, F. (ed.) An Introduction to Data. SBD, vol. 50, pp. 69–76. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-04468-8_11
24. Alasadi, S.A., Bhaya, W.S.: Review of data preprocessing techniques in data mining. J. Eng. Appl. Res. **12**, 4102–4107 (2017)
25. Ali, M.S., Dolui, K., Antonelli, F.: IoT data privacy via blockchains and IPFS. In: Proceedings of the 7th International Conference on the Internet of Things. ACM, New York (2017)
26. King, S., Nadal, S.: PPCoin: peer-to-peer crypto-currency with proof-of-stake, vol. 19 (2012). https://decred.org/research/king2012.pdf
27. Bitfinex: The world Largest Cryptocurrency platform. https://www.bitfinex.com
28. Kiktenko, E.O., et al.: Quantum-secured blockchain. Quantum Sci. Technol. **3**(3), 1–7 (2018)
29. Ellul, J., Pace, G.J.: AlkylVM: a virtual machine for smart contract blockchain connected Internet of Things. In: Proceedings of the 9th IFIP International Conference on New Technologies, Mobility and Security, pp. 1–4 (2018)
30. Ben-Sasson, E., et al.: Zerocash: decentralized anonymous payments from bitcoin. In: Proceedings of IEEE Symposium on Security & Privacy, pp. 459–474 (2014)