Proceedings of the 2023 International Conference on Software Engineering and Machine Learning
DOI: 10.54254/2755-2721/8/20230108

A survey of blockchain IoT integration

Chuanwang Fang

School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan Province, China, 611731

2020010801020@std.uestc.edu.cn

Abstract. The Internet of Things (IoT) brings people increasingly more convenience nowadays. However, due to the simple structure of most IoT devices and the limited budget when designing and building IoT systems, there are often security vulnerabilities in IoT systems. In addition, the accelerated growth of IoT devices and the data they generate also puts greater pressure on traditional centralised computing centers. Due to its openness, transparency, secure communication, and decentralisation, blockchain technology may solve these problems. This paper mainly studies the research trends of blockchain, IoT, and their integrated systems in recent years and puts forward issues worthy of attention in future development. This paper aims to help beginners get started with blockchain and IoT by providing an overview of blockchain, IoT, and their integration through reviewing and analysing literature. It recommends focusing on chain-chain communication security, new information compression and extraction methods, multi-dimensional evaluation of blockchain IoT systems, information security mechanisms against quantum computers in blockchain IoT integrated systems, and so on.

Keywords: Blockchain, Internet of things, Security, Privacy, Communication, Scalability.

1. Introduction

This paper has referred to many papers related to blockchain and the IoT, as well as papers on the integration of the two. Most projects mentioned in the literature have not released source code. Some projects release source code only for simulation or testing, not the key systems proposed in the paper. Among those projects that have given complete source code, some platforms (such as Hyperledger Fabric) used are so old that some of the dependent packages used in the code have been deleted by the developers of the platforms. Some projects use too many programming languages, making them unfriendly to blockchain and IoT beginners. Thus, there is a gap, and the author hopes to survey blockchain and IoT to provide an overview of the theory and applications. This paper covers blockchain security, privacy, scalability, modifiability, performance benchmarking, and real-world applications. In terms of IoT, security, reliability, communication, routing, interoperability, data analysis, real-world applications, etc. are discussed. Security, blockchain solutions to IoT device resource restrictions, data storage and consumption, and practical applications are discussed in this paper. This paper surveys blockchain and IoT and suggests future research. This article may help blockchain and IoT beginners.

2. Literature review

2.1. Blockchain

Blockchain is a distributed, shared ledger that allows for the safer, easier, and more open tracking of assets across a network of businesses.

The key feature of blockchain is security, which is guaranteed by cryptographic methods and protocols. In 1981, Leslie Lamport discovered a method that safeguard user-system communication even if an eavesdropper can read system data, interfere with, or listen in on the communication process[1]. Later in 1982, Ralph C. Merkle invented a method to generate a digital signature in order to authenticate a message. This method avails itself of a one-way authentication tree function[2]. Based on these studies, Jae Cha Choon et al. introduced a Gap Diffie-Hellman (GDH) group-based identity-based signature system in 2003. This system has been shown to be resistant to identity attacks using a random oracle and existential forgeries on adaptively chosen messages[3]. Besides cryptographic methods, behaviours also affect the security of blockchains. In order to solve the problem of Block-hiding behaviours, Johannes Göobel et al. presented a method in 2016 that would monitor the pace at which orphaned blocks are produced in to identify block-hiding behavior[4]. Bitcoin is believed to be vulnerable to 51% attack, but is safe with malicious miners counting less than 50%. However, in 2018, Ittay Eyal et al. proved the Bitcoin mining protocol is vulnerable and presented an attack to show malicious miners' unions of any size are able to cause a nuisance to the Bitcoin system. They also presented a modification to the Bitcoin protocol to forbid selfish mining by a union of malicious miners with less than 25% computational resources[5]. Blockchain is thought to be a "trustless technology" because it builds trust in a trustless network, which also contributes to its security feature. However, in 2020, Primavera De Filippi et al. stated that blockchain is not a "trustless technology" but rather a "confidence machine" that boosts confidence using mathematical principles, cryptographic algorithms, and incentives based on game theory. They argued that the participation of trustworthy actors is also needed[6]. Fraudulent users have the potential to destroy the security of a blockchain system. In 2022, Lin Liu et al. offer a safe blockchain-based machine learning fraud detection approach using XGboost and random forest (RF) algorithms to categorise and forecast transaction patterns to identify fraudulent users in the Bitcoin network[7].

Smart contracts are immutable computer programmes that execute deterministically on the virtual machines of blockchain platforms like the Ethereum virtual machine (EVM). However, smart contracts cannot be modified once released, making security breaches difficult to fix. Therefore, in 2016, Loi Luu et al. proposed methods to make smart contract applications (Apps) safer by enhancing operational semantics. They also created Oyente, a symbolic execution tool for smart contract developers to find security flaws[8]. In 2018, Sidney Amani et al. proposed an extension of an EVM formalisation in Isabelle/HOL to provide formal verification of EVM smart contracts with cost and complexity controlled[9].

To develop a decentralised application (DApp) using a smart contract is very different from developing a normal App because the update of a DApp requires the coordination of all users. In 2018, Giuseppe Destefanis et al. discussed how recognised best practises in software engineering can mitigate the problems caused by bugs in smart contract Apps and called for standardised best practises in smart contract and blockchain programming[10]. The problem of extension and the difficulty of developing DApps on blockchain has been a problem since the Bitcoin system. Up until 2018, Elli Androulaki et al. proposed Hyperledger Fabric, a blockchain platform that is modular and really extendable and on which DApps written in general-purpose programming languages can run. This is a system of high throughput, high scalability, and low latency used for permissioned blockchains[11].

Information is stored in all nodes in the blockchain, which raised people's concern about their privacy. Although the address of an account in the blockchain can be randomly generated, the transactions produced may contain sensitive information. Ahmed Kosba et al. proposed Hawk, a decentralised smart contract platform, as a solution to this issue in 2016. Hawk protects user privacy by not storing plain text on the blockchain, while also simplifying life for developers by eliminating the need for them to implement the cryptographic functions[12]. In 2022, Wei Liang et al. presented PDPChain, a consortium blockchain-based scheme for protecting personal data privacy that stores encrypted data in distributed private clusters. The PDPChain maintains original data encrypted using an upgraded Paillier homomorphic encryption mechanism and allows fine-grained access control based on ciphertext policy attribute-based encryption (CP-ABE)[13].

The protocol of Bitcoin has a scalability problem because data in the blockchain can’t be deleted to prevent double spending and similar attacks, making the blockchain bulky and unscalable. Therefore, in 2014, JD Bruce proposed the "mini blockchain scheme," a lightweight P2P cryptocurrency scheme that automatically forgets old transactions. The account tree stores account balances, and the proof-chain and mini-blockchain secure this scheme. These components reduce blockchain size without compromising security[14]. Ittay Eyal et al. developed Bitcoin-NG (Next Generation), a Byzantine fault-tolerant blockchain architecture, in 2016. This protocol can withstand high churn without compromising security[15]. In the same year, Richard Dennis et al. developed a temporal rolling blockchain that keeps the size of the blockchain fixed. They also carry out a study to demonstrate that security is not jeopardised when data is deleted in this scheme[16].

The unmodifiable nature of blockchain makes it safe, but sometimes people want some information to be erased for "the right to be forgotten." Therefore, in 2017, Giuseppe Ateniese et al. enhanced a framework enabling rewritable blockchains by exploiting the chameleon hash functions. They also suggested a redactable proof-of-concept blockchain based on Nakamoto’s Bitcoin core, which claims to be smaller than the immutable one[17]. After that, in 2021, Ke Huang et al. proposed two cryptographic schemes—linkable-and-redactable ring signature (LRRS) and time-updatable chameleon hash (TUCH)—to enable users to scalably and secretly redact the blockchain[18].

Performance of private blockchain can determine whether companies use blockchain systems for production and increase operational efficiency. Therefore, a benchmarking tool called BLOCKBENCH was proposed in 2018 by Tien Tuan Anh Dinh et al. to assess private blockchain data processing efficiency. Using BLOCKBENCH, the researchers thoroughly evaluated Ethereum, Hyperledger Fabric, and Parity and discovered certain compromises in the design space as well as performance disparities between database systems and blockchain[19]. Another important metric for assessing a blockchain system’s quality is its energy efficiency. In 2020, in order to increase energy efficiency, which will be lowered by nodes with low reliability during spectrum sensing in cognitive wireless networks, Huang Tangsen et al. proposed the Secure Spectrum Sensing based on Blockchain (SSSB) algorithm and the Node Evaluation and Scheduling (NES) algorithm[20].

The positive traits of blockchain that were described above make it applicable in a variety of areas. In the field of medicine, many researchers will manipulate data when operating clinical trials, so some people turn to blockchain technology to find a solution. In 2016, Timothy Nugent et al. advocated employing smart contracts, acting as a trusted supervisor, and honestly capturing immutable trial history to address the issue of data tampering in clinical trials[21]. In the field of intelligent manufacturing, Atin Angrish et al. introduced the "FabRec" technique in 2018, which intends to handle the manufacturing information provided by various companies utilising blockchain technology in order to make manufacturing more intelligent and transparent. They also proposed a system in which decentralised networks of manufacturing and computing nodes could automatically reveal organisational capacities. Third parties verify this capability through historical events and automation mechanisms[22]. In 2018, Lennart Bader et al. proposed CAIPY, an ecosystem utilising smart contracts to support current car insurance processes in order to reduce costs. CAIPY demonstrates its capability of supporting insurers without adding new risks[23]. The use of blockchain in e-commerce is crucial because it may facilitate transactions between parties that lack mutual confidence in the absence of a reliable third party. In 2019, Aditya Asgaonkar et al. proposed a protocol of dual-deposit escrow trade to address the issue of exchanging digital goods without trusted third parties. Because this tactic adheres to the subgame of "Perfect Nash Equilibrium" in the game, it assures that buyers and sellers act honestly[24]. Blockchain also has the potential to support telemedicine. In 2020, Hossain Kordestani et al. presented a patient-centric telemedicine framework based on blockchain technology to provide convenience to patients by offering telemonitoring and teleconsultation services. The system also saves doctors' time by avoiding unnecessary trips[25]. The traceability of products is essential in additive manufacturing. A blockchain-based solution to govern and trace transactions produced during the additive manufacturing process was put forth by Nouf Alkaabi et al. in 2020. Design files, records, and additional product specifications are stored and shared using Interplanetary File Systems[26].

2.2. Internet of Things

The IoT is an enlarged and extended network that can connect numerous sensor devices with the Internet to create a vast network and enable the connectivity of people, machines, and things at any location and at any time.

Security and reliability have always been weaknesses of the IoT. In 2013, Parikshit N. Mahalle et al. proposed the Identity Authentication and Capability-based Access Control (IACAC) model, which provides an integrated approach to identity verification and access control for IoT devices and is secure against replay, man-in-the-middle, and denial of service (DoS) attacks[27]. IoT in smart home systems greatly facilitates our lives, but the security problems of these IoT systems cannot be ignored. In 2019, Wei Zhou et al. analysed the 5 popular smart home platforms and discovered some unexpected state transitions by analysing state machines obtained using reverse engineering. They also arranged attacks using phantom devices to confirm and trigger those unexpected state transitions, leading to the discovery of new vulnerabilities and a series of attacks[28]. A novel model-based framework was put up in 2019 by Moez Krichen et al. to evaluate the security properties of the IoT system adopted in smart cities. This framework is based on Attack Trees and Price Timed Automata, which are two formalisms aimed at describing the attack strategy and generating input for the test generation algorithm adopted in the system[29]. After that, in 2020, Guilin Zhao et al. introduced a combinatorial hierarchical technique to analyse the reliability of IoT systems after modelling the failure of IoT systems due to cascading probabilistic functional dependency and random failure propagation time[30]. In 2022, Alaeddine Mihoub et al. presented an architecture enabling the detection and mitigation of DoS and Distributed Denial of Service (DDoS) attacks. This architecture utilises machine learning techniques and yields an inspiring accuracy of 99.81%[31].

Communication is an essential research direction for the IoT, which affects the performance, scalability, energy efficiency, and user experience of IoT systems. In 2015, Sergey Efremov et al. put forward a general IoT architecture based on the cloud to solve the challenge of device discovery and inter-device communication for large-scale IoT networks[32]. Also, to improve the performance of device discovery and inter-device communication, in 2016, David J. Wu et al. developed two lightweight protocols for automatic service discovery and mutual authentication with privacy preserved, which fill the privacy hole in many popular protocols like Bluetooth Low Energy, Apple AirDrop, and Multicast DNS protocol[33]. To take full advantage of the edge devices and improve performance, in 2017, Yuvraj Sahni et al. proposed Edge Mesh, a computing paradigm for IoT devices that distributes decision-making tasks to all IoT devices within the network instead of sending all the data to a central server, so as to improve performance, reduce latency, enhance scalability, and protect security and privacy[34]. Communication using less energy has attracted the attention of experts in academia and industry. To improve IoT systems' performance in energy, computation, and communication (ECC). In 2020, Qiao Qi et al. developed a framework including ECC and proposed a combined beamforming design method utilised on IoT devices and base stations to enhance the overall performance of the current ECC procedure[35]. To optimize energy and entropy based on Quality of Experience(QoE), Ali Hassan Sodhro et al. developed the Quality of Service(QoS)-based joint energy and entropy optimization(QJEEO) method in 2020. In order to model and evaluate QoE, which is a more accurate factor to analyze customers' satisfaction according to their test results, they also developed a multimedia data structure model and framework driven by 6G to model and evaluate QoE in time[36].

Routing is a key factor influencing the delay and throughput of IoT systems. In 2017, Sofiane Hamrioui et al. proposed Efficient IoT Communications based on Ant System (EICAntS), which is a routing algorithm presented in the context that existing routing protocols are not efficient enough in an IoT environment. This algorithm tackles the difficulty of routing for large-scale IoT systems, reduces delay, raises throughput, expands lifetime, and also conserves more energy[37]. In order to overcome the issues with the routing protocol for low-power and lossy networks (RPL) in large IoT networks, Khadak Singh Bhandari et al. presented various objective functions in 2020. They divided the physical network into multiple instances of RPL. A novel parent selection framework is also offered to overcome the solitary routing metric issue in RPL based on a multi-attribute decision-making technique[38]. To optimise the energy efficiency in the routing process of an IoT network, a resource-aware and reliable objective function (RAROF) was introduced in 2020 by Khadak Singh Bhandari et al. It can design the best routing path by utilising a node's duty cycle, energy condition, link quality, and resource availability. This OF increased energy efficiency while extending the network's lifespan[39].

The interoperability of IoT devices is another crucial factor affecting the scalability of IoT systems besides communication. In order to promote it, Gianluca Aloi et al. presented a mobile gateway for IoT devices based on smartphones in 2017. The gateway consumes less hardware resources while acting as a transparent interface for IoT devices[40].

Heterogeneous and massive IoT data makes analysis difficult. In 2018, Adnan Akbar et al. proposed a two-level architecture for analysing heterogeneous and massive IoT data. The first layer accepts all data from various systems and interfaces and extracts high-level events in real-time, while the second layer uses a Bayesian network to perform probabilistic fusion based on high-level events and provides predictions that take uncertainty and the detection of complex events into account[41].

Having a life cycle view helps design better system architecture. A generic life cycle model for IoT systems was defined by Leila Fatmasari Rahman et al. in 2018, which offers a perspective on system architecture. The model is formed based on observations and the generalisation of current IoT solutions and important IoT functionalities, as well as quality attributes[42].

IoT is widely employed in many different industries. It has the potential to reform retailing and is an important part of Retail 4.0. In 2017, Athul Jayaram proposed the Retail 4.0 IoT model for consumers and retailers, which assists intelligent retailing and strategic marketing for consumer products[43]. IoT provides important technical support for smart home devices. In 2017, Julia Lee invented a location sensor for a deadbolt lock latch strike based on IoT that utilises a microprocessor to process location information and transmit the information to smartphones or IoT gateways via wireless communication[44]. In the field of smart medical devices, IoT devices can be used to monitor people's health conditions when specialists are not available. In 2019, Leo John Baptist Andrews et al. invented an integrated, compact gadget for monitoring heart rate and temperature in order to help detect heart disease and offer alerts to users, especially when specialists are not available nearby or users are ignorant of their hearts' condition[45]. IoT is also used in smart agriculture. In 2020, R. Vijaya Saraswathi et al. presented a technical framework that makes use of IoT technology to upload different parameters read by sensors to the cloud, and after readings are processed in the cloud, commands are given to actuators to achieve precise fertilisation and increase yields[46]. IoT can boost manufacturing efficiency, but smart factory management and upgrades require an objective measurement framework. In 2019, based on the cyber-physical system (CPS) and industrial internet of things (IIoT) technologies, Chui Young Yoon developed a measurement framework for intelligent manufacturing to support the management and upgrade of smart factories. This measurement model estimates the smart factory technology with 2 measurement domains, 7 measurement factors, and 28 measurement items[47].

2.3. Blockchain and IoT integration

The combination of IoT and blockchain technology brings several benefits, including enhanced security, decentralised data storage, increased reliability, improved traceability, increased transparency, automated processes, and so on.

The blockchain's security feature can compensate for the IoT's security shortfalls. In 2018, Mohamed Tahar Hammi et al. proposed a decentralised identity and authentication system called "bubbles of trust" to guarantee data availability and integrity in an autonomously controlled IoT system. Blockchain provides this solution's security characteristic[48]. In the same year, a framework to combine blockchain with IoT was suggested by Yong Yu et al., which offers excellent assurance for IoT data as well as numerous functionalities with satisfying scalability, involving decentralised payment, authentication, and other features. They also offer several blockchain-based options for typical IoT security and privacy problems, demonstrating how blockchain empowers IoT[49]. Then, in 2019, Jiawen Kang et al. introduced a security enhancement solution in which active miners and standby miners are chosen based on their reputation, which is a measure derived from both past behaviours and the recommendations of other vehicles. This scheme avoids internal collusion among active miners by having standby miners verify blocks, thus enhancing the security of the Internet of Vehicles (IoV)[50]. The security and reliability of the IIoT are barriers to its development. To ease this situation, in 2019, Junqin Huang et al. introduced a blockchain system for IoT devices with a credit-based proof-of-work mechanism that simultaneously delivers system security and transaction efficiency and offers a viable solution to security challenges in IIoT[51]. In order to provide trust and confidence in massive and vulnerable IoT networks to outside networks, Jawad Ali et al. developed a device monitor setup in IoT networks in 2019 to extract and analyse the behaviour of IoT devices, attempting to identify attacks within the requested timeframe. They also integrated Trusted Execution Technology (Intel SGX) to safeguard data on blockchains and secure App execution[52]. Also in 2019, Soumyashree S. Panda et al. invented a blockchain-based, decentralised system for effectively managing a large scale of smart devices. A mechanism for proving the authenticity of devices and users is also created[53]. Songlin He et al. developed blockchain-based IoT management systems in the same year to fill the security breach caused by relay node failure and prevent data blockage in IoT networks. The "diffusion" function in this system is used to send messages from sensors to full nodes. They also developed an enhanced consensus mechanism to prevent data loss, replicate processing results, and promote the delivery of opportunistic outcomes[54]. In 2020, to secure communications in the Internet of Drones (IoD) scenario, Basudeb Bera et al. presented a blockchain-based access control scheme to protect communication between drones as well as between drones and the ground station server (GSS). The Ripple Protocol Consensus Algorithm will be used to attach the blocks of data that are formed by GSS's transactions to the blockchain[55].

The performance of blockchain-based IoT systems is frequently constrained by the resource limitations of IoT devices. In 2017, Kazım Rıfat Özyılmaz et al. presented an event-based messaging mechanism for IoT end-devices with IoT gateways configured as blockchain nodes, using proof of concept as a consensus mechanism to solve the resource limitations of IoT devices[56]. To reduce the delay of accessing IoT data and utilising the high-performance computing resources in IoT networks, Pradip Kumar Sharma et al. presented a blockchain-based cloud architecture with software defined networking (SDN) in 2017 to reduce the latency of accessing huge volumes of IoT data securely and allow the edge of IoT networks to have access to high-performance computing resources[57]. After that, in 2018, based on Ethereum, Haoli Sun et al. presented a rich-thin client IoT solution, where only rich clients perform the mining process because they possess more resources. The challenges brought on by the IoT devices' finite resources can be overcome when adapting this solution to a variety of IoT applications[58]. The computation requirements of blockchains usually surpass what IoT devices can provide. In 2019, Ali Dorri et al. presented a lightweight scalable blockchain (LSB) to optimise computation overhead for IoT requirements with end-to-end security guaranteed. They also advanced a distributed time-based consensus algorithm (DTC) to lessen the computational burden and delay in the mining process[59]. A short while later, in 2019, Laizhong Cui et al. created a blockchain protocol called CoDAG that is both effective and secure. To increase the effectiveness of IIoT systems, they also created an IIoT architecture based on CoDAG[60].

Appropriate data storage, exploitation, and trading can bring huge economic benefits. By utilising a sign-encryption method between IoT devices and a gateway, in 2019, Md. Ashraf Uddin et al. advanced a decentralised architecture based on blockchain with the purpose of storing IoT data in smart home and city systems securely and privately. The gateway's software agent chooses the miner nodes according to performance indicators[61]. A brand-new trading scheme built on blockchain technology with smart contracts was proposed by Yuna Jiang et al. in 2019. To solve the lack of trust and robustness in centrally managed data trading platforms in the IIoT, it realises data packet transactions (DPTs) and data analytics service transactions (DASTs) in a decentralised manner[62].

Blockchain and IoT integrated systems have been implemented in numerous industries, including IoT E-commerce, IoV, IIoT, data mining, supply chain management, military equipment, and so on. In 2015, Yu Zhang et al. suggested a new E-business model for IoT E-business that redesigned many elements of conventional E-business, realised smart property, and paid data trading using P2P trading based on smart contracts[63]. In 2016, Konstantinos Christidis et al. demonstrated how blockchain-IoT integration has the potential to create a marketplace for trading services between devices based on service and resource sharing. Additionally, they highlighted how the integration automates time-consuming operations with cryptographic verification[64]. After that, in 2018, Haoli Sun et al. deployed their rich-thin client IoT solution to an electric car battery refilling system that utilised a battery switching strategy[58]. Traceability and transparency have important effects on the manufacturing of autonomous mobiles. In 2018, Marlene Kuhn et al. presented a blockchain and IoT-enabled system to increase the traceability, transparency, and audibility of the electrical system manufacturing of autonomous mobile[65]. Also in 2018, to leverage data collected by vehicles, Regio A. Michelin et al. suggested a framework using blockchain technology to create a trusted data-sharing platform for smart vehicles to exchange data acquired while maintaining privacy, resilience, integrity, and non-repudiation. In their architecture, data is decoupled from the block header in a transaction and may be expired to guarantee the system's efficiency[66]. Blockchain and IoT-integrated systems can reduce the difficulty of supply chain management. In 2019, Amal Alahmadi et al. presented a supply chain management system for the IIoT utilising blockchain technology to overcome the issue of mutual trust and in-time information sharing in supply chain management[67]. Blockchain-integrated IoT is also gaining attention in the military. In 2022, Rubina Akter et al. presented Internet-of-Military-Things (IoMT)-Net, a blockchain-integrated intelligent framework based on a convolutional neural network (CNN) to recognise and track illegal unmanned aerial vehicles (UAV) in the IoMT system[68].

3. Discussion

In the field of IoT, some of the researchers mentioned above are studying protocols, some are studying inter-device communications, and some are applying IoT to real-world industry to improve the overall efficiency and productivity of the whole production system.

Blockchain for IoT has many aspects to improve. For example, chain-chain communication, which secures blockchain-based IoT systems. As for the concept of decentralization, currently, hash algorithms are used to recover data from all previous blocks to support distributed data storage. However, there is a tradeoff: a longer hash loses less information but uses more storage. In addition, from the perspective of information theory, is the hash algorithm the best information processing scheme? Maybe there are better ways to consume less storage while preserving the same amount of information under the premise of ensuring information security.

One of the unclear areas of research includes the evaluation of the IoT integration system, specifically how much the system can increase the production rate and efficiency. Many developing countries cannot afford the system or earn enough to cover input costs. Energy consumption is also important because carbon reduction is a trend and clean energy doesn't meet most of our energy needs. Therefore, the cost performance in multiple dimensions needs to be calculated.

As for data mining and abstraction, further research is needed on information extraction. IoT systems in real production processes can generate massive amounts of data, but storage and processing power are limited. Thus, effectively extracting useful information is crucial. One way of extracting information is through "matrix information extraction," which uses different statistical variables such as average, median, etc. Another direction of information extraction is visualization. For a newly developed system, there is some information that other systems cannot offer. Therefore, a new way of visualising data is needed to fill in the gaps of traditional visualisation in a way that is not confusing.

The security of IoT systems also can’t be ignored. Encryption algorithms and protocols safeguard IoT data. Traditional encryption is secure because brute force is computationally difficult. However, quantum computers can easily break traditional encryption methods based on the factorization of large numbers, such as RSA. Therefore, quantum communication, which can ensure that the communication process cannot be eavesdropped thanks to quantum entanglement and quantum key distribution, is needed. Future encryption methods may need to be updated at any time and implemented in our existing system within a short time.

4. Conclusion

This paper reviews research in the areas of IoT, blockchain, and the integration of blockchain and IoT. There was a gap in the survey of the IoT and blockchain areas, especially in the implementation perspectives. This paper collectively includes all the literature closely related to the current best models, frameworks, algorithms, and evaluation methods.

Based on that, this paper mentioned a few discussions about the current research, raising some ideas that should be explored to apply the current techniques to real-world applications, including some further studies and research in different areas.

References

[1] Leslie Lamport. Password authentication with insecure communication. Communications of the ACM, 24(11):770–772, 1981.

[2] Ralph C Merkle. Method of providing digital signatures, January 5 1982. US Patent 4,309,569.

[3] Jae Cha Choon and Jung Hee Cheon. An identity-based signature from gap diffie-hellman groups. In International workshop on public key cryptography, pages 18–30. Springer, 2003.

[4] Johannes G¨obel, Holger Paul Keeler, Anthony E Krzesinski, and Peter G Taylor. Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. Performance Evaluation, 104:23–41, 2016.

[5] Ittay Eyal and Emin G¨un Sirer. Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM, 61(7):95–102, 2018.

[6] Primavera De Filippi, Morshed Mannan, and Wessel Reijers. Blockchain as a confidence machine: The problem of trust & challenges of governance. Technology in Society, 62:101284, 2020.

[7] Lin Liu, Wei-Tek Tsai, Md Zakirul Alam Bhuiyan, Hao Peng, and Ming sheng Liu. Blockchain-enabled fraud discovery through abnormal smart contract detection on ethereum. Future Generation Computer Systems, 128:158–166, 2022.

[8] Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor. Making smart contracts smarter. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, pages 254–269, 2016.

[9] Sidney Amani, Myriam B´egel, Maksym Bortin, and Mark Staples. Towards verifying ethereum smart contract bytecode in isabelle/hol. In Proceedings of the 7th ACM SIGPLAN International Conference on Certified Programs and Proofs, pages 66–77, 2018.

[10] Giuseppe Destefanis, Michele Marchesi, Marco Ortu, Roberto Tonelli, Andrea Bracciali, and Robert Hierons. Smart contracts vulnerabilities: a call for blockchain software engineering? In 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), pages 19–25. IEEE, 2018.

[11] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the thirteenth EuroSys conference, pages 1–15, 2018.

[12] Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In 2016 IEEE symposium on security and pri- vacy (SP), pages 839–858. IEEE, 2016.

[13] Wei Liang, Yang Yang, Ce Yang, Yonghua Hu, Songyou Xie, Kuan-Ching Li, and Jiannong Cao. Pdpchain: A consortium blockchain-based privacy protection scheme for personal data. IEEE Transactions on Reliability, 2022.

[14] JD Bruce. The mini-blockchain scheme. White paper, page 10, 2014.

[15] Ittay Eyal, Adem Efe Gencer, Emin G¨un Sirer, and Robbert Van Renesse. {Bitcoin-NG}: A scalable blockchain protocol. In 13th USENIX symposium on networked systems design and implementation (NSDI 16), pages 45–59, 2016.

[16] Richard Dennis, Gareth Owenson, and Benjamin Aziz. A temporal blockchain: a formal analysis. In 2016 International Conference on Collaboration Technologies and Systems (CTS), pages 430–437. IEEE, 2016.

[17] Giuseppe Ateniese, Bernardo Magri, Daniele Venturi, and Ewerton Andrade. Redactable blockchain–or–rewriting history in bitcoin and friends. In 2017 IEEE European symposium on security and privacy (EuroS&P), pages 111– 126. IEEE, 2017.

[18] Ke Huang, Xiaosong Zhang, Yi Mu, Fatemeh Rezaeibagha, and Xiaojiang Du. Scalable and redactable blockchain with update and anonymity. Information Sciences, 546:25–41, 2021.

[19] Tien Tuan Anh Dinh, Rui Liu, Meihui Zhang, Gang Chen, Beng Chin Ooi, and Ji Wang. Untangling blockchain: A data processing view of blockchain systems. IEEE transactions on knowledge and data engineering, 30(7):1366– 1385, 2018.

[20] Huang Tangsen, Xiaowu Li, and Xiangdong Ying. A blockchain-based node selection algorithm in cognitive wireless networks. IEEE Access, 8:207156– 207166, 2020.

[21] Timothy Nugent, David Upton, and Mihai Cimpoesu. Improving data transparency in clinical trials using blockchain smart contracts. F1000Research, 5, 2016.

[22] Atin Angrish, Benjamin Craver, Mahmud Hasan, and Binil Starly. A case study for blockchain in manufacturing:"fabrec": A prototype for peer-to-peer network of manufacturing nodes. Procedia Manufacturing, 26:1180– 1192, 2018.

[23] Lennart Bader, Jens Christoph B¨urger, Roman Matzutt, and Klaus Wehrle. Smart contract-based car insurance policies. In 2018 IEEE Globecom workshops (GC wkshps), pages 1–7. IEEE, 2018.

[24] Aditya Asgaonkar and Bhaskar Krishnamachari. Solving the buyer and seller's dilemma: A dual-deposit escrow smart contract for provably cheat-proof delivery and payment for a digital good without a trusted mediator. In 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pages 262–267. IEEE, 2019.

[25] Hossain Kordestani, Kamel Barkaoui, and Wagdy Zahran. Hapichain: a blockchain-based framework for patient-centric telemedicine. In 2020 IEEE 8th International Conference on Serious Games and Applications for Health (SeGAH), pages 1–6. IEEE, 2020.

[26] Nouf Alkaabi, Khaled Salah, Raja Jayaraman, Junaid Arshad, Mohammed Omar, et al. Blockchain-based traceability and management for additive manufacturing. IEEE access, 8:188363–188377, 2020.

[27] Parikshit N Mahalle, Bayu Anggorojati, Neeli R Prasad, and Ramjee Prasad. Identity authentication and capability based access control (ia-cac) for the internet of things. Journal of Cyber Security and Mobility, 1(4):309–348, 2013.

[28] Wei Zhou, Yan Jia, Yao Yao, Lipeng Zhu, Le Guan, Yuhang Mao, Peng Liu, and Yuqing Zhang. Discovering and understanding the security hazards in the interactions between {IoT} devices, mobile apps, and clouds on smart home platforms. In 28th USENIX security

symposium (USENIX security 19), pages 1133– 1150, 2019.

[29] Moez Krichen and Roobaea Alroobaea. A new model-based framework for testing security of iot systems in smart cities using attack trees and price timed automata. In 14th international conference on evaluation of novel approaches to software engineering, pages 570–577. SCITEPRESS-Science and Technology Publications, 2019.

[30] Guilin Zhao and Liudong Xing. Reliability analysis of iot systems with competitions from cascading probabilistic function dependence. Reliability Engineering & System Safety, 198:106812, 2020.

[31] Alaeddine Mihoub, Ouissem Ben Fredj, Omar Cheikhrouhou, Abdelouahid Derhab, and Moez Krichen. Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques. Computers & Electrical Engineering, 98:107716, 2022.

[32] Sergey Efremov, Nikolay Pilipenko, and Leonid Voskov. An integrated approach to common problems in the internet of things. Procedia Engineering, 100:1215– 1223, 2015.

[33] David J Wu, Ankur Taly, Asim Shankar, and Dan Boneh. Privacy, discovery, and authentication for the internet of things. In European Symposium on Research in Computer Security, pages 301–319. Springer, 2016.

[34] Yuvraj Sahni, Jiannong Cao, Shigeng Zhang, and Lei Yang. Edge mesh: A new paradigm to enable distributed intelligence in internet of things. IEEE access, 5:16441–16458, 2017.

[35] Qiao Qi, Xiaoming Chen, Caijun Zhong, and Zhaoyang Zhang. Integration of energy, computation and communication in 6g cellular internet of things. IEEE Communications Letters, 24(6):1333– 1337, 2020.

[36] Ali Hassan Sodhro, Sandeep Pirbhulal, Zongwei Luo, Khan Muhammad, and Noman Zahid Zahid. Toward 6g architecture for energy-efficient communication in iot-enabled smart automation systems. IEEE Internet of Things Journal, 8(7):5141–5148, 2020.

[37] Sofiane Hamrioui and Pascal Lorenz. Bio inspired routing algorithm and efficient communications within iot. IEEE Network, 31(5):74–79, 2017.

[38] Khadak Singh Bhandari, In-Ho Ra, and Gihwan Cho. Multi-topology based qos-differentiation in rpl for internet of things applications. IEEE Access, 8:96686–96705, 2020.

[39] Khadak Singh Bhandari and GI Hwan Cho. An energy efficient routing approach for cloud-assisted green industrial iot networks. Sustainability, 12(18):7358, 2020.

[40] Gianluca Aloi, Giuseppe Caliciuri, Giancarlo Fortino, Raffaele Gravina, Pasquale Pace, Wilma Russo, and Claudio Savaglio. Enabling iot interoperability through opportunistic smartphone-based mobile gateways. Journal of Network and Computer Applications, 81:74–84, 2017.

[41] Adnan Akbar, George Kousiouris, Haris Pervaiz, Juan Sancho, Paula TaShma, Francois Carrez, and Klaus Moessner. Real-time probabilistic data fusion for large-scale iot applications. Ieee Access, 6:10015– 10027, 2018.

[42] Leila Fatmasari Rahman, Tanir Ozcelebi, and Johan Lukkien. Understanding iot systems: a life cycle approach. Procedia computer science, 130:1057– 1062, 2018.

[43] Athul Jayaram. Smart retail 4.0 iot consumer retailer model for retail intelligence and strategic marketing of in-store products. Proceedings of the 17th international business horizon-INBUSH ERA-2017, Noida, India, 9, 2017.

[44] Julia Lee. Internet of things based deadbolt lock latch strike location smart sensor, January 26 2017. US Patent App. 14/804,146.

[45] Leo John Baptist Andrews, Linesh Raja, and Suresh Shanmugasundaram. Mobile android-based remote patient monitoring system through wearable sensors. Journal of Discrete Mathematical Sciences and Cryptography, 22(4):557–568, 2019.

[46] R Vijaya Saraswathi, Sravani Nalluri, Somula Ramasubbareddy, K Govinda, and E Swetha. Brilliant corp yield prediction utilizing internet of things. In data engineering and communication technology, pages 893–902. Springer, 2020.

[47] Chui Young Yoon. Measurement model of smart factory technology in manufacturing fields based on iiot and cps. In Proceedings of the 2019 International Conference on Artificial Intelligence, Robotics and Control, pages 80–84, 2019.

[48] Mohamed Tahar Hammi, Badis Hammi, Patrick Bellot, and Ahmed Serhrouchni. Bubbles of trust: A decentralized blockchain-based authenti- cation system for iot. Computers & Security, 78:126– 142, 2018.

[49] Yong Yu, Yannan Li, Junfeng Tian, and Jianwei Liu. Blockchain-based solutions to security and privacy issues in the internet of things. IEEE Wireless Communications, 25(6):12– 18, 2018.

[50] Jiawen Kang, Zehui Xiong, Dusit Niyato, Dongdong Ye, Dong In Kim, and Jun Zhao. Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory. IEEE Transactions on Vehicular Technology, 68(3):2906–2920, 2019.

[51] Junqin Huang, Linghe Kong, Guihai Chen, Min-You Wu, Xue Liu, and Peng Zeng. Towards secure industrial iot: Blockchain system with credit-based consensus mechanism. IEEE Transactions on Industrial Informatics, 15(6):3680–3689, 2019.

[52] Jawad Ali, Toqeer Ali, Yazed Alsaawy, Ahmad Shahrafidz Khalid, and Shahrulniza Musa. Blockchain-based smart-iot trust zone measurement architecture. In Proceedings of the International Conference on Omni-Layer Intelligent Systems, pages 152– 157, 2019.

[53] Soumyashree S Panda, Utkalika Satapathy, Bhabendu K Mohanta, Debasish Jena, and Debasis Gountia. A blockchain based decentralized au- thentication framework for resource constrained iot devices. In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pages 1–6. IEEE, 2019.

[54] Songlin He, Qiang Tang, Chase Qishi Wu, and Xuewen Shen. Decentral- izing iot management systems using blockchain for censorship resistance. IEEE Transactions on Industrial Informatics, 16(1):715–727, 2019.

[55] Basudeb Bera, Durbadal Chattaraj, and Ashok Kumar Das. Designing secure blockchain-based access control scheme in iot-enabled internet of drones deployment. Computer Communications, 153:229–249, 2020.

[56] Kazım Rıfat Özyılmaz and Arda Yurdakul. Work-in-progress: Integrating low-power iot devices to a blockchain-based infrastructure. In 2017 International Conference on Embedded Software (EMSOFT), pages 1–2. IEEE, 2017.

[57] Pradip Kumar Sharma, Mu-Yen Chen, and Jong Hyuk Park. A software defined fog node based distributed blockchain cloud architecture for iot. Ieee Access, 6:115– 124, 2017.

[58] Haoli Sun, Song Hua, Ence Zhou, Bingfeng Pi, Jun Sun, and Kazuhiro Yamashita. Using ethereum blockchain in internet of things: A solution for electric vehicle battery refueling. In International Conference on Blockchain, pages 3– 17. Springer, 2018.

[59] Ali Dorri, Salil S Kanhere, Raja Jurdak, and Praveen Gauravaram. Lsb: A lightweight scalable blockchain for iot security and anonymity. Journal of Parallel and Distributed Computing, 134:180– 197, 2019.

[60] Laizhong Cui, Shu Yang, Ziteng Chen, Yi Pan, Mingwei Xu, and Ke Xu. An efficient and compacted dag-based blockchain protocol for industrial internet of things. IEEE Transactions on Industrial Informatics, 16(6):4134– 4145, 2019.

[61] Md Ashraf Uddin, Andrew Stranieri, Iqbal Gondal, and Venki Balasubramanian. An efficient selective miner consensus protocol in blockchain oriented iot smart monitoring. In 2019 IEEE International Conference on Industrial Technology (ICIT), pages 1135–1142. IEEE, 2019.

[62] Yuna Jiang, Yi Zhong, and Xiaohu Ge. Smart contract-based data commodity transactions for industrial internet of things. IEEE Access, 7:180856–180866, 2019.

[63] Yu Zhang and Jiangtao Wen. An iot electric business model based on the protocol of bitcoin. In 2015 18th international conference on intelligence in next generation networks, pages 184–

191. IEEE, 2015.

[64] Konstantinos Christidis and Michael Devetsikiotis. Blockchains and smart contracts for the internet of things. Ieee Access, 4:2292–2303, 2016.

[65] Marlene Kuhn, Huong Giang Nguyen, Heiner Otten, and J¨org Franke. Blockchain enabled traceability–securing process quality in manufacturing chains in the age of autonomous driving. In 2018 IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD) , pages 131–136. IEEE, 2018.

[66] Regio A Michelin, Ali Dorri, Marco Steger, Roben C Lunardi, Salil S Kanhere, Raja Jurdak, and Avelino F Zorzo. Speedychain: A framework for decoupling data from blockchain for smart cities. In Proceedings of the 15th EAI international conference on mobile and ubiquitous systems: Computing, networking and services, pages 145–154, 2018.

[67] Amal Alahmadi and Xiaodong Lin. Towards secure and fair iiot-enabled supply chain management via blockchain-based smart contracts. In ICC 2019-2019 IEEE International Conference on Communications (ICC), pages 1–7. IEEE, 2019.

[68] Rubina Akter, Mohtasin Golam, Van-Sang Doan, Jae-Min Lee, and Dong-Seong Kim. Iomt-net: Blockchain integrated unauthorized uav localization using lightweight convolution neural network for internet of military things. IEEE Internet of Things Journal, 2022.