EAI Endorsed Transactions
on Smart Cities

Review Article EAI.EU

A Systematic Review of Blockchain-based Services for Security Upgradation of a Smart City

Noushaba Feroz[1,*]

[1]Department of Computer Science and Engineering, SEST, Jamia Hamdard University, New Delhi India.

Abstract

The concept of smart city has gained popularity in recent years. The elementary concept refers to promoting the uninterrupted sharing of data and services within and across communities by the application of emerging technologies. Smart cities strive for cost reduction, optimal use of resources and the development of a more sustainable environment. Considerable advances in modern technologies such as IoT and wireless communication have enabled sharing of data between remote devices which are geared with open data, hence a smart city is susceptible to a number of security threats. It is important to identify these threats, analyze IoT data to improve privacy and security and identify the corresponding consequences. Blockchain has emerged as a promising solution to resolve these challenges. Blockchain is a peer-to-peer shared database technology that cannot be modified once a transaction is recorded and validated. This study explores the contribution of blockchain to smart cities in terms of decentralized security, immutability, transparency and privacy to provide intelligent, customized and context-aware services to smart city dwellers. A brief overview of this novel technology has been given along with its deployment in a smart city setting, the open issues discussed and prospective scope of blockchain application has been presented.

Keywords: Smart City, Blockchain, IoT, Decentralization, Security.

Received on 29 January 2020, accepted on 22 March 2020, published on 24 March 2020

doi: 10.4108/eai.13-7-2018.163840

*Corresponding author. Email:noushaba.feroz@gmail.com

1. Introduction

Smart City is defined as an urbanized area with information and communication technology (ICT) central to its framework. In order to enhance the quality of life, smart cities provide various novel and specialized services to their citizens. A smart city must include state-of-the-art technology, essentially the Internet of Things (IoT), to offer these services in compliance with privacy and security (Verma, A. et al., 2019). Moreover, smart city policies have gained significant attention and support lately. It is apparent that these policies favor urban economic growth (Caragliu and Del Bo, 2018). Smart City literature highlights the need for a local context in which large-scale funding in cutting-edge technologies is fully exploited (Caragliu et al., 2011).

The notion of smart city has evolved significantly over the last decade with the emergence of the Internet of Things (IoT) as a new trend in promoting sustainability. The World Urbanization Prospects Report (United Nations, 2018) reports that 55% of the global population resides in urban areas, a percentage that is expected to rise to 68% by 2050. Moreover, it is estimated that by 2050, approximately 2.5 billion people will be additionally led to urban areas as a result of the steady transfer of people from rural to urban areas. The increasing congestion, carbon dioxide concentration, greenhouse gas emissions and waste disposal in the urban areas will gradually affect living conditions of the people. Consequently, the consolidation of billions of devices and services under a smart framework is imperative in the near future, ranging from user devices to smart travel, business, buildings, hospitals, energy and ecosystem.

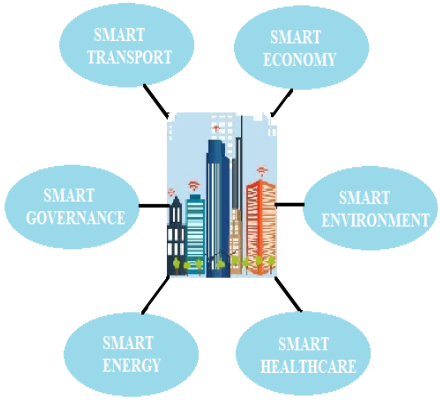

Fig. 1. Components of a Smart City

The prevailing technology revolution has prompted a number of cities around the globe to make huge investments in the design and implementation of smart city plans and proposals to address the critical challenges of rapid urbanization and climate change (Sharifi, A., 2019). In the midst of global urbanization developments, local authorities are posed with pressing issues to satisfy swiftly advancing citizen requirements while tackling the crucial intricacies of world-wide sustainability (Clarke,R., 2013; NIST, 2018; Stratigea et al., 2015). Smart cities are built on an integrated, self-governing and distributed architecture that involves many sensors that capture and send data to base stations, and numerous Internet-enabled devices that provide connectivity for the processing of data. Every individual device produces significant data uninterruptedly to be sent to data centers for processing via heterogeneous networks and subjected to subsequent analysis for decision-making (Albino, V. et al., 2015). Data is, for any individual in the modern world, the most valuable asset. This data may include personal details such as credit card numbers, contact information, bank account details, location coordinates or medical reports including many others. These details are managed by hardware and software modules that might be susceptible to unauthorized access (Popescul, D. and Genete, L.D., 2016). The advanced technologies incorporated in smart cities must resolve the public concerns regarding privacy and security, especially regarding the data deemed as significantly sensitive (Van Zoonen, L., 2016). Privacy and security is a paramount challenge with regard to technical issues, together with other concerns such as interoperability and technological expenses (Naphade, M. et al., 2011). Safeguarding data from malicious attacks, viruses, frauds and other vicious actions is a fundamental task of information security (Ijaz, S. et al., 2016) and any adverse impact of information security greatly affects the society's economic aspects (Anderson, R., 2001).

A Smart City is an instance of an infrastructure that facilitates people and organizations to collaborate, at any level, for public welfare. A robust approach of achieving this is to effectively decentralize any mechanism which can evade the control of a single and centralized administration without requiring any involved party to trust the other. Gartner's study estimates the prevalence of 20 billion connected devices by the year 2020 (Panetta, K., 2017). The massive amount of data generated by these devices would pose serious data management and security challenges. In case this saturation affects the central server or database, all the connected devices will be affected consequently. A fair and transparent data sharing environment may be set up by utilizing blockchain in which unauthorized data alterations can be monitored and traced.

Blockchain allows distributed storage of data and essentially autonomous peer-to-peer communication between IoT devices. Hence, fault in one device doesn't impair the operation of the other devices. Moreover, blockchain offers encrypted data management and access control in its deployment (Fan, L. et al., 2018). Blockchain, though originally developed to assist crypto-currency, can be used without an intermediary in any kind of transaction. Blockchain offers flexible access for maintaining anonymity by providing viable features such as the use of alias accounts (Zyskind, G. and Nathan, O., 2015). The advantage of blockchain is that an attacker must compromise 51% of the systems (51% attack) in order to surpass the target network's hashing power. Therefore, attempting to target a blockchain network is computationally unrealistic (Biswas, K. and Muthukkumarasamy, V., 2016). Smart city, with aggregate elements including but not limited to smart resource use, transportation, healthcare, governance and economy, is the most prospective domain for blockchain application. Blockchain can be leveraged to provide real-time verification, permission, transparency, security and privacy that are not effective in smart city environment via a centralized system (Kshetri, N. and Voas, J., 2018). A smart city aims to create greater social value, as well as to support administrative performance, citizen flexibility and technological development by the application of novel technology and organizational methods. The blockchain system meets the basic requirements of a smart city as a distributed data storage and mutual communication framework (Sun, M. and Zhang, J., 2020).

This manuscript is divided into five sections. Section 2 presents a brief overview of the blockchain technology and its deployment in a smart city, section 3 discusses 15 recent works in this domain, section 4 depicts open issues in current blockchain implementations and section 5 discusses the prospective scope of this technology in a smart city setting.

2. Blockchain Overview and Smart City Deployment

A blockchain is characterized as a distributed ledger (database) that holds the transactional data indefinitely and immutably. The use of a peer-to-peer network renders a blockchain fully decentralized. More specifically, a duplicate of the ledger is maintained at every network node to prevent a single failure point. All the copies are modified and audited concurrently (Hammi, M. T. et al., 2018). Blockchain facilitates communication among non-trusting parties without the need for a trusted authority (Christidis, K. and Devetsikiotis, M., 2016)

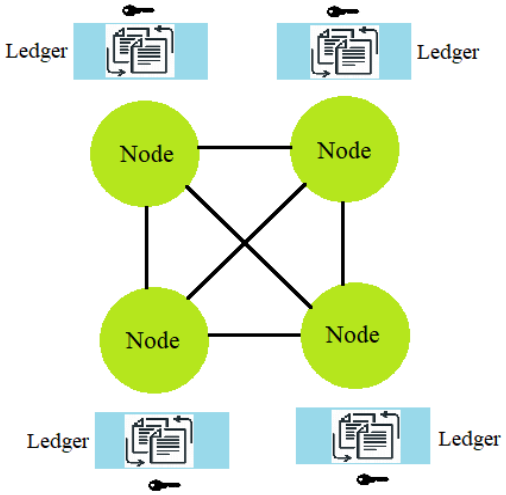

Fig. 2. Blockchain Structure

Satoshi Nakamoto, the anonymous individual/group behind the Bitcoin cryptocurrency, stated nearly a decade ago that blockchain technology, a decentralized peer-to-peer connected system, could be utilized to address the challenge of preserving transactional sequence and to prevent the double-spending issue (Nakamoto, S., 2019). In Bitcoin, transactions are ordered and those with the same timestamp are grouped together in structures of restricted size called blocks. Network nodes (miners) link the blocks to each other in a temporal sequence, with each block holding the hash of the preceeding block for blockchain creation (Crosby, M. et al., 2016). Thus, a reliable and auditable database for all transactions is included in the blockchain architecture. As part of a security matrix, blockchain mechanisms (BCMs), play a role in protecting multiple IoT-based applications. Blockchain architecture and design inherently offers advantages such as security, verifiability, robustness and transparency (Greenspan, G., 2015; Christidis, K. and Devetsikiotis, M., 2016). Blockchain technology has six elements at its core, viz. Autonomy, Decentalization, Transparency, Anonymity, Immutability and Open Source access (Niranjanamurthy, M. et al., 2019). Blockchain has garnered significant attention due to its ability to facilitate relaible transactions through networked computation replacing human supervision and control (Casino, F. et al., 2019). Consequently, it has emerged recently as a new form of data and service organization, supporting the operations of diverse fields beyond its originally intended application area, such as finance, governance, IoT, healthcare, business, education, energy and other miscellaneous domains. Depending on the target audience, three generations of blockchains exist (Zhao, J. L. et al., 2016): Blockchain 1.0 (supporting digital cryptocurrency transactions), Blockchain 2.0 (involving digital finance) and Blockchain 3.0 (covering digital society such as government, health, science and IoT). Governments are responsible for maintaining and storing official records of citizens and/or organizations throughout years. Blockchain-enabled technologies may alter how local or state governments function by eliminating the need of intermediataries for record-handling (Reijers, W. et al., 2016; Hou, H., 2017). Blockchain provides liable, autonomous, secure and transparent record-keeping that would ultimately inhibit corruption and increase the government performance. Blockchain could serve as a secure framework for the physical, social and organizational incorporation into a smart city environment. The surmounting data generation rates are likely to rise with the emergence of IoT and the ongoing population explosion (I. W.Stats, 2019). Although blockchain and IoT already have vast application areas of their own, their intrinsic relationship gives birth to endless possibilities. The growing interest and funding for deploying decentralized IoT systems (Samaniego, M. and Deters, R., 2016; Zhang, Y. and Wen, J., 2017; Novo, O., 2018) is largely driven by the development of blockchain and its innate abilities (Christidis, K. and Devetsikiotis, M., 2016) aiming to ensure secure and verifiable transactions. Moreover, blockchain interoperability facilitates the improvement of conventional transportation and commerce by incorporating secure and autonomous real-time payment services (Christidis, K. et al., 2016).

3. Literature Review

Sun, J. et al. (2016) have discussed how blockchain-based sharing services can contribute to smart cities based on a hypothetical structure. To understand the impact of evolving blockchain technology on the development of smart cities, the authors have suggested examination perspective to determine the fundamental components of smart cities. They have proposed a three-dimensional theoretical framework, comprising of human, technology and organization, based on available literature and discuss a number of core factors that make a city smart from a sharing economy viewpoint. The authors have used this

framework to examine the effect of blockchain on smart cities and aim to comprehend the meaning of 'smart' in the term 'smart city' from a sharing economy perspective to understand the needs of smart cities and how new technology might support them. Biswas, K. and Muthukkumarasamy, V. (2016) have introduced a four-layer blockchain-based security arrangement that allows the institutions of a smart city to connect without risking privacy and security. They have classified smart city threats into five groups, viz. Availability Threats (unauthorized resource maintenance), Integrity Threats (unauthorized data modification), Confidentiality Threats (sensitive information disclosure), Authenticity Threats (unauthorized access to resource and sensitive information) and Accountability Threats (denial of transmission or reception) and propose a secure framework based on blockchain to address these threats in a smart city setting. The authors in (Ibba, S. et al., 2017) have proposed a solution to the problem of storage and management of sensor data using blockchain technology. They have applied Scrum methodology, characterized by flexibility, adaptability and iteratation, to develop the blockchain-based system "CitySense". The proposed system encorgages proactive collaboration of the people and creates the city's health map to acquire real time data and formulate real time remedies. The authors in (Rivera, R. et al., 2017) have presented a comprehensive analysis to compile all the available research of digital identity on blockchain technology in a smart city setting. The findings of their study reveal that the use of blockchain for digital identity is at its initial stage of development. The authors have endorsed the forthcoming deployment of blockchain as a digital identity tool and for the verification of citizens in a multitude of digital services that are available currently. Hammi, M.T. et al. (2018) have proposed a novel decentralized system "Bubbles of Trust" which guarantees robust identification and verification of devices. The system leverages the security benefits offered by public blockchains to protect data integrity and availability so that devices can communicate in a fully secure way. Moreover, the authors have built a threat model that complies with the required safety parameters and is robust against threats. Sharma, P.K. and Park, J.H. (2018) have introduced a novel hybrid model "DistBlockNet" for smart city network that exploits the combined capabilities of innovative technologies of centralized Software Defined Networking (SDN) and decentralized blockchain. The model guarantees privacy and security, and prohibits intruders from accessing data on a secure smart city network. The authors in (Pieroni, A. et al., 2018) have presented a review of the smart environment aspect of a smart city setting, specifically the deployment of smart energy grid for smart city residents. They have proposed incorporating blockchain in the grid and using the blockchain granting ledger for information sharing and transactions between citizens and energy providers. The authors have also introduced a mobile application to facilitate access to the blockchain network. Minoli, D. and Occhiogrosso, B. (2018) have discussed several IoT scenarios where blockchain mechanisms (BCMs) are significant but also suggest that BCMs are just component of the IoT Security (IoTSec) solution. They have summarized and advocated the general use of BCMs for security in IoT with specific focus on e-Health and Intelligent Transport Systems (ITS). The authors have indicated that the application of a complete blockchain protected network in all IoT applications is not realistic due to the general constraints of IoT nodes. They have further asserted that BCMs (firewalling, encryption etc.) must be paired with other security mechanisms for in-depth protection. Michelin, R.A. et al. (2018) have proposed a flexible and private data sharing infrastructure so that the massive amount of sensor data generated by smart vehicles could be leveraged to facilitate a broad range of services in a city. The authors have proposed a framework called "SpeedyChain", which utilizes blockchain technology to allow smart vehicles to exchange their information in a decentralized and secure manner, while preserving anonymity, essence and transparency. Unlike traditional blockchain implementations, this novel architecture incorporates a blockchain mechanism to decouple the data stored in block header transactions so that data may be added to blocks swiftly. Kushch, S. and Prieto-Castrillo, F. (2019) have discussed the deployment of blockchain technology as an IoT component in sensor networks. The authors have introduced the notion of "Rolling Blockchain" intended for building wireless sensor networks together with smart cars and can be applied to IoT and smart city sensor networks. Citing the Estonia blockchain service case, Noh, J.H. and Kwon, H.Y. (2019) have advocated that the blockchain technology is more efficient than 4G technology with a super-low latency of 0.001 seconds, when applied to 5G-based smart city infrastructure. The authors have proposed the simplification of authentication process and the standardization of overall development platform to enhance user experience. Furthermore, they have advocated for the establishment of a code of conduct and insurance policies to facilitate accountability of service providers for any damage due to compromised data. Aggarwal, S. et al. (2019) have discussed the applications of blockchain technology in a smart city setting, with an emphasis on core blockchain components. A comprehensive application taxonomy, process models used and communication infrastructure support required to run different applications have been provided. Additionally, the authors have identified various potential challenges and opportunities for research with focus on the need to develop a lightweight blockchain system, especially for constrained applications, and the assurance of interoperability across different blockchain frameworks. The authors in (Khare, A., et al., 2019) have built and deployed decentralized Distributed Ledger Technology (DLT) based technologies such as "BigchainDB" for sensing, collection, storage and use of data in the real-world smart city deployment, "#SmartME". They have proposed a trust-free strategy for the collection, storage and use of sensor data generated in

a smart city to deal with the issues of completeness, availability and non-modifiability of accessible datasets produced by sensing operations. Rahman, M.A. et al. (2019) have proposed a blockchain-based framework to facilitate secure and confidential spatial-temporal smart contract services that support a sustainable IoT in smart cities. The proposed infrastructure is a sharing economy system based on mobile edge computing (MEC) that uses blockchain and off-chain structure to store unmodifiable data, allowing protected smart city infrastructure, including sharing economy, smart contracts, IoT and blockchain connectivity, to be enabled. Sun, M. and Zhang, J. (2020) have conducted a survey of the function of smart big data platform and have analyzed the development of the smart city of Hefei. The authors have suggested the use of blockchain technology to build a decentralized peer-to-peer security network combined with the current Public Key Infrastructure/Certification Authority (PKI / CA) security system to develop a novel model. Based on this model, the authors have designed the architecture of blockchain smart city for information sharing and communication. Table 1. summarizes the proposals/findings of the papers discussed above.

Table 1. Proposals/Findings of Literature Review

S.No.	Author (Year)	Proposals/Findings
1.	Sun, J. et al. (2016)	Three-dimensional theoretical framework (human, technology and organization) to examine the effect of blockchain on smart cities from a sharing economy perspective.
2.	Biswas, K. and Muthukkumarasamy, V. (2016)	Four-layer (physical, communication, database, interface) blockchain-based security arrangement. Five groups of threats classified (Availability, Integrity, Confidentiality, Authenticity, Accountability).
3.	Ibba, S. et al. (2017)	Blockchain-based system "CitySense" developed on Scrum methodology
4.	Rivera, R. et al. (2017)	Deployment of blockchain as a digital identity tool for the verification of citizens in a multitude of digital services.
5.	Hammi, M.T. et al. (2018)	Decentralized system namely "Bubbles of Trust" for robust identification and verification of devices. Threat model complying with required safety parameters and robust against threats.
6.	Sharma, P.K. and Park, J.H. (2018)	Hybrid model namely "DistBlockNet" for smart city network based on centralized Software Defined Networking (SDN) and decentralized blockchain.
7.	Pieroni, A. et al. (2018)	Incorporation of blockchain in smart energy grid and mobile application to facilitate access to the blockchain network.
8.	Minoli, D. and Occhiogrosso, B. (2018)	Blockchain mechanisms (BCMs) for security in IoT with specific focus on e-Health and Intelligent Transport Systems (ITS).
9.	Michelin, R.A. et al. (2018)	Framework called "SpeedyChain", utilizing blockchain technology to allow smart vehicles to exchange their information in a decentralized and secure manner.
10.	Kushch, S. and Prieto-Castrillo, F. (2019)	Concept of "Rolling Blockchain" for building wireless sensor networks together with smart cars applied to IoT and smart city sensor networks.
11.	Noh, J.H. and Kwon, H.Y. (2019)	Simplification of authentication process and the standardization of overall development platform to enhance user experience.
12.	Aggarwal, S. et al. (2019)	Blockchain application taxonomy, process models and communication infrastructure support to run different applications in smart city.

13.	Khare, A., et al. (2019)	Decentralized distributed ledger technology (DLT) based technologies such as "BigchainDB" for sensing, collection, storage and use of data in the real-world smart city deployment, "#SmartME".
14.	Rahman, M.A. et al. (2019)	Blockchain-based framework for secure and confidential spatial-temporal smart contract services.
15.	Sun, M. and Zhang, J. (2020)	Blockchain-based decentralized peer-to-peer security network combined with Public Key Infrastructure/ Certification Authority (PKI / CA) security system.

4. Open Issues in Current Blockchain Implementations

There are at least three major hurdles to blockchain deployment in a smart city setting which are prevalent in all implementations and have not been addressed effectively yet, viz. scalability, privacy and interoperability (Tapas, N. et al., 2018). Although a number of IT experts contemplate the use of blockchain in almost all ventures, they do not fully understand the key reasons for its use, especially in terms of data management. As an example, blockchain will not add any value to current technical solutions if no data has to be stored at all. Likewise, when only one writer is required in a given system, blockchain is not a guaranteed better option compared to traditional database from the perspective of efficiency (Greenspan, G., 2015).

It is important to examine the appropriateness of blockchain technology against the application specifications before implementing blockchain-enabled solutions (Lo, S.K. et al., 2017). The wastage of mining network resources is one of the key drawbacks of blockchain technology, which particularly affects public blockchains. China-led bitcoin mining (Blockchain HashRate Distribution, 2020) uses more energy than 159 countries worldwide (Digiconomist, 2020). Nonetheless, actual power usage may be far worse as users might be mining unknowingly owing to malware infections (Malwarebytes, 2017). There is a rapid increase in blockchain-based implementations, producing an enormous amount of heterogeneous solutions. The wide array of functionalities and deployments implies interoperability challenges that prevent standardization (Casino, F. et al., 2019). Data protection and confidentiality is still a concern for blockchains, since data is stored as a public archive. Transactional privacy is a prominent blockchain issue (Rahman, M.A. et al., 2017). The traceability of transactions and smart city processes distributed across the network worries both individuals and businesses. Additionally, the use of aliases does not necessarily ensure transactional data to be secure (Kosba et al. 2016). While blockchains preserve confidentiality and privacy, asset safety depends on the security of a digital identity, the private key. No third party can retrieve a private key if it is compromised or lost. Therefore, it is almost impossible to identify the perpetrator and all the assets that a person owns in the blockchain will disappear (Xu, J.J., 2016). Furthermore, decisions stored on a blockchain cannot be reversed and there is the threat of an impending majority attack (51% attack) (Zhu, L. 2019).

5. Conclusion and Future Scope

Ensuing technological advances envisage a super-connected world. In this anticipated super-connected setting, the technologies that can most securely and effectively implement an exponential growth of big data for a service are required. To this end, blockchain is a viable option.

Innovative technologies such as cloud computing, big data, IoT, edge computing artificial intelligence, machine learning, together with urban planning, construction, maintenance and functioning are integral elements of a smart city. This demands a framework of innovation, collaboration, sustenance, transparency and security to promote healthy urban development. With vital characteristics including security, immutability, transparency and decentralization, blockchain has emerged as a promising candidate for consideration in a smart city environment. It will ultimately promote the sustainable and healthy growth of smart cities.

Future research should, among other things, focus on identifying which smart city applications are best suited to implement blockchain safety mechanisms on a practical level. Furthermore, researchers need to explore how to deploy a revocation mechanism for compromised smart devices.

References

[1] Aggarwal, S., Chaudhary, R., Aujla, G.S., Kumar, N., Choo, K.K.R. and Zomaya, A.Y., 2019. Blockchain for smart communities: Applications, challenges and opportunities. Journal of Network and Computer Applications.

[2] Albino, V., Berardi, U. and Dangelico, R.M., 2015. Smart cities: Definitions, dimensions, performance, and initiatives. Journal of urban technology, 22(1), pp.3-21.

[3] Anderson, R., 2001, December. Why information security is hard-an economic perspective. In Seventeenth Annual

Computer Security Applications Conference (pp. 358-365). IEEE.
[4] Biswas, K. and Muthukkumarasamy, V., 2016, December. Securing smart cities using blockchain technology. In 2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS) (pp. 1392-1393). IEEE.
[5] Blockchain Hashrate Distribution, 2020. https://www.blockchain.com/en/pools. Accessed on: 20 Jan 2020.
[6] Caragliu, A. and Del Bo, C.F., 2019. Smart innovative cities: The impact of Smart City policies on urban innovation. Technological Forecasting and Social Change, 142, pp.373-383.
[7] Caragliu, A., Del Bo, C. and Nijkamp, P., 2011. Smart cities in Europe. Journal of urban technology, 18(2), pp.65-82.
[8] Casino, F., Dasaklis, T.K. and Patsakis, C., 2019. A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics and Informatics, 36, pp.55-81.
[9] Christidis, K. and Devetsikiotis, M., 2016. Blockchains and Smart Contracts for the Internet of Things, IEEE Access 4, pp.2292–2303.
[10] Clarke, R., 2013. Business Strategy: IDC Government Insights' Smart City Maturity Model—Assessment and Action on the Path to Maturity. International Data Corporation (IDC) Government Insights, Business Strategy# GI240620. Alexandria, VA: USA.
[11] Crosby, M., Pattanayak, P., Verma, S. and Kalyanaraman, V., 2016. Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), p.71.
[12] Digiconomist, Bitcoin Energy Consumption Index, https://digiconomist.net/bitcoin-energy-consumption, 2020.
[13] Fan, L., Gil-Garcia, J.R., Werthmuller, D., Burke, G.B. and Hong, X., 2018, May. Investigating blockchain as a data management tool for IoT devices in smart city initiatives. In Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age (pp. 1-2).
[14] Greenspan, G., 2015. Avoiding the pointless blockchain project. https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/. Accessed on: 22 Jan 2020.
[15] Greenspan, G., 2015. Ending the bitcoin vs blockchain debate, http://www.multichain.com/blog/2015/07/bitcoin-vs-blockchaindebate. Accessed on: 20 Jan 2020.
[16] Hammi, M.T., Hammi, B., Bellot, P. and Serhrouchni, A., 2018. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. Computers & Security, 78, pp.126-142.
[17] Hou, H., 2017, July. The application of blockchain technology in E-government in China. In 2017 26th International Conference on Computer Communication and Networks (ICCCN) (pp. 1-4). IEEE.
[18] Ibba, S., Pinna, A., Seu, M. and Pani, F.E., 2017, May. CitySense: blockchain-oriented smart cities. In Proceedings of the XP2017 Scientific Workshops (pp. 1-5).
[19] Ijaz, S., Shah, M.A., Khan, A. and Ahmed, M., 2016. Smart cities: A survey on security concerns. International Journal of Advanced Computer Science and Applications, 7(2), pp.612-625.
[20] I. W. Stats, 2019. Internet usage statistics, The internet big picture, http://www.internetworldstats.com/stats.htm. Accessed on: 21 Jan 2020.
[21] Khare, A., Merlino, G., Longo, F., Puliafito, A. and Vyas, O.P., 2019. Design of a Trustless Smart City system: The# SmartME experiment. Internet of Things, p.100126.
[22] Kosba, A., Miller, A., Shi, E., Wen, Z. and Papamanthou, C., 2016, May. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In 2016 IEEE symposium on security and privacy (SP) (pp. 839-858). IEEE.
[23] Kshetri, N. and Voas, J., 2018. Blockchain in developing countries. It Professional, 20(2), pp.11-14.
[24] Kushch, S. and Prieto-Castrillo, F., 2019, April. Blockchain for dynamic nodes in a smart city. In 2019 IEEE 5th World Forum on Internet of Things (WF-IoT) (pp. 29-34). IEEE.
[25] Lo, S.K., Xu, X., Chiam, Y.K. and Lu, Q., 2017, November. Evaluating suitability of applying blockchain. In 2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS) (pp. 158-161). IEEE.
[26] Malwarebytes, 2017. Persistent drive-by cryptomining coming to a browser near you, https://blog.malwarebytes.com/cybercrime/2017/11/persistent-drive-by-cryptomining-coming-to-a-browser-near-you/. Accessed on 15 Jan 2020.
[27] Michelin, R.A., Dorri, A., Steger, M., Lunardi, R.C., Kanhere, S.S., Jurdak, R. and Zorzo, A.F., 2018, November. 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 (pp. 145-154).
[28] Minoli, D. and Occhiogrosso, B., 2018. Blockchain mechanisms for IoT security. Internet of Things, 1, pp.1-13.
[29] Nakamoto, S., 2019. Bitcoin: A peer-to-peer electronic cash system. Manubot.
[30] Naphade, M., Banavar, G., Harrison, C., Paraszczak, J. and Morris, R., 2011. Smarter cities and their innovation challenges. Computer, 44(6), pp.32-39.
[31] Niranjanamurthy, M., Nithya, B.N. and Jagannatha, S., 2019. Analysis of blockchain technology: pros, cons and SWOT. Cluster Computing, 22(6), pp.14743-14757.
[32] NIST, 2008. IES-City Framework: A Consensus Framework for Smart City Architectures. National Institite of Standards and Technology.
[33] Noh, J.H. and Kwon, H.Y., 2019, January. A study on smart city security policy based on blockchain in 5g age. In 2019 International Conference on Platform Technology and Service (PlatCon) (pp. 1-4). IEEE.
[34] Novo, O., 2018. Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal, 5(2), pp.1184-1195.
[35] Panetta, K., Smart Cities Look to the Future, 2017. https://www.gartner.com/smarterwithgartner/smart-cities-look-to-the-future/, Accessed on 17 Jan 2020.
[36] Pieroni, A., Scarpato, N., Di Nunzio, L., Fallucchi, F. and Raso, M., 2018. Smarter city: smart energy grid based on blockchain technology. Int. J. Adv. Sci. Eng. Inf. Technol, 8(1), pp.298-306.
[37] Popescul, D. and Genete, L.D., 2016. Data security in smart cities: challenges and solutions. Informatica Economică, 20(1).

[38] Rahman, M.A., Azad, S. and Kabir, M.N., 2017, April. Blockchain security hole: Issues and solutions. In International Conference of Reliable Information and Communication Technology (pp. 739-746). Springer, Cham.
[39] Rahman, M.A., Rashid, M.M., Hossain, M.S., Hassanain, E., Alhamid, M.F. and Guizani, M., 2019. Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city. IEEE Access, 7, pp.18611-18621.
[40] Reijers, W., O'Brolcháin, F. and Haynes, P., 2016. Governance in blockchain technologies & social contract theories. Ledger, 1, pp.134-151.
[41] Rivera, R., Robledo, J.G., Larios, V.M. and Avalos, J.M., 2017, September. How digital identity on blockchain can contribute in a smart city environment. In 2017 International smart cities conference (ISC2) (pp. 1-4). IEEE.
[42] Samaniego, M. and Deters, R., 2016, December. Blockchain as a Service for IoT. In 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 433-436). IEEE.
[43] Sharifi, A., 2019. A critical review of selected smart city assessment tools and indicator sets. Journal of cleaner production, 233, pp.1269-1283.
[44] Sharma, P.K. and Park, J.H., 2018. Blockchain based hybrid network architecture for the smart city. Future Generation Computer Systems, 86, pp.650-655.
[45] Stratigea, A., Papadopoulou, C.A., Panagiotopoulou, M., 2015. Tools and Technologies for planning the development of smart cities. J. Urban Technol. 22 (2), 43e62.
[46] Sun, J., Yan, J. and Zhang, K.Z., 2016. Blockchain-based sharing services: What blockchain technology can contribute to smart cities. Financial Innovation, 2(1), pp.1-9.
[47] Sun, M. and Zhang, J., 2020. Research on the application of block chain big data platform in the construction of new smart city for low carbon emission and green environment. Computer Communications, 149, pp.332-342.
[48] Tapas, N., Merlino, G. and Longo, F., 2018, June. Blockchain-based IoT-cloud authorization and delegation. In 2018 IEEE International Conference on Smart Computing (SMARTCOMP) (pp. 411-416). IEEE.
[49] United Nations, 2018. 2018 revision of world urbanization prospects.
[50] Van Zoonen, L., 2016. Privacy concerns in smart cities. Government Information Quarterly, 33(3), pp.472-480.
[51] Xu, J.J., 2016. Are blockchains immune to all malicious attacks? Financial Innovation, 2(1), pp.1-9.
[52] Verma, A., Khanna, A., Agrawal, A., Darwish, A. and Hassanien, A.E., 2019. Security and privacy in smart city applications and services: Opportunities and challenges. In Cybersecurity and Secure Information Systems (pp. 1-15). Springer, Cham.
[53] Zhang, Y. and Wen, J., 2017. The IoT electric business model: Using blockchain technology for the internet of things. Peer-to-Peer Networking and Applications, 10(4), pp.983-994.
[54] Zhao, J.L., Fan, S. and Yan, J., 2016. Overview of business innovations and research opportunities in blockchain and introduction to the special issue, pp. 1-7.
[55] Zyskind, G. and Nathan, O., 2015, May. Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE.