Int. J. Appl. Math. Comput. Sci., 2022, Vol. 32, No. 3, 403–413
DOI: 10.34768/amcs-2022-0029

A HOLISTIC STUDY ON THE USE OF BLOCKCHAIN TECHNOLOGY IN CPS AND IoT ARCHITECTURES MAINTAINING THE CIA TRIAD IN DATA COMMUNICATION

ANIRUDDHA BHATTACHARJYA [a]

[a]Department of CSE
Koneru Lakshmaiah Education Foundation
Vaddeswaram, AP, India
e-mail: abthuee@kluniversity.in

Blockchain-based cyber-physical systems (CPSs) and the blockchain Internet of things (BIoT) are two major focuses of the modern technological revolution. Currently we have security attacks like distributed denial-of-service (DDoS), address resolution protocol (ARP) spoofing attacks, various phishing and configuration threats, network congestion, etc. on the existing CPS and IoT architectures. This study conducts a complete survey on the flaws of the present centralized IoT system's peer-to-peer (P2P) communication and the CPS architecture's machine-to-machine (M2M) communication. Both these architectures could use the inherent consensus algorithms and cryptographic advantages of blockchain technology. To show how blockchain technology can resolve the flaws of the existing CPS and IoT architectures while maintaining confidentiality, integrity, and availability (the CIA triad), we conduct a holistic survey here on this topic and discuss the research focus in the domain of the BIoT. Then we analyse the similarities and dissimilarities of blockchain technology in IoT and CPS architectures. Finally, it is well understood that one should explore whether blockchain technology will give advantages to CPS and IoT applications through a decision support system (DSS) with a relevant mathematical model, so here we provide the DSS with such a model for this purpose.

Keywords: CPS, BIoT, blockchain, IIoT, DDoS, ARP spoofing, M2M, P2P, CIA triad.

1. Introduction

The creator of the initial blockchain network in 2008 was Satoshi Nakamoto (Nakamoto, 2008). The architectural and development improvement of the blockchain was conducted in this work; for example, the clients' sign was not required nor was the users' sign. Another prominent contribution was network system design and configuration for the bitcoin cryptocurrency (Nakamoto, 2008) and the bitcoin network was up to 100 GB in January 2017. The traditional cloud (Xu, 2012) is less secure, while blockchain (Aste *et al.*, 2017; Bailis *et al.*, 2017) has much more security and it is an irrevocable tamper-proof digital ledger. Moreover, practical alterations of the records are impossible, resulting in more accurate entries. Blockchain (Baliga, 2017; Bano *et al.*, 2017; Banerjee *et al.*, 2018) is a decentralized data structure. It does not required any central data hub. Another advantage is that no third party will be able to access it. P2P transactions (Li *et al.*, 2018) are a very unique benefit of blockchain technology to be used in CPSs and the IoT without any intermediary and no central hub doing so, despite each node confirming the transaction. This distributed architecture also enhances the robustness of the all-inclusive blockchain network system. But this distributed system does not hamper the operation of the all-inclusive network system caused by the fault of some nodes. The self-healing toughness with anti-attack and data confidentiality features make this technology good for CPS (Banerjee *et al.*, 2018; Monostori *et al.*, 2016; Bhattacharjya *et al.*, 2019a; 2019b; 2019c; 2019d) and IoT architectures (Lee *et al.*, 2015; IOTA, 2017a; Bhattacharjya *et al.*, 2019b; 2019c; 2019d; 2019e).

In fact this blockchain technology is like a bundled technology with its inherent consensus algorithms, end-to-end (E2E) secure protocols and distributed data storage (Chowdhury *et al.*, 2019). These properties are perfectly needed for CPS and IoT architectures. For example, suppose these architectures' information

validation processes are distributed across the network of peers using blockchain technology; in that case, we can eliminate all the disadvantages of the centralized architecture of the present M2M communication in CPS and IoT architectures. So blockchain technology has certain advantages for using it in the present CPS and IoT architectures. Here we discuss in detail how this blockchain technology can be useful for the present CPS and IoT architectures.

We have a detailed discussion on the disadvantages of the present centralized system in CPS and IoT architectures in this paper. These centralized cloud based CPSs and IoT systems can perform better in terms of security, trustworthiness, P2P networking and efficiency especially. A single-point failure is a big problem for cloud based centralized CPS and IoT systems; with integration of blockchain technology in existing CPSs and IoT systems, we will never have single-point failures.

This paper is a holistic study on how, by using blockchain technology in CPS and IoT architectures, we can resolve the disadvantages of centralized systems (Sethi and Sethi, 1990) with maintaining the CIA triad of data communication in all peers.

Section 2 describes the benefits of using blockchain technology in CPS architectures. Section 3 describes how blockchain technology can be used in the present CPS architectures. Section 4 describes the problems of the present centralized IoT systems. Section 5 describes blockchain technology's advantages over the present IoT systems. Section 6 describes the future research on blockchain technology's use in the IoT. Section 7 describes the similarities and dissimilarities regarding blockchain technology in the IoT and CPSs. Section 8 describes blockchain technology's suitability in specific architectures. Section 9 describes a mathematical model based DSS for getting the decision if the use of blockchain technology in the real-time implementations is going to benefit us or not. Section 10 describes the major problems that still exist with blockchain technology in CPSs and IoT systems. Finally, Section 11 is conclude the paper.

2. Benefits of using blockchain technology in CPS architectures

We have a detailed review of security attacks like DDoS, ARP spoofing attacks, various phishing and configuration threats, network congestion, etc. on the present CPS architectures (Zissis and Lekkas, 2012). These attacks harm the CIA triad of data and have very harmful impacts on the functioning of any of these systems. Currently, these CPS architectures are managing these threats with a centralized, client-server-based architecture with all the control and power with the centralized system, so a well understood matter is that if the centralized system collapses, all the privileges will be zero. So, we need a new kind of secure communication.

We have found that a Petri net-based model for the CPS (Wisniewski *et al.*, 2019) has some limitations like verification and optimization, etc. However, at the same time, it has unique features (Wisniewski *et al.*, 2020) like reduced faults with the use of this model along with easiness and a proper correction model.

In this paper, one of the highlighted areas is how this blockchain technology (Underwood, 2016) can be used in CPSs for maintaining the CIA triad of data communication. In this research paper, we focus more and more on how the CIA triad can be maintained in the data communication of CPSs. So, for M2M communication in CPSs, the security protocols are not able to resolve the inter-communications among different heterogeneous devices in CPSs. So, security issues of M2M communication are big problems that blockchain technology can resolve.

In the work of Li *et al.* (2018) a five-level architecture called 5C-CPS was anticipated for evolving CPSs specifically for the manufacturing industries.

There are many researchers who have shown us that blockchain technology's unique features can be much more beneficial for CPS and IoT applications. Here we discuss them one after another.

Swan (2015) demonstrated three utmost fit distributed ledgers for real-time applications of the IoT and CPSs. These are hyperledger fabric (Hyperledger, 2017), IOTA (IOTA, 2017b) and Ethereum (Trón and Lange, 2015; Pustišek and Kos, 2018). In that research the profound features of using blockchain technology in the IoT (termed the BIoT) and CPSs were described and can be highlighted as follows: immutable (hash functions) (Sigrid and Samman, 2016), decentralized operation, no intermediaries (consisting of self-executable algorithms like Smart Contract (Palma *et al.*, 2019)), transparency, anonymity (in this technique public and private keys can be used for interaction without any private information), distributed operation and, last but not least, authenticity.

A very well-known fact is that the most important part of all blockchain systems (Marc, 2016; Michael *et al.*, 2016) are their underlying consensus algorithms (Sigrid and Samman, 2016; Cachin and Vukolic, 2017; Sankar *et al.*, 2017; Wang *et al.*, 2019). The algorithm decides on the whole architecture or system efficiency, scalability and security mainly. So, in the past, to highlight the limits of these different blockchain systems, numerous existing along with several novel consensus algorithms have been introduced (Baliga, 2017; Bano *et al.*, 2017; Cachin and Vukolic, 2017). We actually need to conduct a deep study on several aspects of these blockchain consensus protocols. Now a major problem is that the present analyses of consensus algorithms are not wide-ranging. Those studies are not encompassing all the properties of the algorithms and did not analyze numerous major

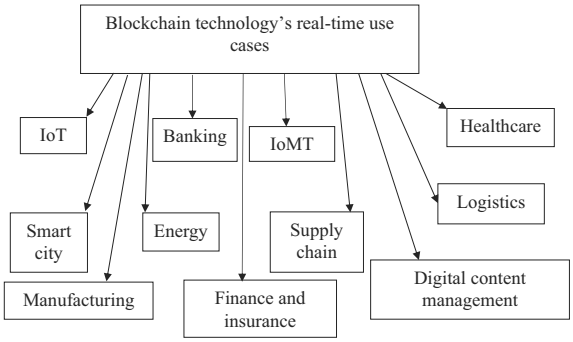

Fig. 1. Blockchain technology's usability in real-time applications.

blockchain consensus algorithms as per their scopes.

We have three kinds of blockchain consensus strategies (Baliga, 2017; Bano *et al.*, 2017; Cachin and Vukolic, 2017): decentralized/permissionless (Bitcoin, Ethereum) (Trón and Lange, 2015; Pustišek and Kos, 2018), somewhat decentralized (Ripple, Stellar), and consortium/permissioned (byzantine fault tolerance (BFT) consensus) (Sigrid and Samman, 2016; Sankar *et al.*, 2017; Wang *et al.*, 2019). We also have consortium consensus which is still in the developing stage by Juno/Kadena, Iroha, Hyperledger Fabric (includes PBFT protocol), Axoni, Tendermint, JPMC Quorum, Chain and others. Also HoneyBadgerBFT and many existing BFT libraries employ blockchain—the works at the University of Lisbon and John Hopkins University (Prime, 2017) as well as BFT-SMaRT are still evolving.

Blockchain technology has certain advantages to be used in financial technology and it has the ability and momentous prospective to sustainably upkeep not only the Industry 4.0 initiative (evaluation from Industry 1.0, 2.0, 3.0) (Lee *et al.*, 2014; 2015; Yang, 2017; Vora *et al.*, 2018), but it is able to resolve the issues for the Industry 4.0 initiative. The use of blockchain technology in real-time applications is widespread now; a simplified summary of where blockchain is in use is shown in Fig. 1.

Past works (Cachin and Vukolic, 2017; Bano *et al.*, 2017) were novel in this focus area. Cachin and Vukolic (2017) showed high some specialty of distributed systems along with the consensus part, and their main highlights were also on the consensus algorithm of blockchain systems, but as a matter of fact these were not in public domain. But Bano *et al.* (2017) highlighted different aspects and focused on consensus algorithms of public and private blockchain systems.

Another novel work was done by Wang *et al.* (2019), who provided a comprehensive and in depth review of diversified aspects of consensus, mining, and blockchain.

Xiao (2016) suggested a four-layer architecture consisting of consensus, mining, propagation, and semantic layers. But it is evident that the four-layer architecture does not have suitable grouping of functionalities, which is needed (consensus and mining should be in one layer only as mining can be well-thought-out as an inherent part for accomplishing consensus). So, a solution to these problems can be a four-layer architecture with the following components:

(i) network layer,

(ii) consensus layer,

(iii) application layer,

(iv) meta-application layer.

Here the meta-application layer will offer an overlay above the application layer for exploring the semantic representation of a blockchain architecture for different works in different application areas. An example can be bitcoin, which can have many more real-time implementation domains, such as the decentralized naming system (DNS) (Namecoin, 2018; Fromknecht *et al.*, 2014). The decentralized public key infrastructure (PKI) certcoin (Fromknecht *et al.*, 2014) can be another example.

If we see the layers of blockchain architectures, we can find that these layers have several functionalities like collection of the transactions, propagation of blocks, mining, accomplishment of the consensus and upholding the ledger for its underlying cryptocurrencies (Mukhopadhyay *et al.*, 2016), and many more. All these functionalities can be clustered together according to their jobs by using specific layers alike TCP/IP. In past works we have seen design of a blockchain system by using a layered approach (Joichi, 2016; Xiao, 2016). As per these works the design is much more modular and can be maintained easily.

Recently blockchain technology has been proliferating in academia, industry (Mukhopadhyay *et al.*, 2016; Baliga, 2017; Bano *et al.*, 2017; Cachin and Vukolic, 2017), and government sectors in the world. This technology has numerous application domains almost in all spheres of the human lives. This technology's potential has made the research and industry communities explore its usefulness in different application domains. So, now we have a plenty of blockchain systems omnipresent in several domains with real-time use.

Presently security and privacy of blockchain scenarios are in four directions (Mukhopadhyay *et al.*, 2016; Baliga, 2017; Bano *et al.*, 2017; Cachin and Vukolic, 2017):

(i) transactional privacy,

(ii) contract privacy,

(iii) accountability & non-repudiation and

(iv) auditability & transparency.

But the problem is that many of these need advanced cryptographic protocols.

We have RapidChain for better scaling in the blockchain and we have Proof of Luck for efficiency in the blockchain consensus protocols arena. But an in-depth study or major consensus algorithms is needed for their future case specific applicability. These algorithms (Mukhopadhyay *et al.*, 2016; Baliga, 2017; Bano *et al.*, 2017; Cachin and Vukolic, 2017) are as follows: Proof of Activity, Proof of Stake Velocity, Proof of Burn (PoB), Proof of Believability, Proof of Existence, Byzantine Fault Tolerance (BFT), Proof of Work (PoW), Proof of Stake (PoS), Delayed Proof-of-Work (dPoW), Delegated Proof-of-Stake (dPoS), Proof-of-Weight, Proof of Reputation, Proof of History, Proof of Time, Ouroboros, Proof of Retrievability, Elapsed Time, Proof of Identity, Delegated Byzantine Fault Tolerance (dBFT), RAFT, Stellar Consensus, Proof-of-Authority, Proof of Space, Directed Acyclic Graphs, Proof of Importance, Tangle (IOTA) (IOTA, 2017a; 2017b), Hashgraph, Holochain, Block-Lattice (Nano), SPECTRE, ByteBall, etc.

3. How blockchain technology can be used in the present CPS architectures

We know that most important properties of blockchain technology are the irreversibility of the chain state, immutability and data (transaction) persistence, distributed data control, distributed consensus on the chain state, data provenance and accountability and transparency. The semantic representation of a blockchain system can be performed by the application layer. The third layer is the consensus layer, which facilitates the distributed consensus technique that fundamentally makes the blocks in the order; this is the main job of the consensus layer. The proof protocol, e.g., POW and POS, validates every single block, which at the end makes the architecture capable of accomplishing the obligatory consensus. The network layer is responsible for managing network functionalities like connecting the underlying P2P network. It is also responsible for connecting others in the network with the help of the underlying networking protocol. It is also responsible for broadcasting the present status of the blockchain to all connected nodes newly joined. Propagating, along with receiving the transactions and blocks is also the responsibility of the network layer. These are the main responsibilities and apart from these many responsibilities are there.

In CPS architectures' and M2M-security systems based on blockchain technology, we have three areas:

(i) public network area,

(ii) device area,

(iii) private area.

We know that the public network area in the industrial IoT (IIoT) forms communication platforms for all machines. The public network area and the private area are connected by the device area as a channel. The private area is responsible for beginning and storing the blocks of the communication procedure among all the machines. This area is also responsible for saving the data of the communication procedure; it takes the external query, or obtains outside but related data by querying.

In the case of designing machine-equipment blockchain (Monostori *et al.*, 2016) in the public network area for devices that have to be replaced due to a fault, the new devices must be connected to the production line via the registration procedure. In this procedure, by use of a specific algorithm, for example, SHA256, the new device finds a private key. After this procedure, the next process produces a public key using a different algorithm, for instance Secp256K1. Then the digital certificate is sent by the new device to the public network area for getting registered. After approval it is registered. So the next step is for the public network to produce an equivalence between the certificate and its identity, and after that it will save the public key of that device in the key pool. Here in this process the device joins the network as a new blockchain in the machine-equipment blockchain (M-EB). In the case of designing the communication blockchain (CB) in the private area, as in the public domain the information of the communication technique can be available, so these private sectors guarantee that it is tamper-protected.

We know that M2M systems are always needed to be extensible, and being dynamic is the inherent quality of the M2M system. Now, in the above case, like the use of blockchain technology in a CPS with its M2M systems, the blockchain is used to maintain the option of extension which is necessity of M2M systems of CPSs (Monostori *et al.*, 2016). So, IIoT platforms ought to identify the IDs of the new devices and then the devices needed to be timestamps. As part of the procedure in this system, as a new block, these devices will be put in the blockchain of devices. For example, in one IIoT platform, there are 1 to m processes in the blockchain for device and 1 to n processes in the blockchain for material; as an outcome, the working architecture of the blockchain based IIoT for creating device and material as well as the communication blockchain will look as shown in Fig. 2.

So, it is clear that some inherent features of blockchain technology make CPS architectures safer and efficient, and financially (Yu *et al.*, 2018) beneficial. These features are the decentralized architecture with a

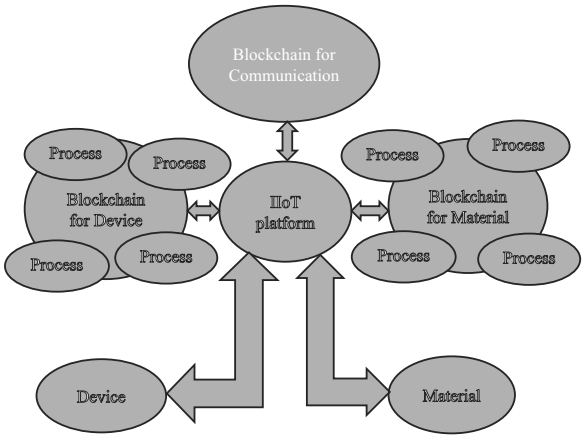

Fig. 2. Working architecture of the blockchain based IIoT for creating devices as well as material and communication blockchain.

unique trust and transparency model; efficiency comes in with distributed P2P architectures' uniqueness and also as this technology's cryptographic approaches protect CPS architectures from many attacks like DDoS, ARP spoofing attacks, various phishing and configuration threats, network congestion, etc, resulting in huge financial savings (usually the organizations pays huge amounts for damages done by these attacks on CPS architectures still now). The system of system (SOS) of CPS architectures, which is actually a cross-system, cross-platform interconnected and interpretable, giving the perfect opportunity of configuration, scheduling and execution. So, blockchain technology make these much more secure with efficiency.

As we have found, all these works have lots of shortcomings. In some cases, the features based on which consensus algorithms were studied practically are not comprehensive. In past works, in some cases, lots of consensus algorithms and internal mechanisms used with those consensus algorithms have not been investigated, but those algorithms are used in today's cryptocurrencies (Mukhopadhyay *et al.*, 2016). Additionally, these surveys and research do not discuss one of the main matters, that is, the interrelation among blockchain systems and consensus algorithms used in those systems.

4. Problems of the present centralized IoT systems

It is very well known that these days we have security attacks like DDoS, ARP spoofing attacks, various phishing and configuration threats and network congestion, etc. on the present CPS and IoT architectures used in Industry 4.0 applications. These attacks are very dangerous towards maintaining the CIA triad of the data. Also, as a whole, these attacks can make significant impacts on smooth functioning of these systems. Industry 4.0 applications have problems in dealing with the CIA triad along with access control and authorization. The reason is the fact that we are increasing the automation of these systems, so more security breaches are going on, and new kinds of cyber-attacks are increasing resulting huge financial losses.

In the present cloud based (Xu, 2012; Zissis and Lekkas, 2012) centralized server/client model of the IoT, identification, authentication and connection ought to be through cloud based servers with huge capacity. The connection between devices ought to be made through the cloud, in spite of their geographical distances. The major problem is that this centralized cloud based system is unable to fulfil the ever increasing necessities of the robust IoT ecosystems of the future.

The present major problems of centralized IoT architectures (Xu, 2012; Zissis and Lekkas, 2012) are as follows:

1. No specific and proper tutorials and helping data are there for the maintenance of the life cycle (Xu, 2012).
2. No specific and proper tutorials and helping data are there for the controlling of the way-out for IoT devices (Zissis and Lekkas, 2012).
3. Privacy is a very complex matter and presently in many cases it is not sufficient (Xu, 2012).
4. The ever expanding nature of the IoT is worrisome in the case of scalability issues (Zissis and Lekkas, 2012).
5. IoT devices and platforms are unprotected from physical tampering, so new innovations are needed against proper protection for physical tampering (Xu, 2012).
6. No solutions are there for impersonating the connected things in IoT networks (Zissis and Lekkas, 2012).
7. No solutions are there for the protection of denial-of-sleep attacks (Zissis and Lekkas, 2012).
8. In the future, uniquely sophisticated security approaches might not be able to provide security for the present connected things as they still use old processors and operating systems (Zissis and Lekkas, 2012).

5. Blockchain technology's advantages for the present IoT systems

Here we describe the technical benefits of blockchain technology to be used in the IoT, the so-called BIoT. The

advantages are follows.

One of inherent novel abilities of blockchain technology is its security features. The database cannot be altered, only extended, and records stored earlier cannot be altered; generally only can be done with very high cost. In real time, cryptographic algorithms used by the blockchain will enhance the privacy of consumer data. Public audits, consensus mechanisms and timestamps are used for storing the data in an immutable manner. This enables the architecture to maintain the CIA triad.

We know that the unique structural distributed database of blockchain technology, which is data storage for all the nodes, is one of the prominent features of blockchain technology. An excellent feature is that this structural distributed database stores the data in an encrypted form validated by using several checks for example, the Merkle hash tree (MHT) and elliptical curve cryptography (ECC). Also research is going on the PKI type of cryptography technique for increasing the security of blockchain-based data management.

As we have discussed earlier, for many reasons a centralized system is one of the main disadvantages of the present IoT architectures. Blockchain by its inherent ability is able to register and keep the data of the registrations of the IoT's registered connected devices. So, with blockchain technology, smart devices work very smoothly where there is no necessity for the centralized authority.

In blockchain networks, the blocks along with the transactions stored in them are visible to everyone; only the actual content of personal transaction cannot be visible to others as private keys protect these transactions. So, it can be said that public availability of the transactions in blocks and visibility of blocks are one of the best advantages of the BIoT.

Maintaining all the transactions' trusted ledger is a unique advantage of blockchain technology. So, it is well understood that the trustworthiness is a unique advantage for using blockchain technology in the IoT level's huge scalability (billions connected devices). Blockchain technology is able to provide verifiability of a distributed ledger in a decentralized network, which is a significantly good way for trustworthiness in the IoT. Immutability is also another significant contribution.

Blockchain technology can be very much useful for tracking billions of devices (connected), resulting in faster transactions and coordination within devices; so, in other words, it can contribute towards major savings for IoT industry manufacturers.

Blockchain technology creates trustless P2P messaging a reality and has a unique contribution to financial services in the globe through cryptocurrencies, for example, bitcoin, facilitating guaranteed P2P payment services deprived of the need for third-party brokers. So, Fintech has smooth running without a third-party.

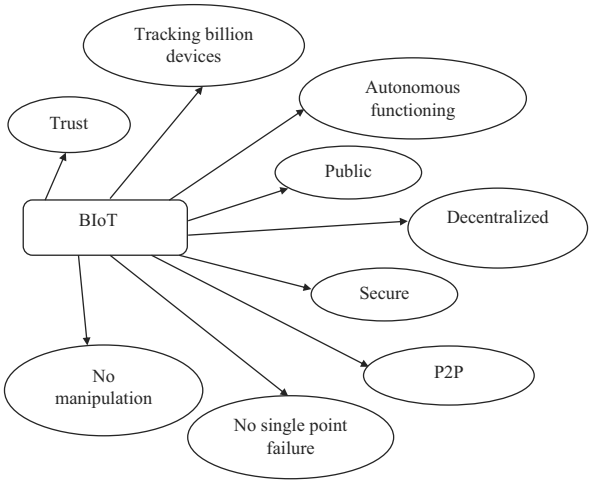

Fig. 3. Advantages of blockchain technology in the IoT.

Blockchain is a public ledger of all transactions, upheld by dissimilar decentralized nodes. So, it is well understood that for accepting the transactions all the participants need to reach for a consensus, so trustworthiness is the main inherent quality of this blockchain technology. Cryptographic keys and immutable ledgers are linked with all transactions in blockchain networks. So, it is obvious that the attackers cannot tamper or remove the stored information. This ability is a novel inherent feature of blockchain technology and it is obligatory for many networked architectures. So, it is well understood that IIoT applications' compliance and regulatory necessities are by this advantage of blockchain technology. The blockchain gives us a decentralized and trust-less P2P network. Here it is unnecessary for peers to have a trusted intermediary inter-communications. The peers do not necessitate mutual trust among them due to the fact that a central authority does not coordinate the blockchain network and all the transactions are not only verified but also validated by a consensus among the peers.

Blockchain technology's network is a decentralized P2P network, so, like a centralized system, it is not at all vulnerable to the well-known single point failure.

The ledger used in blockchain technology does not exist in any single location, so manipulation by a malicious entity is impossible. Hence, man-in-the-middle attacks cannot happen here.

Summarized advantages of using blockchain technology in the IoT are shown in Fig. 3.

It is clear that the blockchain Internet of things (BIoT) can bring revolutions in the recent era.

6. Future research on blockchain technology's use in the IoT

The IoT is the present and future of the modern technological and industrial revolution, as we have discussed in our past works (Bhattacharjya *et al.*, 2019a; 5019b; 2019c; 2019d; 2019e; 2019f). We have also discussed the differences and similarities of blockchain technology (Bhattacharjya *et al.*, 2019a). Blockchain technology has some pitfalls, which are as follows:

1. CPU-intensive computations, including mining, encryption, and decryption, are inherent procedures of blockchain technology. Being a growing ledger, maintaining and storing are significant challenges of this technology. The solution can be cooperative processing of the transactions, storing the ledger, and upholding the blockchain network.
2. All the various IoT devices are unable to execute the same encryption algorithm with the same speed, so processing power and computing capabilities issues are there in the blockchain-based IoT ecosystem.
3. Presently, very few legal or compliance precedents are there in the world to abide by, so IoT industrialists and service enablers are fewer in this domain.
4. As we know, the digital ledger need to be saved in blockchain nodes themselves, and the ledger size is ever increasing in practical IoT applications. However, as sensors in IoT architectures always have less storage capacity, they cannot have ample storage. So, storage capability is an issue in the case of large IoT architectures.
5. The size of the blockchain ledger is becoming bigger and bigger. This is paving the way for the necessity for a centralized record management system, which can replace the advantages of blockchain technology's distributed nature. So, scalability is a future disadvantage.
6. Skilled people are needed to run these BIoT systems presently; we have a shortage of skilled people who understand the working principles of BIoT structures.

So, the fact is the BIoT has to deal with many difficulties these and coming days, including the decentralized system of security, the intensive computational requirements of the blockchain and the less computing power and small storage capability of IoT devices. Along with these, the trust and ad-hoc connectivity are a problem, too, along with other issues.

Authentication, access control and decentralized trust for the BIoT should be the future research focus. Also, along with decentralized control, we ought to have querying and permissions services, low latency, and high throughput. Summarized disadvantages of using blockchain technology in the IoT (BIoT) are shown in Fig. 4.

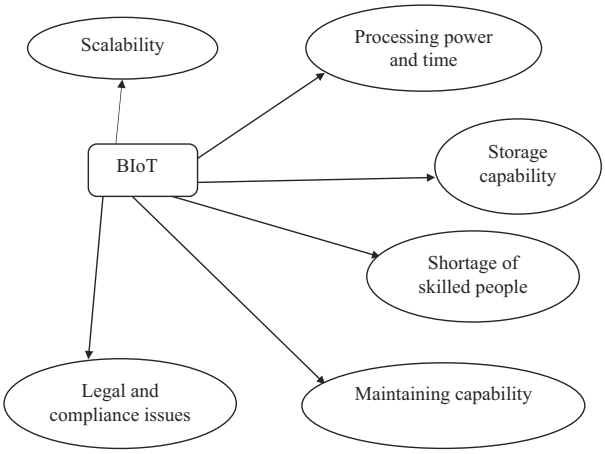

Fig. 4. Disadvantages of blockchain technology in the IoT.

7. Similarities and dissimilarities in the use of blockchain technology in the IoT and CPSs

It is very clear that blockchain technology will be in use for several IoT and CPS application specific architectures in near future, due to its decentralized nature with secure and P2P communications with other advantages as discussed in Sections 2 and 5. Figure 3 adds more clarity also. Now the matter is when we are trying to use blockchain technology in both IoT and CPS architectures, then we need to know what are these architectures' similarities and dissimilarities. So if we can map the similarities and dissimilarities in using blockchain technology in the IoT and CPSs, then it can be summarized as shown in Fig. 5. This figure gives technical details in a pictorial way about what is common for both IoT and CPS architectures, and also it depicts dissimilar needs of IoT and CPS architectures. So when we are talking about using blockchain technology in both CPS and IoT architectures, this will be very helpful for understanding the technical facts.

8. Blockchain technology's suitability in specific architectures

Based on our previous discussion of future research on blockchain technology's use in the IoT, we have found that many architectures are suitable for using blockchain technology for resolving their existing problems related

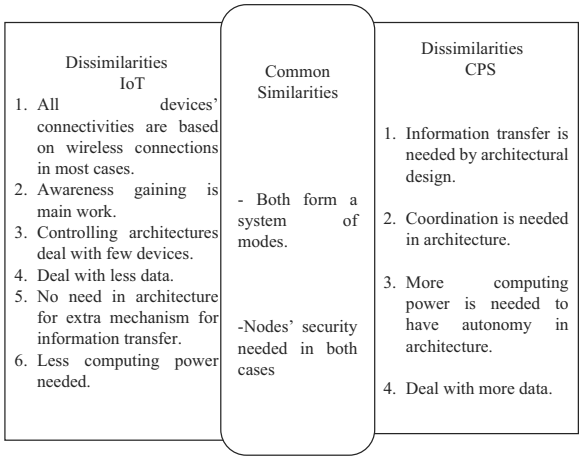

Fig. 5. Similarities and dissimilarities in using blockchain technology in the IoT and CPSs.

to security and centralized systems. Now we can classify, based on the above sections, which architecture is suitable for the use of blockchain technology:

Hyperledger Fabric (Hyperledger, 2017); IOTA (IOTA, 2017b); and Ethereum (Trón and Lange, 2015; Pustišek and Kos, 2018) are all suitable distributed digital ledger systems that can be used in CPS and IoT applications to resolve security problems and disadvantages of a centralized system. Hyperledger Fabric is very suitable for IoT and CPS architectures for its features like being immutable (hash functions), decentralized, requiring no intermediaries (as consisting of self-executable algorithms like, e.g., Smart Contract), transparent, anonymous (as in this technique public and private keys can be used for interaction without any private information), distributed and authentic.

It is well understood that bitcoin can have several application domains like DNS, such as Namecoin (Namecoin, 2018), which is a decentralized naming system, and Certcoin (Certcoin, 2019), which is a decentralized public key infrastructure (PKI), etc. All these are secure and decentralized, replacing all disadvantages of centralized systems.

IIoT architectures can use blockchain technology, as discussed in Section 3. Figure 2 shows how a practical model will work.

The BIoT is a new terminology these days as inherent qualities of blockchain technology can replace many disadvantages of the present centralized IoT systems. For example, in Section 5, it is discussed in detail why blockchain technology can be revolutionary in the present IoT architectures.

9. Mathematical model based DSS for decision of advantage

Now the question is how we can judge that our application of CPS and IoT architectures can be beneficial. We already know that a major cost and performance trade-offs are there at the time of using the decentralized database like the blockchain. But whether the application of CPS and IoT architectures will be beneficial or not is the decision that will be taken by the DSS. We have the model presented by Box (1979), who says that all models are incorrect but some are useful. So, the mathematical model for making a decision if the use of blockchain technology is beneficial or not can be as

$$v = \frac{1}{M}\sum_{x=1}^{N} s_x w_x, \tag{1}$$

where v is actually the overall score, w_x is the weight for the metric which is considered, $0.0 \leq w_x \leq 1.0$, M is the number of metrics which are used, $M > 1$, and $s_x$is the measuring factor for the metric under consideration, $0.0 \leq s_x \leq 1.0$.

The output of this model can evaluate the overall value of v, using cost-benefit exploration principles (Robert and Alan, 1978), and it can be concluded if a specific application can benefit from the use of a decentralized database (blockchain technology). Here s, the value of the measuring factor, is in general a complex function of the specific metric considered, for example, m. So this way with execution of the complex mathematical analysis works to decide if the decentralized database (blockchain technology) is beneficial for a particular application of CPS and IoT architectures.

Recently, Lee *et al.* (2019) described a unified three-level blockchain system for blockchain technology's use in cyber-physical production systems (CPPSs) towards a vast implementation of Industry 4.0.

10. Major problems still exist with the use of blockchain technology in CPSs and IoT systems

Major problems still exist with the use of blockchain technology in CPSs and IoT systems such as the following.

Blockchain technology based architectures were hacked in the past years, e.g., the Bitfinex attack in August 2016 and the Ethereum attack in June 2016. If bitcoin and private keys are put in safekeeping on a device, which is connected by the Internet, then any hacker can steal those keys. If the private keys are stolen, the security of the blockchain and the encryption technique are nothing to hackers. So, confidentiality and integrity of data of these systems and overall functioning of CPSs and IoT systems

should not be hampered due to network congestion, phishing and configuration threats, ARP spoofing attacks, data rate alteration, and DDoS, etc.

We have found that the lack of centralized control, multiple attack surfaces, context-aware and nature of risks as per situations, heterogeneity in device resources and security vulnerabilities which are already identified in connected devices like smart locks to vehicles, etc. are huge problems currently.

Optimizing the resources of CPSs and IoT systems are essential, as in the case of high level and complex security methods, the resource constrained devices used in CPSs and the IoT are not at all good to be used in that scenarios.

We know that the data in a blockchain can be viewed by any members in the corresponding blockchain, so any moment data privacy can be a big issue.

User privacy is the main matter also to be protected in all transactions while exposing the diverse types of data during transactions and operations.

We know that the growth of transactions registered into a blockchain is totally unpredictable; as a result, an indistinguishability exists about the blockchain platform on the scalability matter relating to the increase of the amount of business transactions on this platform.

The malware has proven to be vulnerable to this technology. A demonstration was there on the vulnerability by using the POC software by the Interpol at Black Hat Asia in March 2015. Researchers have also demonstrated that botnets (for example, Fujacks Trojan, a botnet backdoor) have the capability to send messages by using the bitcoin network.

We know that centralized methods are inappropriate for CPSs and IoT systems as the single point of fail use and many-to-one mode are big concerns to make the whole systems failure. But the reduced scalability of the whole system is a big problem.

Lots of international banks have raised alarms about the security level of cryptographic algorithms which are in use in blockchain-based transactions; also they have raised alarms about blockchain based transactions' confidentiality and how these systems can secure private keys used in those transactions.

Any false transactions can be approved by other nodes in blockchain transactions, which could be a huge loophole resulting in fraudulent activity.

Now we have less structured blockchain governance, which could be dangerous for retaining data in a blockchain. As to date, we do not have common governing regulatory for handling blockchain protocols.

11. Conclusions

As discussed in the paper, blockchain technology has unique advantages for centralized CPS and IoT architectures. Blockchain technology can benefit financially by securing all transactions and protecting the above-said attacks. The present system of CPS and IoT architectures is vulnerable to faults in centralized control, and due to such control, it is not efficient, either. However, blockchain technology's distributed secure system can make these CPS and IoT architectures much more secure and efficient. So, a single-point failure of centralized systems will never happen in these systems when using blockchain technology.

Only very large connected devices in IoT systems cannot be tackled by blockchain technology, as it cannot scale the number of devices connected in the system. So, it is a well-understood fact that the computational and storage space requirements of this technology's participants are extensive. So, in 2017, to resolve these disadvantages, we got Tangle technology (works on a directed acyclic graph defined as Tangle) for authentication of transactions and for IoT-related applications' security (Tangle, 2018). All transactions have to validate two earlier transactions in this Tangle network by executing a POW. So, it is well understood that Tangle is more decentralized than blockchain technology. We can say that blockchain may connect many IoT devices to a single gateway, and after that the gateway itself ought to be part of the blockchain network as a member. So, as discussed in the future research section, we need a new model to resolve those pitfalls. The above mathematical approach-based DSS will give us an idea of the advantages of blockchain technology in CPS and IoT applications.

Acknowledgment

This work is supported by the Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India, and the open access fee is partially supported by the Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India, through an incentive.

References

Aste, T., Tasca, P. and Matteo, T.D. (2017). Blockchain technologies: The foreseeable impact on society and industry, *Computer* **50**(9): 18–28, DOI: 10.1109/MC.2017.3571064.

Bailis, P., Narayanan, A., Miller, A. and Han, S. (2017). Research for practice: Cryptocurrencies, blockchains, and smart contracts; hardware for deep learning, *Communications of the ACM* **60**(5): 48–51.

Baliga, A. (2017). Understanding blockchain consensus models, `https://www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Blockchain-Consensus-Models.pdf`.

Banerjee, M., Lee, J. and Choo, K.K.R. (2018). A blockchain future for Internet of things security: A position paper, *Digital Communications and Networks* **4**(3): 149–160.

Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., and Danezis, G. (2017). Consensus in the age of blockchains, *arXiv:* 1711.03936, https://arxiv.org/abs/1711.03936.

Bhattacharjya, A., Zhong, X. and Li, X. (2019a). A lightweight and efficient secure hybrid RSA (SHRSA) messaging scheme with four-layered authentication stack, *IEEE Access* **7**: 30487–30506, DOI: 10.1109/ACCESS.2019.2900300.

Bhattacharjya, A., Zhong, X., Jing, W. and Li, X. (2019b). Security challenges and concerns of Internet of things (IoT), *in* S. Guo and D. Zeng (Eds), *Cyber-Physical Systems: Architecture, Security and Application,* Springer, Cham, pp. 153–185.

Bhattacharjya, A., Zhong, X., Jing, W. and Li, X. (2019c). Secure IoT structural design for smart cities, *in* D.B. Rawat and K.Z. Ghafoor (Eds), *Smart Cities Cybersecurity and Privacy*, Elsevier, Amsterdam, pp. 187–201.

Bhattacharjya, A., Zhong, X., Jing, W. and Li, X. (2019d). Present scenarios of IoT projects with security aspects focused, *in* M. Farsi *et al.* (Eds), *Digital Twin Technologies and Smart Cities: Internet of Things (Technology, Communications and Computing),* Springer, Cham pp. 95–122.

Bhattacharjya, A., Zhong, X., Jing, W. and Li, X. (2019e). CoAP—Application layer connection-less lightweight protocol for the Internet of things (IoT) and CoAP-IPSEC security with DTLS supporting CoAP, *in* M. Farsi *et al.* (Eds), *Digital Twin Technologies and Smart Cities: Internet of Things (Technology, Communications and Computing)*, Springer, Cham, pp. 151–175.

Bhattacharjya, A., Zhong, X., Jing, W. and Li, X. (2019f). A secure hybrid RSA (SHRSA)-based lightweight and efficient personal messaging communication protocol, *in* M. Farsi *et al.* (Eds), *Digital Twin Technologies and Smart Cities: Internet of Things (Technology, Communications and Computing)*, Springer, Cham, pp. 191–212.

Box, G.E.P. (1979). Robustness in the strategy of scientific model building, *in* R.L. Launer and G.N. Wilkinson (Eds), *Robust Statistics*, Academic Press, Cambridge, pp. 201–236, DOI: 10.1016/B978-0-12-438150-6.50018-2.

Cachin, C. and Vukolic, M. (2017). Blockchains consensus protocols in the wild, *arXiv:* 1707.01873, https://arxiv.org/abs/1707.01873.

Chowdhury, M.J.M., Ferdous, M.S., Biswas, K.N., Chowdhury, N., Kayes, A.S.M., Alazab, M. and Watters, P. (2019). A comparative analysis of distributed ledger technology platforms, *IEEE Access* **7**: 167930–167943, DOI: 10.1109/ACCESS.2019.2953729.

Fromknecht, C., Velicanu, D. and Yakoubov, S (2014). CertCoin: A Namecoin based decentralized authentication system, *6.857 Unpublished Class Project*, MIT, Cambridge, http://courses.csail.mit.edu/6.857/2014/files/19-fromknecht-velicann-yakoubov-certcoin.pdf.

Hyperledger (2017). IBM blockchain based on Hyperledger Fabric from the Linux Foundation, https://www.ibm.com/Blockchain/hyperledger.

IOTA (2017a). IOTA Developer Hub, https://www.iota.org/get-started/for-developers.

IOTA (2017b). IOTA: A cryptocurrency for the Internet-of-things, https://iota.org/.

Joichi, I. (2016). The Fintech Bubble, *Joi Ito's Web,* DOI: 10.31859/20160614.1805.

Lee, J., Azamfar, M. and Singh, J. (2019). A blockchain enabled cyber-physical system architecture for Industry 4.0 manufacturing systems, *Manufacturing Letters* **20**: 34–39.

Lee, J., Bagheri, B. and Kao, H.A. (2015). A cyber-physical systems architecture for Industry 4.0-based manufacturing systems, *Manufacturing Letters* **3**: 18–23, DOI: 10.1109/ACCESS.2019.2900300.

Lee, J., Kao, H.A. and Yang, S. (2014). Service innovation and smart analytics for Industry 4.0 and big data environment, *Procedia CIRP* **16**: 3–8.

Li, Z., Barenji, A.V. and Huang, G.Q. (2018). Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform, *Robotics and Computer-Integrated Manufacturing* **54**: 133–144.

Marc, P. (2016). Blockchain technology: Principles and applications, *in* F.X. Olleros and M. Zhegu (Eds), *Research Handbook on Digital Transformations*, Edward Elgar Publishing, Cheltenham, pp. 225–253, DOI: 10.4337/9781784717766.00019.

Michael, C., Nachiappan, Pattanayak, P., Verma, S., Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin, *Applied Innovation* **2**: 6–10.

Monostori, L., Kádár, B., Bauernhansl, T., Kondoh, S., Kumara, S., Reinhart, G., Sauer, O., Schuh, G., Sihn, W. and Ueda, K. (2016). Cyber-physical systems in manufacturing, *International Academy for Production Engineering CIRP Annals* **65**(2): 621–641.

Mukhopadhyay, U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L. and Brooks, R. (2016). A brief survey of cryptocurrency systems, *14th Annual Conference on Privacy, Security and Trust (PST), Auckland, New Zealand*, pp. 745–752, DOI: 10.1109/PST.2016.7906988.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf.

Namecoin (2018). Namecoin: An experimental open-source technology, https://namecoin.org/.

Palma, L.M., Vigil, M.A.G., Pereira, F.L. and Martina, J.E. (2019). Blockchain and smart contracts for higher education registry in Brazil, *International Journal of Network Management* **29**(3): 1–21, DOI: 10.1002/nem.2061.

Prime (2017). Prime: A Byzantine fault-tolerant replication engine, Johns Hopkins University, Baltimore, www.dsn.jhu.edu/byzrep/prime.html.

Proof of Existence (2018). Proof of Existence: Written forever, https://proofofexistence.com.

Pustišek, M. and Kos, A. (2018). Approaches to front-end IoT application development for the Ethereum blockchain, *Procedia Computer Science* **129**: 410–419.

Robert, S. and Alan, W. (1978). *The Principles of Practical Cost-Benefit Analysis*, Oxford University Press, Oxford.

Sankar, L.S., Sindhu, M. and Sethumadhavan, M. (2017). Survey of consensus protocols on blockchain applications, *4th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India,* pp. 1–5, DOI: 10.1109/ICACCS.2017.8014672.

Sethi, A.K. and Sethi, S.P. (1990). Flexibility in manufacturing: A survey, *International Journal of Flexible Manufacturing Systems* **2**: 289–328, DOI: 10.1007/BF00186471.

Sigrid, S. and Samman, G. (2016). Consensus: Immutable agreement for the Internet of value, KPMG, Amstelveen, https://assets.kpmg/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf.

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*, O'Reilly Inc Media, Newton.

Tangle (2018). Version 1.4.3, https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf.

Trón, V. and Lange, F. (2015). Ethereum specification, https://github.com/ethereum/go-ethereum/wiki/Ethereum-Specification.

Wiśniewski, R., Bazydło, G., Szcześniak, P. and Wojnakowski, M. (2019). Petri net-based specification of cyber-physical systems oriented to control direct matrix converters with space vector modulation, *IEEE Access* **7**: 23407–23420, DOI: 10.1109/ACCESS.2019.2899316.

Wiśniewski, R., Grobelna, I. and Karatkevich, A. (2020). Determinism in cyber-physical systems specified by interpreted Petri nets, *Sensors* **20**(19): 5565.

Underwood, S. (2016). Blockchain beyond bitcoin, *Communications of the ACM* **59**(11): 15–17.

Vora, J., Nayyar, A., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M.S. and Rodrigues, J.J.P.C. (2018). BHEEM: A blockchain-based framework for securing electronic health records, *2018 IEEE Globecom Workshops, Abu Dhabi, UAE*, pp. 1–6, DOI: 10.1109/GLOCOMW.2018.8644088.

Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y. and Kim, D.I. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks, *IEEE Access* **7**: 22328-22370.

Xiao, D. (2016). The four layers of the blockchain, https://medium.com/@coriacetic/the-four-layers-of-the-Blockchain-dc1376efa10f.

Xu, X. (2012). From cloud computing to cloud manufacturing, *Robotics and Computer-Integrated Manufacturing* **28**(1): 75–86.

Yang, L. (2017). Industry 4.0: A survey on technologies, applications and open research issues, *Journal of Industrial Information Integration* **6**: 1–10, DOI: 10.1016/j.jii.2017.04.005.

Yu, T., Lin, Z. and Tang, Q. (2018). Blockchain: The introduction and its application in financial accounting, *Journal of Corporate Accounting & Finance* **29**(4): 37–47.

Zissis, D. and Lekkas, D. (2012). Addressing cloud computing security issues, *Future Generation Computer Systems* **28**(3): 583–592.

Aniruddha Bhattacharjya is a professor of computer science and engineering in the School of Computing in KL University (Koneru Lakshmaiah Education Foundation), India. He was a PhD scholar (Chinese Government Scholarship (CGS) holder) in 2015–2019 in the Department of Electronic Engineering, Beijing National Research Center for Information Science and Technology, Tsinghua University, Beijing, China. He has more than 14 years of teaching and research experience in India and abroad. He has authored 40 papers at international conferences and in journals. His research area includes applications of cryptography, end-to-end secure communication, blockchain technology's security aspects and IoT securities. He is a senior IEEE member and an ACM professional member.

Received: 29 August 2021
Revised: 7 March 2022
Re-revised: 25 April 2022
Accepted: 15 May 2022