Issues and Challenges associated with Blockchain in Smart Cities

Gerasimos Vonitsanos*, Theodor Panagiotakopoulos†,‡, Andreas Kanavos†,§,
Manolis Maragoudakis¶ and Phivos Mylonas¶
*Computer Engineering and Informatics Department
University of Patras, Patras, Greece
mvonitsanos@ceid.upatras.gr
†School of Technology and Science
Hellenic Open University, Patras, Greece
panagiotakopoulos@eap.gr
‡Business School
University of Nicosia, Nicosia, Cyprus
§Department of Digital Media and Communication
Ionian University, Kefalonia, Greece
akanavos@ionio.gr
¶Department of Informatics
Ionian University, Corfu, Greece
{mmarag, fmylonas}@ionio.gr

***Abstract*—Since its inception, the blockchain technology has shown promising application prospects. From the initial cryptocurrency to the current smart contract, blockchain has been applied to many fields. Conventional IoT ecosystems involve data streaming from sensors and different devices to a centralized cloud computing server. Issues that arise include security and privacy concerns due to third party management of cloud computing servers, single points of failure, a bottleneck in data flows and difficulties in regularly updating firmware for millions of smart devices from a point of security and maintenance perspective. One can enable smart cities with a blockchain to offer enhanced security via storing transactions in a secure, transparent, decentralized, and immutable ledger. However, both blockchain and smart cities are in their infancy and significant research efforts are needed to integrate them. In this paper, we comprehensively review the role of blockchain in enabling IoT-based smart cities.**

***Index Terms*—Blockchain, Consensus Algorithms, Healthcare, Internet of Things, Security, Smart Cities, Sustainability**

I. Introduction

In the last decades, the huge technological advances have managed to reshape or even radically change most, if not all, areas of businesses. More specifically, in the field of economy, this technological explosion has managed not only to improve and facilitate the ways of trading, but also to ask questions about money and whether its very form can be turned into an alternative genre, much more transparent, and mostly highly compatible with the digital world.

Today there is much interest in the Internet of Things (IoT) from academics, but also from professionals, as innovative products have been created in different fields [26], [28]. Different devices can connect to an IoT network, creating a new physical network where no human intervention is required to control or manage [27]. It is estimated that by 2020 more than 50 billion devices will be connected to smart networks such as smart homes and smart cities [16].

Furthermore, due to evolution of internet platforms and social media, cryptocurrency remains a challenging issue to investigate. Authors in [24] surveyed several widely used cryptocurrency systems such as Bitcoin, Litecoin, Peercoin, Ethereum, Ripple, etc.

The most basic component regarding the operation of cryptocurrencies at the technological and structural level, is the Blockchain technology. Blockchain could be described as a a form of database that accepts a large number of registrations from users. These records are placed in a data sheet, also known as a block and over time, these records increase and the blocks that are created are connected to each other in the form of a chain. This feature makes the blockchain look like an account book, open to all users, which verifies its designation as the most decentralized trading system.

The blocks mentioned above are connected to each other in a unambiguous way, while they arise through the process we call proof of work. It is no longer necessary to have an intermediate trust authority (e.g., a bank), while the trust of the trading parties is based on an algorithmic confirmation. So, unlike the more traditional approaches, the decentralized solution of Blockchain technology offers transparency, speed of transactions, low cost and of course cross-border communication, since distance is a factor that does not does not affect the specific exchange system at all.

According to UN's "2018 Revision of World Urbanization Prospects", 4.2 billion people (55% of the global population)

lives in cities[1], with an estimation to increase by 2050 to 6.2 billion.Therefore, it can be recognized that new challenges are emerging and expected to be solved through Blockchain technology. A new digital ecosystem model is necessary for social, governmental, technological, and economic development in a smart city. In applications such as e-commerce, therefore, blockchain can be applied to improve security, privacy, and reliability issues [12].

High volume, high variety, high velocity, and high veracity are the characteristics of the data is created by various smart devices in a smart city [7]. However, it is not easy to take full advantage of them as there are issues related to privacy and security. For example, Federated Learning (FL) [18] protects privacy through a distributed machine learning technique without sending raw data. However, because the standard FL has low reliability, Blockchain can be used to provide security and reliability to the services of a smart city [17].

The full adoption of the blockchain in a smart city can not be done directly, as private blockchains are characterized by low security and scalability. However, gradually, of course, the services offered by the blockchain will be more reliable, and in particular, through smart contracts, the necessary intelligence is ensured to enable secure transactions in a smart city.

It is not allowed to delete data stored on a blockchain and stamped, contrary to data protection and privacy legislation, such as the European General Data Protection Regulation (GDPR). The "right to erasure" or "right to be forgotten" [22], falls under Article 17 of the GDPR. The blockchain must be standardized in order for it to be fully adopted in a smart city. However, innovative guidelines for the smooth transition to blockchain for existing smart city services have yet to be developed.

II. The Concept of Blockchain

Blockchain technologies contain Cryptography, Mathematics, Algorithm, and economic model. To solve traditional distributed database synchronize problems, a combination of peer-to-peer networks and distributed consensus algorithm is used; hence it is not just a single technique, but an integrated infrastructure construction in multiple fields [10], [11], [25].

The blockchain technologies composed of six key elements.

- Decentralization. The data is stored and updated distributively since the blockchain system is not based on a centralized node.
- Transparency. The records of data is transparent from one node to another in a blockchain system
- Open Source. The source code of a blockchain system is public and anyone use blockchain technologies for other applications.
- Autonomy. The main concern of a blockchain system is to ensure that the data is transferred safely. Therefore there is no intervention between the single users and the whole system between the nodes.
- Immutable. The data records cant be transformed unless a user controls over 51% of the node simultaneously.
- Anonymity. All the transactions between trusted nodes can be anonymous, users need only the blockchain addresses.

[1]https://www.un.org/development/desa/publications/2018-revision-of-world-urbanization-prospects.html

III. Recent Advances of Blockchain Applications in Smart Cities

This section presents the recent advances regarding blockchain-based smart cities and associated smart environments. In a smart environment, the business logic is executed by smart contracts, while various entities maintain the distributed ledger. A detailed review of the evolution and role of blockchain in the development of IoT-based smart cities is presented by the authors in [21]. Also, the very recent state-of-the-art works related to Blockchain in several fields of IoT are reviewed in [31].

A. Smart Electronic Commerce

In electronic commerce, buyers and sellers exchange their assets on electronic platforms based on trusted third parties for reliable delivery. In Blockchain, using smart contracts, reliable transactions can be made without intermediaries between the involved parties. After all, an audit of the stakeholders is also possible through the classified log files. Asgaonkar et al. in [2] proposed a smart contract based protocol for selling a digital asset based on a contract. More specifically, the buyer is required to make a refundable deposit and payment of the product while the seller deposit with a refund. Therefore if one of the two cheats, then the deposit will be lost. In [13] a blockchain-enabled Proof of Delivery framework is proposed employing the InterPlanetary File System for a secure, transparent logistics management solution for the delivery of physical goods through the sole carrier.

B. Smart Electronic Voting

In the traditional way of voting, which is based on ballots, there are always difficulties related to the high cost of the process, the possibility of fraud, and the case of low voter turnout. Instead, through smart governance in a smart city, through e-governance, the voting process can be automated with the help of digital technology. As a result, the level of security is higher, although these platforms are vulnerable to cyber-attacks. There is no single point of failure in a Blockchain-based network that is not controlled by any central authority. So in a blockchain-based voting system, each voter can have a wallet with a private key for authentication so they can only vote once [20]. In [3], different electronic voting systems that provide authentication and anonymity with blockchain architecture for online voting were reviewed.

C. Smart Healthcare

Using blockchain technologies, smart contracts, and access control technologies, state-of-the-art healthcare delivery in a smart city can be improved. Each patient's electronic health record can be stored securely without any privacy issues.

Generally, in these cases, there is a need for access from different departments to information in the stored medical history of patients [19]. The prevention of counterfeiting can be achieved by managing the supply chain of medical products through blockchain [1], as medical products are detected and tested for their origin [23]. The MedRec prototype is presented in [4] to store electronic health records using blockchain technology.

D. Smart Home

In a smart home, there are ubiquitous computing systems and wireless sensor networks used to manage devices such as lights, cooling and heating control and entertainment platforms [32]. Remote monitoring and control of home appliances are done through the internet connection. The main goals of smart homes are to upgrade the quality of services and home comfort, reliability, and privacy [15]. Nevertheless, there is a risk of privacy leaking as an IoT network in a smart home is connected to external servers in addition to local devices.

E. Smart Transportation

In this application of Blockchain in the transmission systems, they integrate cutting-edge technologies such as wireless sensor networks, computer peripheral computing devices to make them more secure and efficient. Traffic management systems include automated traffic control methods and license plate recognition and speed calculation cameras. The frame proposed in [35], consists of 7 layers which are the network, the data, the physical, the consensus, the application, the incentive, and the contract layer. As the volume of passengers and flights is constantly increasing, a technological solution to improve the management processes will include IoT systems that will be interconnected with other platforms and will implement the concept of smart airports [33].

IV. Requirements

Next, we will describe the basic requirements for blockchain to be a key technology in smart cities.

A. Bandwidth

In every practical design of a blockchain network for use in a smart city, the need for high network bandwidth should have been considered from the start. Controlling a multi-sensor network requires increased data exchange, so if bandwidth is insufficient, blockchain performance will be reduced, and it will not be easy to extend.

B. Data Access and Privacy

Personalized data in smart cities is vital in several customized processes such as smart healthcare and smart electronic voting. It is, therefore, necessary to control the use of personalized data to ensure privacy. Furthermore, in smart cities, it is necessary to design specialized access mechanisms for data access to support data privacy, as personal data is stored and controlled through the blockchain.

C. Data Availability

The permanent availability of data stored in blockchain technologies is essential for the activation of smart contracts. In a smart city, however, the number of stakeholders is massive, and the size of the network is just as significant. Therefore permanent availability will not be easily achievable, and specialized planning for smart cities is required.

D. Data Format

The network of sensors in a smart city constantly produces data characterized by heterogeneity and is generally unstructured, as different devices produce them. However, the importance of this data is significant as it can be analyzed and then aid decision-making processes. However, their analysis is not easy as there is no single standard, and they can have different formats. Therefore, it is crucial in blockchain technologies that there is no delay in the pre-processing stage of the data, and the analysis will be efficient.

E. Data Storage

Decentralized data storage in Blockchain facilitates expansion and protection against a single point of failure [5]. Of course, the amount of data generated by millions of devices is enormous in smart cities. One solution would probably be to store only the indexes in the Blockchain to reduce the volume significantly. In any case, a specialized mechanism should be designed that will satisfactorily manage the need to store the vast volume of data.

F. Latency

New technologies required in real-time operations, such as self-driving cars, can not rely on existing blockchain technology to handle a small number of transactions every second. We, therefore, need new mechanisms that will be integrated into the existing blockchain technology and will upgrade the handling of many transactions at the same time.

V. Challenges

In this section, we introduce a number of essential open challenges which can prevent the utilization of the corresponding blockchain technology into a smart city.

A. Consensus Algorithms

Smart city prerequisites have remarkably different requisitions that must be taken into account when designing them. Hence, these diverse requirements of the blockchain technology into a smart city can be considered a potential open research field. Regarding consensus algorithm, it must be noted that it supplies with regulations for coming to agreement between a few nodes included in a blockchain network. The implementation of consensus algorithms is characterized by several factors, like energy consumption or node identity [8]. Subsequently, in [9], significant parameters for designing consensus algorithms for varying implementations, like adversary tolerance, bandwidth, blockchain type, communication model, consensus finality, scalability and throughput. Nevertheless,

the planning and execution of this kind of algorithms require further research.

B. Cost

In order for alternating the existing framework, particularly when considering an infrastructure, it is important to identify numerous costs, like time and money. Hence, we need to make beyond any doubt that this novel technology does not only create financial advantages and meet the necessities of supervision, but also continuously experiences challenges from the inside organization which exists at a specific time period.

C. High-performance Computing Memories

An exceptional raise in smart IoT devices is anticipated within the future of smart cities. The allowance of blockchain-based services to this kind of devices postures a critical challenge of high storage necessities. This drives to the fact that each device in a blockchain network should maintain a total set of transactions and such type of high storage necessity limits the scalability of the blockchain network. On the other hand, scalability is one of the fundamental prerequisites of smart cities and hence, it is of the utmost importance to utilize high-performance memory with high storage necessity for empowering the scalable operation of blockchain-enabled smart cities. Moreover, storage can be implemented outside the blockchain network in case the high-performance computing memories are not located at a blockchain node. This kind of storage can be enabled with use of high-performance computing memory although this can pose additional robustness and security challenges. Blockchains can utilize off-chain decentralized storage and file systems such as InterPlanetary File System (IPFS) and Swarm, rather than centralized storage. However, before uploading to IPFS, data can be encrypted despite the fact that this includes more encryption-decryption delay. Finally, the sharing of encryption-decryption keys in a decentralized but secure way remains another issue to be taken into consideration.

D. Identity

When considering public/open blockchains, anyone has the ability to observe every transaction while every device can be identified with use of its public address. Regarding cryptocurrency-based smart city applications, the privacy issue can be moderated by creating a novel expendable address for each new payment. As of now, the identity of the users in smart city services is given with use of digital identity management systems, which are granted by central authorities. More to the point, Decentralized ID (DID) and Self-sovereign Identity (SSI) empower users to completely control their digital identity without an intermediate centralized third-party and this permits users to control how their personal information are public. Within the IoT-based smart city services, blockchain-based DID and SSI can be employed for initially identifying, as well as for the authentication and authorization of users in a decentralized way. However, there arise some issues, i.e. a user may lose the private key and therefore, formulating secure recovery mechanisms for DID and SSI could be a critical issue. Pioneer privacy strategies can be exploited for particular information sharing in mutual and anonymous multi-party transactions in a privacy-preserving way in terms of different smart city services [6].

E. Latency

Latency indicates the processing time of each transaction while throughput represents a maximum number of transactions within a specific pre-defined time period. Both latency and throughput limitations significantly influence the scalability of smart cities. In a blockchain-enabled smart city, latency occurs because of the computation at decentralized nodes, as except computation at local nodes, data communication between nodes is further added to the total value of latency. Latency due to propagation delay causes forking and thus, for avoiding this forking impact, the propagation delay must be minimized; an acknowledgment upon accepting a novel block to determine if forking occurred or not is presented in [17]. Following the forking taking place, the operation of block production restarts and this process continues until the update of the block occurs without forking.

F. Scalability

Scalability deals with the function of the smart environments empowered by blockchain services without missing Quality of Service (QoS) as the number of smart city devices are increasing. On the contrary, key design features of a conventional blockchain network consist of decentralization, fault tolerance and security. Nevertheless, by simultaneously accomplishing these aspects, several limitations on scalability are caused as each node of a blockchain network requires a developing number of records to be stored and further to participate in the validation procedure. Hence, a commonplace blockchain is inherently challenging to scale due to its completely decentralized nature. Furthermore, the number of smart IoT devices is anticipated to reach 64 billion in 2025[2] and this phenomenal increment in smart IoT devices forces challenges on planning scalable blockchain-based smart city infrastructures. Proof of Work (PoW) constitutes a consensus algorithm that aims to preserve the integrity of a blockchain network despite the fact that the typical PoW protocol seriously prevents the scalability of blockchain in terms of transactions per second. To moderate these scalability issues, a PoW-based in terms of parallel mining is introduced in [14].

G. Sustainability

Sustainability concerns the planning of blockchain-based smart cities without consumption of natural resources. However, the uncommon expansion of smart IoT devices in smart cities results in higher energy consumption. Except this issue, the consensus algorithms having big computational complexity seem to additionally increase energy consumption. In order to address the problem of energy consumption, a feasible solution

[2]https://techjury.net/blog/internet-of-things-statistics/

can be the energy-efficient planning as well as renewable energy sources. Subsequently, numerous energy-efficient features should be considered in terms of sustainable smart cities, like communication networks, consensus algorithms, storage and renewable energy resources [34]. A number of sustainable consensus algorithms are basically centering on energy utilization minimization [36], while less energy-demanding hardware, like the application-specific integrated circuits (ASICs), can be applied for sustainable smart city services [30]. Generally, for accomplishing long-range sustainability of blockchain-enabled smart city services from economic, environmental, and social points of view, less energy-intensive frameworks are desired to be implemented [29].

VI. Conclusions

Blockchain appears as a unmanageable technology for secure relationship between peers within an untrusted environment. In this paper, we have investigated the role of blockchain in smart cities by initially discussing the inherent technologies in blockchain technology. In following, numerous challenges regarding blockchain technology in the domain of IoT are recognized and the way of addressing them is proposed. In addition, we examined the elementary prerequisites for the application of blockchain in smart cities and displayed the research challenges anticipating blockchain from becoming a key innovation in smart cities.

Furthermore, blockchain can be identified as a significant technology in the era of an information-driven world. Novel mechanisms in blockchain frameworks along with their applications in smart cities for improving life quality are prevalent in modern research communities. What is more, several challenges and prerequisites limitations are still to be identified in order to be solved for applying blockchain in the area of IoT-based smart cities.

Acknowledgement

Supported by the Erasmus+ KA2 under the project DEVOPS, "DevOps competences for Smart Cities" (Project No.: 601015-EPP-1-2018-1-EL-EPPKA2-SSA Erasmus+ Program, KA2: Cooperation for innovation and the exchange of good practices-Sector Skills Alliances, started in 2019, January 1).

References

[1] S. Angraal, H. M. Krumholz, and W. L. Schulz. Blockchain technology: Applications in health care. *Circulation: Cardiovascular Quality and Outcomes*, 10(9):e003800, 2017.

[2] A. Asgaonkar and B. 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. *CoRR*, abs/1806.08379, 2018.

[3] A. B. Ayed. A conceptual secure blockchain based electronic voting system. *International Journal of Network Security & Its Applications*, 9(3):01–09, 2017.

[4] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman. Medrec: Using blockchain for medical data access and permission management. In *2nd International Conference on Open and Big Data (OBD)*, pages 25–30, 2016.

[5] N. Z. Benisi, M. Aminian, and B. Javadi. Blockchain-based decentralized storage networks: A survey. *Journal of Network and Computer Applications*, 162:102656, 2020.

[6] K. Bhaskaran, P. Ilfrich, D. Liffman, C. Vecchiola, P. Jayachandran, A. Kumar, F. Lim, K. Nandakumar, Z. Qin, V. Ramakrishna, E. G. S. Teo, and C. H. Suen. Double-blind consent-driven data sharing on blockchain. In *IEEE International Conference on Cloud Engineering (IC2E)*, pages 385–391, 2018.

[7] G. Caridakis, G. Siolas, P. Mylonas, S. D. Kollias, and A. Stafylopatis. Intelligent and adaptive pervasive future internet: Smart cities for the citizens. In *14th International Conference on Engineering Applications of Neural Networks (EANN)*, volume 384, pages 269–281, 2013.

[8] N. Chalaemwongwan and W. Kurutach. State of the art and challenges facing consensus protocols on blockchain. In *2018 International Conference on Information Networking (ICOIN)*, pages 957–962, 2018.

[9] N. Chaudhry and M. M. Yousaf. Consensus algorithms in blockchain: Comparative analysis, challenges and opportunities. In *12th International Conference on Open Source Systems and Technologies (ICOSST)*, pages 54–63, 2018.

[10] J. A. Garay, A. Kiayias, and N. Leonardos. The bitcoin backbone protocol: Analysis and applications. In *34th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, volume 9057, pages 281–310, 2015.

[11] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun. Is bitcoin a decentralized currency? *IEEE Security and Privacy*, 12(3):54–60, 2014.

[12] S. Hakak, W. Z. Khan, G. A. Gilkar, M. Imran, and N. Guizani. Securing smart cities through blockchain technology: Architecture, requirements, and challenges. *IEEE Network*, 34(1):8–14, 2020.

[13] H. R. Hasan and K. Salah. Proof of delivery of digital assets using blockchain and smart contracts. *IEEE Access*, 6:65439–65448, 2018.

[14] S. S. Hazari and Q. H. Mahmoud. A parallel proof of work to improve transaction speed and scalability in blockchain systems. In *IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 916–921, 2019.

[15] M. Khan, B. N. Silva, and K. Han. Internet of things based energy aware smart home control system. *IEEE Access*, 4:7556–7566, 2016.

[16] M. A. Khan and K. Salah. Iot security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82:395–411, 2018.

[17] H. Kim, J. Park, M. Bennis, and S. Kim. Blockchained on-device federated learning. *IEEE Communications Letters*, 24(6):1279–1283, 2020.

[18] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon. Federated learning: Strategies for improving communication efficiency. *CoRR*, abs/1610.05492, 2016.

[19] A. Krania, M. Statiri, A. Kanavos, and A. K. Tsakalidis. Internet of things services for healthcare systems. In *8th International Conference on Information, Intelligence, Systems & Applications (IISA)*, pages 1–6, 2017.

[20] N. Kshetri and J. M. Voas. Blockchain-enabled e-voting. *IEEE Software*, 35(4):95–99, 2018.

[21] U. Majeed, L. U. Khan, I. Yaqoob, S. M. A. Kazmi, K. Salah, and C. S. Hong. Blockchain for iot-based smart cities: Recent advances, requirements, and future challenges. *Journal of Network and Computer Applications*, 181:103007, 2021.

[22] A. Mantelero. The EU proposal for a general data protection regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review*, 29(3):229–235, 2013.

[23] M. Mettler. Blockchain technology in healthcare: The revolution starts here. In *18th IEEE International Conference on e-Health Networking, Applications and Services (Healthcom)*, pages 1–3, 2016.

[24] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. R. Brooks. A brief survey of cryptocurrency systems. In *14th Annual Conference on Privacy, Security and Trust (PST)*, pages 745–752, 2016.

[25] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260, 2008.

[26] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne. Integration of blockchain and cloud of things: Architecture, applications and challenges. *IEEE Communications Surveys and Tutorials*, 22(4):2521–2549, 2020.

[27] S. S. Panda, U. Satapathy, B. K. Mohanta, D. Jena, and D. Gountia. A blockchain based decentralized authentication framework for resource constrained IOT devices. In *10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pages 1–6, 2019.

[28] M. H. U. Rehman, I. Yaqoob, K. Salah, M. Imran, P. P. Jayaraman, and C. Perera. The role of big data analytics in industrial internet of things. *Future Generation Computer Systems*, 99:247–259, 2019.

[29] C. Schinckus. The good, the bad and the ugly: An overview of the sustainability of blockchain technology. *Energy Research & Social Science*, 69:101614, 2020.

[30] J. Sedlmeir, H. U. Buhl, G. Fridgen, and R. Keller. The energy consumption of blockchain technology: Beyond myth. *Business & Information Systems Engineering*, 62(6):599–608, 2020.

[31] A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian. A survey on the adoption of blockchain in iot: Challenges and solutions. *Blockchain: Research and Applications*, page 100006, 2021.

[32] A. Vlachostergiou, G. Stratogiannis, G. Caridakis, G. Siolas, and P. Mylonas. Smart home context awareness based on smart and innovative cities. In *16th International Conference on Engineering Applications of Neural Networks (EANN)*, pages 32:1–32:10, 2015.

[33] G. Vonitsanos, T. Panagiotakopoulos, A. Kanavos, and A. K. Tsakalidis. Forecasting air flight delays and enabling smart airport services in apache spark. In *17th International Conference on Artificial Intelligence Applications and Innovations (AIAI)*, volume 628, pages 407–417, 2021.

[34] E. K. Wang, Z. Liang, C. Chen, S. Kumari, and M. K. Khan. Porx: A reputation incentive scheme for blockchain consensus of iiot. *Future Generation Computer Systems*, 102:140–151, 2020.

[35] Y. Yuan and F. Wang. Towards blockchain-based intelligent transportation systems. In *19th IEEE International Conference on Intelligent Transportation Systems (ITSC)*, pages 2663–2668, 2016.

[36] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *IEEE International Congress on Big Data*, pages 557–564, 2017.