Journal of Network and Computer Applications 181 (2021) 103007

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges[☆]

Umer Majeed[a], Latif U. Khan[a], Ibrar Yaqoob[b], S.M. Ahsan Kazmi[c], Khaled Salah[b], Choong Seon Hong[a,*]

[a] Department of Computer Science & Engineering, Kyung Hee University, Yongin-Si, South Korea
[b] Department of Electrical Engineering and Computer Science, Khalifa University of Science and Technology, Abu Dhabi, United Arab Emirates
[c] Institute of Information Security and Cyber Physical System, Innopolis University, Innopolis, Tatarstan, Russia

ARTICLE INFO

Keywords:
Blockchain
Ethereum
Internet of Things
Smart city
Security
Smart contracts
Smart environments

ABSTRACT

A remarkable interest in the Internet of Things (IoT)-based smart cities from both academia and industry has been observed in recent years. Smart cities can offer various smart applications such as intelligent transportation, industry 4.0, smart banking, among others, for boosting the life quality of citizens. Security is one of the key challenges of a smart city. 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. First, we present the evolution of blockchain technology in terms of constituent technologies, consensus algorithms, and blockchain platforms. Second, we discuss and critically evaluate various smart applications enabled by blockchain. Third, we present real-world blockchain implementation in smart cities as case studies. Fourth, we present the key requirements to integrate blockchain with smart cities. Finally, we present open research challenges along with their key causes and possible solutions.

1. Introduction

The ongoing development of the Internet of Things (IoT)-based applications, is paving the way towards the development of smart cities (Khan et al., 2020a, 2020b). Smart cities offer intelligent transportation, industry 4.0, smart healthcare, smart homes, smart banking, among others. These applications require immense security for handling data while improving the standard of citizens' life. To enable smart cities with enhanced security and privacy, we can use blockchain (Biswas and Muthukkumarasamy, 2016; Feng et al., 2019). Blockchain is a decentralized, traceable, transparent, and immutable ledger of transnational records in Peer-to-Peer (P2P) networks (Yaqoob et al., 2020). Blockchain was first introduced as bitcoin that is a solution to transfer digital payments between different parties without the need for a central authority (Nakamoto, 2008). Bitcoin has gained huge success with a market capitalization of over US $230 billion in 2017 (Bitcoin Market Capitaliza,). Other than improving the financial industry (Wang et al., 2020a; Kabra et al., 2020), blockchain has potential applications in many other fields such as the IoT (Rathore et al., 2019), e-Commerce, accounting & auditing, e-Voting (Khan et al., 2020c), asset management, identity management (Liu et al., 2020), supply chain, taxation, telecommunication (Nguyen et al., 2020), healthcare (McGhin et al., 2019; Yaqoob et al., 2021) and government public services.

The smart city comprises the ecosystem of smart environments provided in the city which can improvise its inhabitants' lifestyle. Smart city concerns with the adoption of information and communication technologies for enhancement in public welfare, economy, government services, environment, resource management, and urban planning (Razaghi and Finger, 2018). Smart cities envision the use of existing and developing digital technology to enhance every aspect of city life. One of the primary objectives of smart cities is reformed provision of fundamental services like housing, education, healthcare, transportation

[☆] This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the Grand Information Technology Research Center support program(IITP-2021-2015-0-00742) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation).

[*] Corresponding author.
E-mail addresses: umermajeed@khu.ac.kr (U. Majeed), latif@khu.ac.kr (L.U. Khan), ibraryaqoob@ieee.org (I. Yaqoob), a.kazmi@innopolis.ru (S.M.A. Kazmi), khaled.salah@ku.ac.ae (K. Salah), cshong@khu.ac.kr (C.S. Hong).

https://doi.org/10.1016/j.jnca.2021.103007
Received 26 August 2020; Received in revised form 13 December 2020; Accepted 29 January 2021
Available online 16 February 2021
1084-8045/© 2021 Elsevier Ltd. All rights reserved.

(Yang et al., 2020), energy, water (Wu et al., 2020), utilities, surveillance, and law enforcement. Smart cities mitigate the problems of population growth and expeditious urbanization by integrating social, business, and physical infrastructure of the city through technology (Musa, 2018). Recent advancements of technologies such as Information & Communication Technologies (ICT), blockchain, Big Data, machine learning, automation, Artificial Intelligence (AI), and the IoT will make smart cities more interconnected, instrumented, intelligent, livable, safer, sustainable, and resilient.

The performance measures for the success of a smart city constitutes the integration of fundamental services with seamless assimilation in the daily lives of its residents, thereby assuring the effective usage of resources and improving quality of life (Tu, 2018). However, this involves a huge amount of data traffic generated by information systems flowing through communication networks of city technological infrastructure (Al Nuaimi et al., 2015). Blockchain is a solution to the key challenge of security, privacy, and transparency of this personal, organizational, and operational data (Yu et al., 2018; Ma et al., 2020). Several types of transactions of smart cities can be recorded in a blockchain. By using smart contracts, complex legal procedures can be executed and data-exchange can be done automatically. With smart contracts and decentralized applications, blockchain gives a high level of autonomy for executing smart transactions during the operational process of smart city (Ibba et al., 2017). Blockchain can give features like seamless authentication, privacy, security, effortless deployment & maintenance. Tremendous efforts have been made for exploring blockchain applications in smart cities. In (Mohanty et al., (2020)), the role of blockchain for the security of IoT has been discussed. Authors in (Sharma and Park, (2018)) proposed hybrid network architecture for a blockchain-based smart city to tackle communication issues like latency, bandwidth, scalability, security & privacy of communication networks operating at the heart of the smart city.

1.1. Blockchain and smart cities market statistics

International Data Corporation (IDC) predicted the widespread adoption of blockchain in the industry (FutureScape, 2018). According to the IDC, at least 25% of the 2000 World's Largest Public Companies (G2000) will use Blockchain for establishing the foundation of digital trust by 2021. Moreover, a quarter of top global banks, nearly one-fifth of healthcare organizations, 50% of manufacturers and retailers will exercise blockchain in their production environment in 2021. The blockchain market size is estimated to expand from 3.0 billion USD to 39.7 billion USD by 2025 with a Compound Annual Growth Rate (CAGR) of 67.3% throughout 2020–2025 (Blockchain Market by Comp, 2020).

The global smart cities market was worth 624.81 billion USD in 2019 and is estimated to grow at CAGR of 18.30%–1712.83 billion USD by 2025 (Smart Cities Market, 2020). Moreover, the IDC predicts that international disbursement for the smart cities' development initiatives will be approximately 124 billion USD in 2020 alone, with the expansion up to 189.5 billion USD by 2023. The global focus will be on smart environments such as data-driven public safety, intelligent smart transportation, resilient energy, and infrastructure development (IDC Trackers, 2020).

1.2. Existing surveys

Several studies surveyed smart cities, IoT, blockchain, and smart contracts (Wu et al., 2019; Li et al., 2020; Wang et al., 2019a; Wang et al., Zou; Sookhak et al., 2019; Gharaibeh et al., 2017; Eckhoff and Wagner, 2018; Cui et al., 2018; Khan and Salah, 2018; Reyna et al., 2018; Ali et al., 2019a; Fernández-Caramés and Fraga-Lamas, 2018; Ferrag et al., 2019; Alladi et al., 2019; Wang et al., 2020b; Chen et al., 2020; Xie et al., 2019; Ahmed et al., 2020). The work in (Wu et al., (2019)) comprehensively studied blockchain from forking, cryptography, networking, layered architecture, consensus, and security perspective. The authors explored different applications of blockchain and investigated the challenges and opportunities inherent in contemporary blockchain technologies (Li et al., 2020). examines the security risks, real attacks, and practical solution for security in blockchain. The operating mechanism of smart contracts in popular blockchain platforms was thoroughly analyzed in (Wang et al., (2019a)). Moreover, They presented a six-layered framework for the smart contract life-cycle, challenges, applications, and future development trends. The authors of (Wang et al., Zou) reviewed the contemporary security vulnerabilities in smart contracts and corresponding possible solutions.

The evolution, functional layered architecture, and applications of smart cities were presented in (Sookhak et al., (2019)). They divide the smart city into four infrastructural pillars such as institutional, physical, social, and economic infrastructure. The privacy concerns, security requirements, security solutions, and security challenges were discussed. The data-centric perspective to smart cities was provided in (Gharaibeh et al., (2017)). The key smart city application deployment scenarios were analyzed. The data life cycle in a smart city with the perspective of acquisition, processing, dissemination, presentation, security, and privacy of data as well as enabling networking and computing technologies were discussed. The significance of privacy in smart cities was emphasized in (Eckhoff and Wagner, (2018)). They discussed the key applications of privacy within the smart city alongside the enabling technologies, associated challenges, and state-of-art solutions for enabling privacy-first smart cities. L. Cui et al. in (Cui et al., (2018)) analyzed security and privacy concerns within smart cities from the point of cyber-security. The protective measures for the security of smart cities from various technologies such as cryptography, biometrics, blockchain was discussed.

In (Khan and Salah, (2018)), the authors discussed IoT layered architecture, IoT network protocol. They categorized the crucial security concerns in IoT and investigated corresponding blockchain-based solutions. A. Reyna et al. in (Reyna et al., (2018)) discussed the potential benefit and ways to integrate blockchain with IoT. The authors discussed the potential applications, associated challenges, and blockchain platforms specific for IoT. In (Ali et al., (2019a)), researchers discussed comprehensively the blockchain-based privacy, trustless architecture, security, identity management, data management, monetisation, challenges, and research directions specifically for decentralized IoT. In (Fernández-Caramés and Fraga-Lamas, (2018)), researchers presented an optimized blockchain for blockchain-based IoT (BIoT) applications in a smart city and corresponding open research challenges. M. A. Ferrag et al. in (Ferrag et al., (2019)) surveyed the blockchain protocols for IoT and presented various threat models and challenges in BIoT networks. In (Alladi et al., (2019)), researchers discussed the application areas of blockchain in the Industrial Internet of Things (IIoT), corresponding industry-specific challenges, and open issues. In (Wang et al., (2020b)), the authors presented the security requirements for IoT and IIoT and discussed that blockchain can play the role of security enabler in IIoT. The study conducted in (Chen et al., (2020)) discussed the role of blockchain as a trusted third party, data security platform, access control platform, and automatic payment platform in IoT. The relevant research challenges were also investigated. J. Xie et al. in (Xie et al., (2019)) discussed the application of blockchain technology in various smart areas in smart cities and the relevant research challenges.

In contrast to the works summarized in Table 1, we investigate the following five research questions:

- RQ1: What are the constituent technologies in blockchain technology? How has blockchain technology been evolved? What consensus algorithms have been proposed for blockchain technology? What are the available blockchain platforms in the ecosystem?
- RQ2: What are the key application areas for blockchain-based smart cities in diverse smart environments? How blockchain solves the problems in these smart environments?

Table 1
Comparative study of this paper with existing surveys on the blockchain, IoT, and smart city.

Subject	Ref.	Prime focus	Contributions
Blockchain	Wu et al. (2019)	Blockchain technology	Detailed analysis of blockchain from forking, cryptography, networking, layered architecture, consensus, privacy and security perspective. Discussion on potential blockchain applications, challenges, and opportunities.
	Li et al. (2020)	Security aspects of blockchain	Survey of security risks, security attacks, relevant practical solutions, and future directions in the blockchain.
Smart contract	Wang et al. (2019a)	Smart contracts	0perating mechanism of smart contract and layered framework for smart contract life-cycle. Discussion on challenges, applications and future development trends for smart contracts.
	(Wang et al., Zou)	Security aspects of smart contract	Review of identification, exploitation, and mitigation of security vulnerabilities in smart contracts.
Smart city	Sookhak et al. (2019)	Security and privacy in smart city	Evolution, functional layered architecture, infrastructural pillars, privacy concerns, security requirements, security solutions, and security challenges of smart cities
	Gharaibeh et al. (2017)	Data-centric perspective to smart city	Discussion on smart city application deployment scenarios and enabling technologies. An in-depth survey of smart cities from data acquisition, data processing, data dissemination, data presentation, data security, and data privacy.
	Eckhoff and Wagner (2018)	Privacy-first smart cities	Taxonomy of applications, empowering technology, privacy types, and attacking methods in privacy-paramount smart cities. Overview of privacy protection techniques, challenges, and solutions.
	Cui et al. (2018)	Cyber-security perspective to smart city	Discussion on security and privacy issues, security requirements, enabling cyber-security and privacy technologies, challenges and future direction in smart city
Internet of Things	Khan and Salah (2018)	Security in IoT	Discussion on IoT architecture, categorization of security concerns, associated challenges and blockchain-based solution for mitigation security concerns in IoT.
Blockchain and Internet of Things	Reyna et al. (2018)	Integration of blockchain and IoT	Discussion on challenge and ways to integrate blockchain and IoT, corresponding benefits and available blockchain platforms.
	Ali et al. (2019a)	Application of blockchain in decentralized IoT	Discussion on recent advances for blockchain based decentralized IoT, related issues, challenges, and integration schemes. Discussion on blockchain-based-IoT privacy, trustless architecture, security, identity management, data management, and monetisation.
	Fernández-Caramés and Fraga-Lamas (2018)	blockchain-based IoT (BIoT)	Discussion on BIoT applications. Deliberation on optimized blockchain design for IoT. Discussion of associated challenges and recommendation.
	Ferrag et al. (2019)	Blockchain technology for IoT	Discussion on applications, classification of threats models, security and privacy, research challenges in BIoT network.
	Alladi et al. (2019)	Blockchain applications in IIoT	Review of current research trends for blockchain-enabled IIoT, application areas, and corresponding open issues.
	Wang et al. (2020b)	Blockchain as security enabler in IIoT	Summarize the security requirements of IIoT and blockchain applications as security enabler in IoT and IIoT.
	Chen et al. (2020)	Role of blockchain in IoT	Summarize the role of blockchain as trusted third party, data security platform, access control platform, and automatic payment platform in IoT.
Blockchain and Smart city	Xie et al. (2019)	Blockchain technology for smart cities	Discussion on blockchain application in smart cites, challenges, future research directions, and broader perspective to enhance other ICT technologies using blockchain in smart city
	Ahmed et al. (2020)	Blockchain as an enabler of smart city	A systematic literature review of hurdles and barrier in a smart city and their mitigation using blockchain.
	Our Work	Blockchain-based smart cities	In-depth discussion on blockchain technology chronological genesis, inception, and evolution in terms of constituent technologies, consensus algorithms, and blockchain platforms. Discussion on recent advances of blockchain-based smart environments within a smart city. Discussion on case studies, data-centric requirements, and novel challenges in blockchain-enabled smart cities.

- RQ3: How is blockchain technology solving real-world problems?
- RQ4: What key requirements should blockchain technology satisfy for enabling smart cities?
- RQ5: What are the main challenges in engaging blockchain technology in smart cities?

The answers to each of these research questions are given in a separate section.

1.3. Methodology

The methodology of this research is mainly comprised of four steps:

- Step1: For section 2, we use the subsections' heading as keywords to formulate the search queries. For section 3, we use the combinations of subsections' heading and 'blockchain' to formulate the search queries, e.g., For 'Smart Electronic Commerce', we search ('Smart Electronic Commerce' AND 'Blockchain') OR ('Electronic Commerce' AND 'Blockchain'). For the rest of the sections, we use ('Smart city' AND 'blockchain') OR (subsections' heading and 'blockchain') as keywords for search queries. The formulated search queries are performed on several digital libraries (e.g., Google Scholar, IEEE Xplore, Science Direct, Web of Science) to identify and retrieve the relevant studies. For section 2, the coverage period is 1976–2020. While for other sections, the coverage period is 2015–2020.
- Step 2: The gathered papers are examined by manually removing duplicate articles from the repository. Among the selected papers, we further identify only those papers that were written in the English language.
- Step 3: The collected articles are further evaluated in the next stage, whereby we selected only original references, conferences, journals, white papers, magazines, and online web resources.
- Step 4: For Section 2, the published articles are reviewed to formulate blockchain genesis, inception, and further enhancements in blockchain technology in chronological order in terms of constituent technologies, consensus algorithms, and blockchain platforms as well as the relevant discussion. For other sections, the published articles are reviewed to identify and discuss applications (in smart environments), case studies, and data-centric requirements and challenges for blockchain-enabled smart cities.

1.4. Contributions

The key contributions of this article are summarized below:

- We present blockchain genesis, inception, and further enhancements in blockchain technology in chronological order in terms of constituent technologies, consensus algorithms, and blockchain platforms. Additionally, we discuss the factors affecting the selection of the blockchain platform for a particular application.
- We conduct a state-of-art survey of recent advances on the applications of blockchain in smart cities with a particular focus on smart environments such as smart e-Commerce, smart e-Voting, smart transportation, smart healthcare, smart grid, supply chain management, smart property management, and smart home.
- We present case studies for real-world implementation of blockchain in smart cities such as Dubai Blockchain strategy, Estonian blockchain technology, WWF seafood traceability solution, and Walmart & IBM food safety solution.
- We present several key data-centric requirements including data accessibility, data privacy, data format consistency, data availability, data storage, sufficient bandwidth, low latency, and interoperability for enabling smart cities using blockchain.
- We present open research challenges with possible solutions related to blockchain-enabled smart cities. We also provide inflicting causes and guidelines to overcome these challenges.

These contributions are provided in separate sections from 2 to 6. Finally, We provide concluding remarks in section 7.

2. Genesis, inception, and evolution of blockchain technology

Blockchain is a distributed ledger based on the decentralized P2P network. The distributed ledger is arranged in the form of a chain of blocks. Transactions in a block are arranged in the form of a Merkle tree. The Merkle tree uses cryptographic hashing to store transactions in an immutable manner. The root of this Merkle tree is added in the block header. The block header contains the hash of the previous block to form a kind of chain and is time-stamped. The transactions of blockchain are signed using digital signature using asymmetric cryptography. Fig. 1 shows the blockchain (chain of block headers), while the Merkle root of block 2 is expanded to the corresponding Merkle tree. The consensus on the distributed ledger is maintained using consensus algorithms such as Practical Byzantine fault tolerance (PBFT), Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated PoS (DPoS). The state of blockchain is maintained through state machine replication. The business logic is executed using smart contracts.

Blockchain technology made its public debut in 2008 in a white paper that conceptualizes an e-cash system that promised to have resolved the so-called double spending problem (Nakamoto, 2008). The technology behind bitcoin came from decades of research in cryptography, distributed & decentralized computing, and financial sectors from the 1980s and 1990s. “Bitcoin Core” (Bitcoin Core Developers) software which runs on bitcoin node was initially released in 2009 (Nakamoto et al., 2009). In 2014, Vitalik Buterin realizes that blockchain can be used for more than cryptocurrency and develop a second popular public blockchain known as Ethereum that introduces the execution of smart contracts.

Fig. 2 shows the genesis, inception, and evolution of blockchain in terms of constituent technologies, consensus algorithms, and blockchain platforms. In the following subsections, we explain how the blockchain has employed various techniques and technologies for its enhancement. For each of the blockchain platforms, we provide insightful discussion.

2.1. Digital signature

Digital signature is a mathematical scheme to validate that a particular digital data is authentic. Digital signature gives the recipient non-repudiable proof that an unforged message was devised by the corresponding sender. The first digital signature scheme was introduced by Hellman and Diffie (Diffie and Hellman, 1976) in 1976. In symmetric cryptography, a secret key is shared between the communicating parties for encryption and decryption. However, Hellman brought the revolution in cryptography by introducing asymmetric cryptography which is used in blockchain technology.

Each member is assigned a pair of cryptographic keys in the blockchain network. Digital signature has two phases: the signing phase and the verification phase. The private key is used to sign the transaction, while the public key is used by network nodes to verify the broadcasted transaction. A valid transaction has the digital signature of the initiator of the transaction. Specifically, bitcoin employs the elliptic curve digital signature algorithm (ECDSA) for digitally signing the transactions (Conti et al., 2018).

2.2. Cryptographic hashing

A hash function is an encoding function that maps an arbitrary string of any size to a string of fixed size. The output of the hash function is termed as the hash value of the input string. A cryptographic hash function is a one-way function. In 1976, Hellman and Diffle emphasized the necessity of a one-way hash function for their digital signature scheme (Diffie and Hellman, 1976). Hellman introduces a trapdoor function that is easy to compute in the forward direction but is hard to invert without additional information. The term “one-way hash function” was later coined and defined in detail by Merkle in 1979 (Merkle). An optimal cryptographic hash function is deterministic, efficient, non-invertible, avalanche effective (Bansod et al., 2015) and collision-free (Xu et al., 1512). Hashing is used in blockchain for tamper-proof storage, block mining, and digital signature on transactions.

2.3. Merkle tree

Merkle tree (MT) (Merkle, 1980) is used to store data in a secure, efficient, and tamper-proof manner. MT was patented by Ralph C. Merkle in 1979 (Merkle, 1982). The MT allows secure verification of data of large size. MT is the binary tree such that each leaf node is a hash of one of the data blocks. Each non-leaf node is labeled with the hash of its two children combined. The root node of the MT generated in this way is called the Merkle Root (MR). Any changes in the data blocks are reflected up to the MR. MT is one of the hash-based cryptography employed in blockchain technology. Simplified payment verification (SPV) is used by partial nodes of blockchain to verify that particular transactions are part of a block without downloading the entire block. SPV enables partial nodes to download only a branch of a block for verification and authentication of their relevant transactions by exploiting the hierarchical nature of the MT.

2.4. State machine replication

In distributed computing, the state and functionality of the system are replicated across the network for providing Byzantine-fault-tolerant services and sustainability in-case of failure of some nodes. Each node in the network maintains the same deterministic state so that despite the failure of some node the state of the system remains available (Nogueira et al., 2017). State machine replication was first proposed by L. Lamport in a seminal 1984 paper (Lamport, 1984). This involved the effectuation of the arbitrary state machine, such that after every fixed interval, each process executes certain broadcasted commands with “time out” action for non-respondent processes. The execution of these commands results in state transitions. In 1990, F. Schneider explained the abstract approach as a general protocol in detail (Schneider, 1990). The State Machine Replication (SMR) has two downsides. First, the delayed response because of overhead introduced for maintaining the same state (synchronization) at each node. Second, the scalability is limited to the throughput of a single node as each state-transition-request needs to be executed by every node in the network so service-throughput cannot be

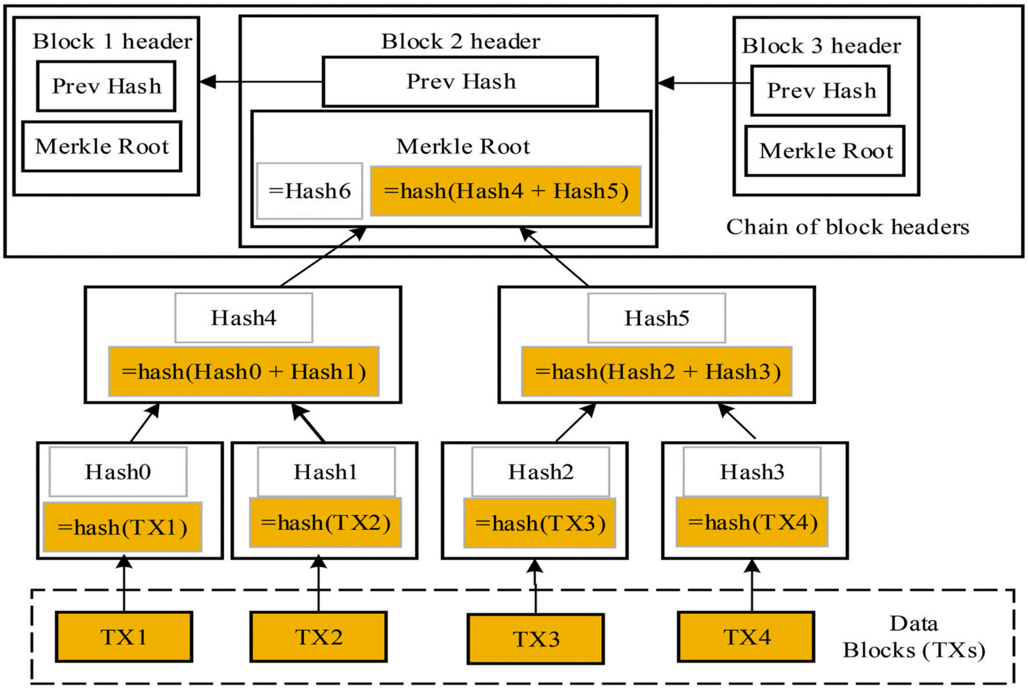


Fig. 1. Blockchain: chain of hash-linked blocks with transactions arranged in Merkle tree.

augmented by the addition of more nodes in the network (Wojciechowski et al., 2017). The ledger in blockchain is maintained in replicated state machine fashion, such that each node in the blockchain network agrees on the ever-growing chronological log of transactions. The shared-distributed state across the nodes of the blockchain network has significant importance upon consensus-finality in the blockchain.

2.5. Time-stamping

Time-stamping is the way of keeping track of creation or modification time for a digital document. Through time-stamping, the involved parties can validate that the particular document existed at a given date and time. In 1990, S. Haber et al. in (Haber and Stornetta, (1990)) introduces ways to time-stamp digital documents without relying on any third-party for record-keeping and verification. They proposed two methods for such time-stamping are linear-linking scheme and random-witness scheme. The proposed methods could time-stamp digital documents in such a way that the privacy of the document remains intact while certifying the time the document was created or modified. Any third party can verify the validity of the time-stamp. The timestamp (number of seconds elapsed since Unix Epoch) is used as an attribute in each block header to indicate the creation time of the block and to certify that transactions within the block existed in the blockchain at the specified date & time.

2.6. PoW

The concept of PoW was first given by Cynthia Dwork and Moni Naor in 1992 (Dwork and Naor, 1992). The idea was to enforce the client to solve a reasonably hard mathematical puzzle called the “pricing function” of the request message for accessing the services of a shared resource, thus preventing the absurd use and DoS attacks. This computational technique was used to hinder email spamming. The term “POW” was later devised by Markus Jakobsson in 1999 (Jakobsson and Juels, 1999). A prover doing the PoW has to demonstrate to a verifier that it has done a certain computation in a given time. The requirement of an effective PoW mechanism is such that it should be hard enough for the prover to compute but relatively easy for the verifier to verify the PoW. It is the first-ever consensus algorithm for blockchain. Miners used PoW to mine new blocks and receive their rewards. The PoW is to find the hash of the block such that it is less than the threshold set by the current mining difficulty of the blockchain network. The miners alter the nonce of the block header to find such a hash. Once such a hash is found by one of the competing miners, the other nodes in the blockchain network verify its correctness followed by the validation of transactions in the newly created block.

The main downside of PoW is the requirement of expensive specialized equipment with a higher hash-rate. PoW not only demands computational power, but it also involves high electricity consumption (O’Dwyer and Malone, 2014) which has associated environmental implications (Gimein, 2013). For small PoW networks, it is facile to carry out 51% attack at a much lower cost (Cho, 2018a). However, in a larger blockchain network technically mining pools can collaborate to own over 51 percent computational power of the network and perform the mining attack (Lin and Qiang, 2019).

2.7. PBFT

In distributed systems, Byzantine Fault Tolerance (BFT) is the characteristic of a distributed computer network to reach a sufficient consensus among majority nodes, regardless of the presence of a few malicious (Byzantine) nodes. The term “Byzantine fault tolerance” finds its origin in the famous Byzantine Generals Problem (BGP) (Lamport et al., 1982), where actors settle upon a coordinated strategy to achieve rewards and avoid catastrophic loss in the presence of few unreliable actors. PBFT is the most popular solution to BGP and was proposed by M. Castro and B. Liskov in 1999 (Castro Liskovet al., 1999). The PBFT was the first to illustrate cost-effective state machine replication in asynchronous networks. It was sustainable against Byzantine faults and unassailable to the DoS attack. PBFT is one of the significant aspects of blockchain technology. The blockchain using solely PBFT can have high throughput. The execution cost, power consumption, and latency of PBFT are low because it has no mining involved. However, it offers limited scalability (Vukolić, 2015). PBFT can be easily implemented in private blockchain because permissioned participation prevents Sybil attacks. The prominent blockchain projects such as Hyperledger Fabric,

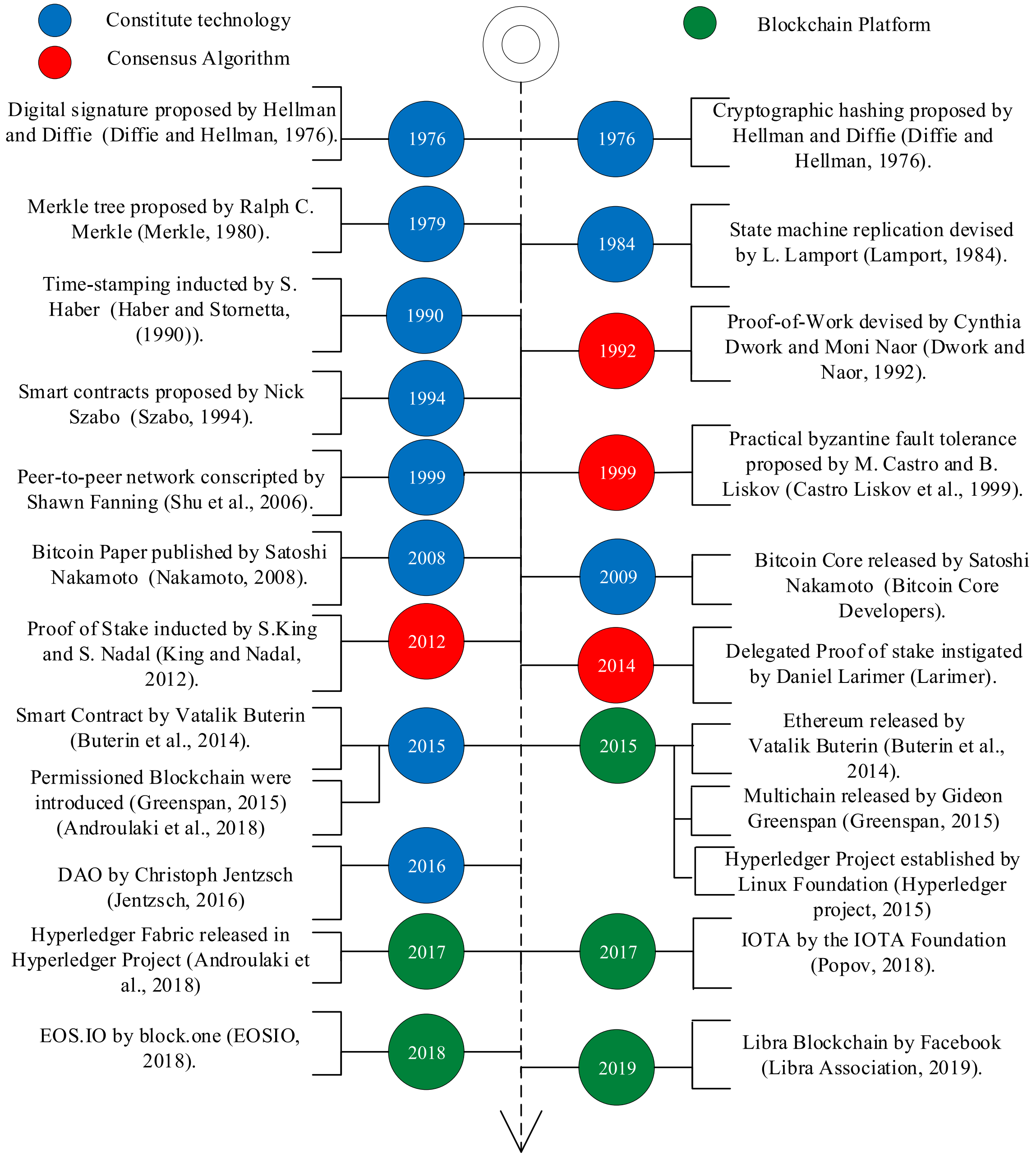

Constitute technology
Consensus Algorithm
Blockchain Platform
Digital signature proposed by Hellman and Diffie (Diffie and Hellman, 1976).
1976
1976
Cryptographic hashing proposed by Hellman and Diffie (Diffie and Hellman, 1976).
Merkle tree proposed by Ralph C. Merkle (Merkle, 1980).
1979
1984
State machine replication devised by L. Lamport (Lamport, 1984).
Time-stamping inducted by S. Haber (Haber and Stornetta, (1990)).
1990
1992
Proof-of-Work devised by Cynthia Dwork and Moni Naor (Dwork and Naor, 1992).
Smart contracts proposed by Nick Szabo (Szabo, 1994).
1994
Peer-to-peer network conscripted by Shawn Fanning (Shu et al., 2006).
1999
1999
Practical byzantine fault tolerance proposed by M. Castro and B. Liskov (Castro Liskov et al., 1999).
Bitcoin Paper published by Satoshi Nakamoto (Nakamoto, 2008).
2008
2009
Bitcoin Core released by Satoshi Nakamoto (Bitcoin Core Developers).
Proof of Stake inducted by S.King and S. Nadal (King and Nadal, 2012).
2012
2014
Delegated Proof of stake instigated by Daniel Larimer (Larimer).
Smart Contract by Vatalik Buterin (Buterin et al., 2014).
Permissioned Blockchain were introduced (Greenspan, 2015) (Androulaki et al., 2018)
2015
2015
Ethereum released by Vatalik Buterin (Buterin et al., 2014).
Multichain released by Gideon Greenspan (Greenspan, 2015)
Hyperledger Project established by Linux Foundation (Hyperledger project, 2015)
DAO by Christoph Jentzsch (Jentzsch, 2016)
2016
Hyperledger Fabric released in Hyperledger Project (Androulaki et al., 2018)
2017
2017
IOTA by the IOTA Foundation (Popov, 2018).
EOS.IO by block.one (EOSIO, 2018).
2018
2019
Libra Blockchain by Facebook (Libra Association, 2019).

Fig. 2. Genesis, inception, and evolution of blockchain technology.

TendermintCore, Ripple, Stellar, and Dispatch have PBFT as a consensus algorithm.

2.8. P2P network

P2P networking is a decentralized & distributed computing infrastructure where the workload is distributed across the decentralized nodes (peers) of the network. Typically, the P2P network is virtually overlaid upon the top of the physical network and the links between the peers are considered logical links (Yang and Yang, 2010). Each node in the P2P network willfully runs a software program so that it can act both as server and client as well as hold the same responsibilities and status in the network. The P2P scheme was first introduced commercially by Shawn Fanning as Napster in 1999, which is a platform to share files across the nodes in the network (Shu et al., 2006). Blockchain uses the robust P2P network for its operation in a trustless manner, such that each full node (peer) in the network stores the complete distributed ledger. A peer may act as an entry point for multiple users in the blockchain network. Peer repetitively validates new transactions, mine new blocks for potential incentives and broadcast blocks to other peers in the network, and finally update their own local append-only chain (Christidis and Devetsikiotis, 2016). All the peers in the public blockchain have equal rights in querying, validating, committing the transaction, and engaging in fault-tolerant consensus mechanism (Tang et al., 2018). Moreover, the blockchain size is also a constraint because of the heterogeneous nature of nodes in the P2P network.

2.9. Bitcoin

Bitcoin (capital B) is an open-source payment network platform, while bitcoin (small b) specifically refers to its associated native cryptocurrency. After the 2008 financial crisis and bankruptcy of several financial institutes, the innate trust in banks eroded. S. Nakamoto designed the Bitcoin (Nakamoto, 2008) as a decentralized currency exchange protocol to eliminate the role of banks as an intermediate for financial transactions. The transactions are based on bitcoin addresses to ensure anonymity. Bitcoin is a P2P network, which allows rapid worldwide payments, with low transaction fees and lower network cost. Bitcoin provides a distributed public ledger that records digital transactions from sender to receiver in a chronological manner. Bitcoin was the first to solve the double-spending problem of digital currencies without centralized administration from the third party. The consensus protocol in Bitcoin is PoW which ensures the immutability of the public ledger.

Bitcoin core (Bitcoin Core Developers) is freeware and open-source software released in 2009. Bitcoin core serves as a transaction verification engine and needs to be installed on all full nodes. Because of numerous full nodes (over 9000) participating in the network, Bitcoin is the securest and popular blockchain-based payment channel. However, because of pool mining, the bitcoin is becoming less decentralized. Bitcoin wallet stores the secret private key for bitcoin addresses, which is needed for signing the outgoing transaction.

The logic in Bitcoin is implemented using a build-in Turing-incomplete stack-based programming language called Bitcoin Script (Bitcoin Wiki, 2018; Nakamoto, 2010). Bitcoin Script offers simple arithmetic, conditionals, hashing, and verification of the digital signature. However, Bitcoin Script does not support loops and recursion. Bitcoin Script allows users to create custom smart contracts such as multi-signature accounts, escrows, multilateral raffle, and time-locked payment schemes (Youb et al., 2019).

2.10. PoS

It is a distributed consensus algorithm in a cryptocurrency-based blockchain network. The originator of a succeeding block in PoS-oriented cryptocurrencies is picked on the criteria defined by wealth (e.g., digital assets at stake) of the originator and random selection. The arbitrary randomized selection avoids the centralization of the network to the wealthiest members. Moreover, By employing PoS, the energy consumption, associated financial cost, and ecological damage of PoW can be avoided. Due to the energy-efficient nature of PoS, several cryptocurrencies are making a transition towards PoS. There are plans to move the Ethereum consensus algorithm from PoW-based EThash to PoS-variant Casper (Buterin and Griffith, 2017).

PoS (King and Nadal, 2012) was originally inducted by S. King and S. Nadal in 2012 to resolve Bitcoin's high-energy ingestion predicament and Peercoin was the first to implement the PoS consensus algorithm. They used the concept of "coinAge" (Fernández-Caramés and Fraga-Lamas, 2018) (defined as 'sum of the value of coins sent in transaction' multiplied by 'average holding time of the coins') for cryptocurrencies to be independent of energy-intensive algorithms. Although the timestamp parameter was previously associated with blocks, they introduced the timestamp field in every single transaction for the intent of determining the coinAge. The imperative value of coinAge to be put to the stake (also known as target) is determined by specified by difficulty, which is established flexibly by the network in a similar fashion as the difficulty of PoW to maintain block generation time. After the new block is generated, the associated coinAge put at stake by the minter is destroyed. Since the coinage is time-dependent and so difficult to obtain, the minters are less likely to behave maliciously. The mechanism for generating new blocks and rewarding transaction fees to minters in PoS is known as "minting". All the coins (or tokens) of PoS-based cryptocurrency are issued on the launch and initially minted in the genesis block. The PoS is also barely forgeable, so the associated cryptocurrencies are arduous to counterfeit. Since the expenditure of acquiring a considerable stake might be greater than the expense of controlling influential mining-power, PoS is more restrained to notorious 51% attack in comparison with PoW (Wu and Liang, 2017). The primary detriments of PoS are *nothing at stake* (Dinh et al., 2018), *long-range attacks* (Deirmentzoglou et al., 2019) and *stake-bleeding attack* (Gaži et al., 2018).

2.11. DPoS

It is an afresh democratic method for transaction processing and reaching consensus in the cryptocurrency blockchain networks. It aims to resolve the drawbacks of both PoW & PoS and is recognized as an evolved form of PoS consensus protocol. Daniel Larimer is the instigator of the DPoS consensus algorithm. DPoS first implementation was accomplished by BitShare (Larimer) in 2014.

DPoS leverages the concept of approval voting (Chaturvedi and Rao, 2019) to select the pool of witnesses which are responsible for validation of transaction and writing new blocks. Under approval voting, stakeholders can select Witnesses in a perpetual real-time multi-candidate election such that one vote per witness per token is assigned to stakeholders. The voting power of a stakeholder is determined by the number of tokens it holds. Thus, the influence of stakeholders in the voting process is directly correlated with the ownership of tokens. The stakeholder also votes for the cardinality of witnesses necessary for adequate decentralization in the network. The number of witnesses to be approved by a stakeholder per token is at its discretion provided that it does not exceed the prior chosen cardinality by the stakeholder. The top N candidates are picked out under continuous approval voting paradigm as winner witnesses (Larimer, 2014). Whereby, N is the number of witnesses such that 50% of stakeholders admit sufficient decentralization in the network. Afterward, these N witnesses write new blocks in succession to each other. The list of winner witnesses is shuffled after each of the winner witnesses had his turn. Consequently, the order of minters is changed in the subsequent cycle. The shuffling is based upon a variation of the weighted fair queueing algorithm with criteria defined by the number of votes and waiting time of particular witness (Dhillon et al., 2017). A certain percentage of block rewards received by winner Witnesses is distributed to their voters that are proportional to the voting power of the voters. The competing Witnesses themselves may not hold a large stake in the network. However, anyone can write new blocks by persuading stakeholders to vote for it and becoming among one of the winner witnesses. If a particular delegate frequently fails to publish blocks or validate erroneous transactions, the stakeholder can vote out to substitute it by the more affirmative delegate.

The network parameters like block size, block interval, transaction size, the block reward, and witness's pay-rate are adjusted by elected delegates (Committee) (Larimer, 2014). Afterward, Stakeholders will accept or reject the newly adjusted network parameters in the cooling-off period (Shahaab et al., 2019). The "witness's pay-rate" is specified before the election, which epitomizes that the winner witnesses will take a certain proportion of the transaction fee, distribute some reward to their voters and the rest will be burned. This results in the reduction of the overall supply of cryptocurrency within the network consequently increasing the value of remaining tokens. The coinage, which plays a vital role in PoS, is insignificant in DPoS. Therefore, the lost coinage is not pernicious in DPoS. As fewer nodes take part in the consensus process in DPOS, The transaction processing time in DPoS is shortened. DPoS is cost-effective, less energy-intensive, and faster. Stakeholders can set the degree of decentralization. Since the stakeholders get some share of block rewards from corresponding witnesses based upon their voting power, the stakeholders with more stakes are bond to grow richer with the further escalation in their voting capacity. Since DPoS success depends on the loyalty of witnesses, it is regarded as partially centralized.

2.12. Ethereum

Ethereum (Buterinet al., 2014) is an open-source blockchain-oriented platform that supports decentralized computing and the execution of smart contracts. The Ethereum can be used to deploy public blockchain-oriented services to capture the Business-to-Consumer (B2C) market. Ethereum, which went public on 30 July 2015 was developed by Vitalik Buterin. Ethereum enables the development and deployment of Decentralized Applications (DApps), whereby Dapps are applications that run on the P2P network and are not controlled by any single authority. Ethereum comes with a Turing-complete Ethereum Virtual Machine (EVM), which allows the execution of scripts on the Ethereum network. With the assistance of EVM, the development of blockchain applications with enhanced scalability, interoperability, feature-fullness has been made simplified. The transactions in Ethereum are based on state transition functions so the Ethereum can be regarded as a transaction-based state machine (Wood, 2014). The Turing-complete (Atzei et al., 2017) programming language such as Solidity innated in Ethereum made it possible to create customized rules for ownership, specialized transaction formats, and custom-built state transition functions. Ether is the native cryptocurrency of Ethereum which serves as inducement fuel for performing application operations on the Ethereum network and incentivize miners to mine blocks. Gas is the unique fee scheme and internal pricing currency to allocate resources proportionally for transaction processing and counter spamming. The execution cost (in metrics of gas units) for performing the operations is determined before initiating the transaction process and termed as gas cost (Hasan and Salah, 2018a). Gas price is the amount paid per unit of gas and it is inversely correlated with the pricing of Ether in the open market. The mining nodes in Ethereum use EThash for its PoW algorithm (Cho, 2018a, 2018b). However, the cryptographic hashing algorithm employed in Ethereum is Keccak-256, which is a modified version of standardized SHA3 (Hildenbrandt et al., 2018).

Ethereum offers two types of accounts: Externally Owned Accounts (EOA) and Contacts accounts. Both kinds of accounts have a balance attribute by default which facilitates the inquiry of the current Ether balance owned by the account. Externally Owned accounts are owned by users, have no associated code, and are protected through private keys. The EOA has the corresponding 256-character public key, but they can be identified by only the first 160 characters of the public key. When a user register on the Ethereum network, an externally owned account will be automatically created as default and users can initiate transactions directly via them. Contracts accounts hold the associated code known as a smart contract. Contract accounts have to be created by setting up policies for handling transactions. The contract account lacks private keys and is recognized by its public address.

2.13. Smart contracts

Smart contract is a self-executing electronic transaction protocol or digital contract which contains sets of rules and runs on the distributed blockchain network. The set of rules is agreed upon by at least two predefined, disparate but maybe anonymous participants and executed upon trigger by some event or delineated time. The contract typically involves smooth redistributed of digital assets or ownership of digitized identities of physical assets to enlisted stakeholders without any centralized third-party enforcement or human intervention (Magazzeni et al., 2017). In this way, smart contract exercise trusted agreements and corresponding transactions which are transparent, traceable, irreversible, and reliable. Once a smart contract is deployed, it cannot be interfered with or altered (Zheng et al., 2020). The key limitation of a smart contract is the limitation of immutable computer code to map real-world contractual reconciliations, particularly if a dispute or situation occurs which is not taken care of earlier in the smart contract.

In 1994, computer scientist and law scholar Nick Szabo proposed the concept of Smart Contract (Szabo, 1994). The smart contract is defined as "A smart contract is a computerized transaction protocol that executes the terms of a contract." Nick Szabo emphasized improving four basic requirements in legal settlements which are privity, discernability, validity, and enforceability. The key use-cases mentioned were, cost-effective commercial transactions without an intermediary; cost-effective trading of synthetic assets and smart property, with self-executing embedded smart contracts, that can revoke ownership in case of non-payment of the lease. The digitized contractual clauses can be lodged into the smart property for self-imposing of contract terms (Szabo, 2006).

Bitcoin endowed Turing-incomplete language for smart contracts. The first implementation of blockchain assisted smart contract was Bitcoin Script (Bitcoin Wiki, 2018). Bitcoin Script has a collection of elementary, predetermined commands which were fundamentally limited in expressiveness. However, Smart contract attained prominence with the rise of Ethereum which uses solidity (a Turing complete language having a broader instruction set) to code the contracts in 2015 (Buterinet al., 2014). Each smart contract is assigned a unique address in a blockchain network. The code within the smart contract is visible to every participating node in the network so that partaking members can decide to engage in a contract. The smart contract is generally triggered subsequently after a transaction is addressed to it whereby it is executed independently in a predefined and deterministic manner on every node in the blockchain network as per parameters set in initiating transaction (Christidis and Devetsikiotis, 2016). Smart contracts store data which can be state, information, balances, facts, relationship, associations to implement the logic embedded in them. The challenges associated with current smart contracts are security flaws, enforcement, and scalability deficiencies (Beck et al., 2016).

2.14. Multichain

Multichain (Greenspan, 2015) is an enhanced version of the Bitcoin core software, and primarily used for the deployment of private permissioned blockchains for enhancing the performance of the institutional financial sector. Multichain was introduced in 2015. Multichain offers the basic framework and executables for the deployment of private and consortium blockchain. Multichain can provide private blockchain solutions for either a single organization or multi-organization with better privacy and control. The Blockchain is reachable for pre-defined participants only that is only chosen members can access the transactions, regulate the type of acceptable transaction, and mine new blocks without using PoW. The consensus protocol in Multichain is almost the same as PBFT. However, instead of having multiple validations peers, a single validation node is selected using a round-robin scheme. Round-robin can be selected because of the permissioned nature of Multichain (Pahl et al., 2018). Therefore, the throughput that is Transactions Per Second (TPS) is relatively high whereas overhead is relatively low. The block-size of multichain is set at 32 Mb as of 2017, however, the proposal to extend the block-size is being considered.

The main drawback of Multichain was no innate support of smart contracts. However, MultiChain version 2.0 introduces smart filters to implement smart logic. Smart filters validate the transactions based on user-defined deterministic rules. The validated transactions are added in blocks and subsequently streams. Smart filters are limited as they are not designed to access off-chain data or information stored on streams (Avantaggiato and Gallo, 2019).

2.15. Hyperledger Fabric

Hyperledger (Hyperledger project, 2015) is an open-source multi--project effort by the Linux foundation for global collaborative development of blockchain-based distributed ledgers and related tools as Free and Open Source Software (FOSS). It aims to develop cross-industry standardized blockchain platforms that can enhance the way business is conducted worldwide and transactions are made. More than 220 organizations are part of collaborative development, including market leaders from information technology, supply chain, IoT, banking, finance, communication, and manufacturing enterprises as well as prominent varsities.

Hyperledger Fabric (Androulaki et al., 2018) is the most popular project under the Hyperledger umbrella and was released in 2017. Hyperledger Fabric is an open-source blockchain platform for cross-industry business purposes. Fabric is the prime distributed operating system to utilize the permissioned blockchain for enterprise-level transaction-based applications. Hyperledger Fabric is a permissioned blockchain to provide the enterprise entities with a distributed ledger to record their transactions in an environment whereby participating entities of business networks don't wholly trust each other. The consensus alongside the membership services in Fabric is designed to be plug & play. Fabric open-source software is available at (Hyperledger Fabric licence, 2017) under the Apache License, Version 2.0 (Apache-2.0).

The registration and read & write permission in Fabric are set by a Certification Authority (CA) by issuing enrollment certificates to participating peers. The Fabric modular architecture delivers high scalability, privacy, confidentiality, permission support, flexibility to business networks while tackling the complication involved in the economic ecosystem. The modular architecture enables developers to reuse and integrate common functional modules with customized components, thus enabling rapid innovation in distributed ledger technology. Hyperledger Fabric does not rely on the conventional mining process for generating new blocks and does not support any inbuilt cryptocurrency (Androulaki et al., 2018). The block size is not fixed in Fabric. The transactions are validated by endorsement peers on criteria set by endorsement policy. However, orderer nodes are responsible for packaging the endorsed transactions into blocks and broadcasting the blocks back to peers in the network. The consensus among the network peers is achieved using PBFT (Zheng et al., 2018).

The smart contracts in Fabric are called chaincodes which can be built using conventional programming languages. The Fabric also supports complex data queries just like SQL & NoSQL databases. The distinct feature of Fabric is the so-called "Channel" which brings data-partitioning capability through which the separation of sensitive data for increased confidentiality has been made possible. The data of a particular channel is visible to the participants of that channel only and is confidential from other members of the business network. The Fabric also provides support for CouchDB (Anderson et al., 2010) in which data can be stored as key-value pair.

2.16. *Decentralized Autonomous Organization*

The Decentralized Autonomous Organization (DAO) is a digital democratic organization governed by rules as written in a smart contract and operated by the decentralized distributed network without any centralized authority (Buterin, 2014). The DAO is established to achieve a certain set of goals according to predefined business logic. In a DAO, all the management and decision-making power is incorporated in immutable blockchain to ensure self-governance (Wang et al., 2019b). In 2016, The first DAO entitled "The DAO" also known as "genesis DAO" was launched for a crowdfunding project (Jentzsch, 2016). However, The DAO was subjected to the infamous "The DAO attack" on 17 June 2016. The DAO attacker exploited reentrancy vulnerability. The security aspects of DAOs is still an open research area.

2.17. *Internet of Things Application (IOTA)*

IOTA is a Directed Acyclic Graph (DAG) based block-less distributed ledger for the IoT (Popov, 2018). The DAG in IOTA is called the tangle that stores the transactions. IOTA processes a higher number of micro-transactions per second without charging any fee. In IOTA, a new transaction must validate and approve two previous transactions using a PoW mechanism. The tangle grows more efficient, faster, reliable, and secure as the number of users in the IOTA network increases.

2.18. *EOS.IO*

EOS.IO is a novel blockchain protocol that wipes out transaction fees and scalable enough to process a few million transactions per second (EOSIO, 2018). The open-source software for the EOSIO platform was released in June 2018 by Block.one. EOS blockchain architecture supports vertical as well as horizontal scaling for enterprise-level DApps. The promising features of EOS are low latency, high TPS, high sequential performance, and elevated parallel performance. EOS also supports Inter-blockchain Communication (IBC). EOS uses DPoS as its consensus algorithm.

2.19. *Libra*

Libra Blockchain is a decentralized database that supports stable value cryptocurrency backed by low-volatility reserves such as fiat currency. Libra was launched by Facebook in June 2019 to provide fast, secure, and scalable financial services to the unbanked population (Libra Association, 2019). Libra is initially launched as a distributed permissioned blockchain platform. One of the key features of Libra is seamless auditing services for validators and regulators. Libra has its native programming language called Move that reinforces the implementation of tailored transactions and smart contract with characteristics of safety, flexibility, and verifiability (Blackshear et al., 2019).

2.20. *Discussion*

In this section, we have briefly discussed constituent technologies, consensus algorithms, and blockchain platforms in chronological order. For a more in-depth review of blockchain technology (Wu et al., 2019), is referred. The main goal of a public blockchain network is to enhance decentralization securely. However, there is a blockchain trilemma around three factors; namely, decentralization, security, and scalability. Blockchain trilemma (Singh et al., 2020) refers to the empirical and logical observation that enhancement of any one of these factors, results in impairment of at least one of the other two factors. Therefore, simultaneous refinement of all the three factors is currently infeasible. However, researchers are investigating possible solutions. Based on the different levels of decentralization, there are different types of blockchain as discussed in the following subsection.

2.20.1. *Permissioned, permissionless and consortium blockchains*

Blockchain was first introduced as a public permissionless blockchain, e.g., Bitcoin and Ethereum. However, now there are many variants to accommodate diverse needs and levels of decentralization. This opens up applications of blockchain in enterprises and industries beyond the Financial Technology (Fintech). The blockchain types are divided based on configurations such as read and write access to the ledger, participation in the validation and consensus process, and level of decentralization. In the public blockchain, anyone can view the ledger; whereas, in the private blockchain, read access is restricted to specific members only. In the permissioned blockchain, only known members can write transactions and participate in the consensus. In the permissionless blockchain, anyone can write transactions and participate in the consensus. The permissioned blockchain is controlled by a single organization. The consortium blockchain is a modified variant of the permissioned blockchain that involves multiple organizations. In consortium blockchains, only known members can write transactions; whereas, the subset of these members can validate transactions and take part in the consensus process. In general, the permissioned blockchain has no mining process involved, and consensus finality is guaranteed in a shorter time compared to the permissionless blockchains. Table 2 compares different types of blockchain with generally applicable specifications. There are also private permissionless (hybrid) blockchains that have not been extensively explored in the literature. Anyone can configure a node in a private permissionless network; however, other nodes will only recognize the presence of the new node and will not share any data at first. A private side-chain is created for each smart contract on a permissionless private network. The data in private permissionless blockchains are accessible to certain cryptographic signatures only instead of direct read access to any nodes. The examples of private permissionless networks are LTO network (documentation), Monet, and Holochain.

2.20.2. Consensus algorithms

Consensus mechanisms play a significant role in the throughput, scalability, and performance of blockchain. There are many consensus mechanisms available in the blockchain ecosystem. Some of them are discussed above such as PBFT, PoW, PoS, and DPoS. Table 3 shows the comparison between popular blockchain consensus algorithms.

2.20.3. Blockchain platforms

Utilizing open-source platforms play a critical role in the cost-effective implementation of information & communication technology (ICT) projects in a smart city. There are many blockchain platforms available in the eco-system which can be engaged to enhance smart city services and discussed above such as Bitcoin, Ethereum, Hyperledger Fabric, Multichain, EOS, IOTA, and Libra. In this subsection, We established factors for determining the blockchain use-cases and discussed various factors influencing the selection of blockchain platforms.

The first step for suggesting a blockchain-based solution for a project is to determine the feasibility of a blockchain-based solution as per the requirements of the project. A valid use case for blockchain is determined based on the following factors:

- The need for shared data across diverse participants without a centralized intermediary.
- The data needs to be stored in an immutable manner.
- The shared history of ledger-data is visible and accessible to the participant according to access rights (Lin et al., 2018).
- A strong transparency or audit trail is required for each participant according to access policies.
- A repetitive longtime process is involved in the project that may be automated and orchestrated through blockchain.
- The centralized ledger does not accommodate the needs of the project.

Different blockchain provides distinctive features and functionality. Table 4 compares the popular blockchain platforms. Once, it is established that a blockchain-based solution is needed for the application under consideration, the next step is to select a suitable blockchain platform. Blockchain platforms are versatile and the selection of one of them is quite challenging. An assessment framework for picking the blockchain platform for the specific application was presented in (Alm et al., (2019)). An extensible framework to scrutinize private blockchains entitled “Blockbench” is proposed in (Dinh et al., (2017)). Blockbench provides elementary APIs which can be integrated with blockchain platforms to evaluate them based on latency, scalability, energy consumption, and fault-tolerance. The key factors for the selection of the blockchain platform depend on the nature of the intended application and its specified attributes. These factors are discussed as follows:

- Anonymity: Anonymity refers to the fact that how in-nominate a participant is in the blockchain network. Whether the real identity of the participant is trackable on-chain. Different blockchain offers a varying degree of anonymity. The cryptocurrency based public blockchain such as bitcoin confirms complete on-chain pseudo-anonymity. Private blockchain solutions, particularly for business enterprises, e.g., Hyperledger fabric, requires known identities.
- Scalability: different blockchain platforms have a disparate level of scalability. Hyperledger Fabric can accommodate a few participants. While Ethereum is highly scalable. The scalability is also determined by throughput in terms of the number of TPS. The scalability of the blockchain network is directly related to the validation process of newly generated blocks and the consensus mechanism of the blockchain network.
- Participation: How the participants will partake in the network? Permissioned blockchain platforms such as Multichain and Hyperledger needs the prior authorization of participants for partaking in the network. However, permissionless and public blockchain platforms allow anyone to register and participate in the network by creating a public/private key pair.
- Smart process integration: If the application needs complex self-enforcing actions and self-executing contracts, the selection of a platform which supports smart contract is optimal. However, if the application only needs temper-resistance storage and exchange of data, a lightweight blockchain platform can be employed.
- Access and Privacy Policy: The selection of blockchain platforms depends on the restriction of data access and visibility between participants. Different blockchain offers a varying degree of data privacy and data visibility. The access to the ledger in the permissioned blockchain is confined to prior registered and validated members. In public blockchains, anyone can see the transaction in the network through tools such as Block Explorer. In the permissionless blockchain, access to the distributed ledger can be acquired by creating a public/private key pair after registration.

3. Blockchain applications in smart city - recent advances

This section reviews the recent research work accomplished in blockchain-based smart cities and associated smart environments. The section aims to critically investigate and classify the latest research advances as potential solutions for blockchain-oriented smart cities. Fig. 3 illustrates the smart city, where various smart environments operate in parallel. Within a smart environment, several entities maintain the distributed ledger on a blockchain network while smart contracts execute the business logic.

3.1. Smart electronic commerce

Electronic commerce or e-Commerce involves sellers and buyers to exchange assets on platforms such as Amazon.com. Moreover, current e-commerce systems rely on trusted third parties (TTPs) for the delivery of traded items. Blockchain allows the transactions to be made between the parties in a trust-less environment without intermediaries. By using blockchain and smart contracts, centralized online retailers can be snuffed out from such an e-commerce ecosystem. Besides, ordered logs can be used for traceability and auditability of intermediate logistic carriers.

Asgaonkar et al. in (Asgaonkar and Krishnamachari, (2018)) proposed a dual-Deposit escrow protocol to solve the buyer and Seller’s dilemma for selling a digital good. The dilemma involves the matter of trust for payment and delivery of genuine digital goods. An extensive-form game is contrived where the seller is the leader while the buyer takes the role of follower. The utility of players is determined based on a refundable deposit, the actual value of digital good, and the price of the good (Liu et al., 2019a). The smart contract-based protocol requires the seller to make a refundable deposit while the buyer has to make a refundable deposit as well as payment of the product. If either of the buyer or seller cheats the deposit can get lost. This creates a situation where the subgame perfect Nash equilibrium based strategy for the buyer and seller is, to be honest with each other. The researchers assumed that the buyer can verify the authenticity of digital goods once delivered. The researchers also suggested a mechanism for selling physical goods without a trusted intermediary using an electronic locker.

Salah et al. in (Hasan and Salah, (2018b)) proposed blockchain-enabled Proof of Delivery (PoD) framework for tangible assets. The procedure involves a secure, transparent logistics management solution for the delivery of physical goods through the sole carrier or

Table 2
Comparison of blockchain types.

	Public Permissioned	**Public permissionless**	**Private Permissioned**	**Private Consortium**	**Public Consortium**
description	A permissioned blockchain network with public read access	A permissionless blockchain network with public read/write access	A single-organization multi-node blockchain	A multi-organization private permissioned blockchain	A multi-organization public permissioned blockchain
Read access	Anyone	Anyone	Restricted to members only	Restricted to members only	
Write access (commit TX)	Anyone/Restricted to members only	Anyone	Restricted to members only	Restricted to members only	Restricted to members only
Write access (create blocks)	Restricted to members only	Anyone	Restricted to members only	Restricted to members only	Restricted to members only
Validators/full node	Restricted to members only	Everyone	Restricted to members only	Predefined members of Consortium	Predefined members of Consortium
Network Type	Centralized	Decentralized	Centralized	Decentralized	Decentralized
Participants[a]	Identified	Anonymous	Identified	Identified	Identified
Consensus participation	Restricted to members only	Everyone	Restricted to members only	Predefined members of Consortium	Predefined members of Consortium
Ownership	Single organization	Public	Single organization	Consortium	Consortium
Examples	Ripple	Bitcoin/Ethereum	HyperLedger Fabric	HyperLedger Fabric	Public instance of HyperLedger Fabric

[a] Identity of transaction writers, validators, full nodes operators, and consensus participants.

Table 3
Comparison of prominent blockchain consensus protocols.

	PBFT	**PoW**	**PoS**	**DPoS**
Metaphor	Byzantine generals problem	City state democratic system (Cai et al., 2018)	Capitalism System	Parliamentary system
Mechanism	Two-third majority	One vote per miner	One vote per token	Vote for nominated delegates
Based upon	Byzantine tolerance	Computing power	Coinage	Voting
Node handling	Permissioned	Permissionless	Both	Both
Throughput	High	Low	Highigher than PoW	Higher than PoS
Latency	Low	High	Low	Low
Transaction finality	Absolute	Probabilistic	Probabilistic	Probabilistic
Scalability	Low	High	High	High
Tolerated power of adversary	$\leqslant$ 33.3% malicious byzantine replicas	$\leqslant$ 25% computing power	$\leqslant$ 49% stake	$\leqslant$ 49% validators
Energy consumption	Low	High	Medium	Low
Block rewards	No rewards	To miners who solve PoW	To minters who put token at stake	To elected super nodes which produce blocks
Detrimental environmental impact	Nothing	Huge	Nothing	Nothing
Example of Usage	• Hyperledger • Ripple • Stellar	• Bitcoin • Ethereum • Litecoin	• Peercoin • Lisk • BlackCoin	• Bitshares • Steem • EOS

several intermediate transporters. They utilized Ethereum blockchain and Ethereum smart contracts as the underlying technology. The framework employs the InterPlanetary File System (IPFS) to guarantee the integrity of signed terms and conditions, whereby the IPFS hash is included in the Ethereum smart contract. Double deposit collateral ensures the honest behavior of each partaking entity. Besides, the framework provides automated remuneration and dispute settlement, independent of involvement from any trusted third party (TTPs). They

Table 4
Comparison of prominent blockchain platforms.

	Bitcoin	**Hyperledger Fabric**	**Ethereum**	**Multichain**	**IOTA**[a]	**EOS.IO**	**Libra**
Release year	2009	2017	2015	2015	2016	2018	2020
Source	Open-source	Open-source	Open-source	Open-source	Open-source	Open-source	Open-source
Network Type	Public	Private	Public	Private	Public	Public	Public
Ledger type	Permissionless	Permissioned	Permissionless	Permissioned	Permissionless	Permissioned	Permissioned
Hashing algorithm	SHA-256	• SHAKE256 • SHA3	• Ethash • KECCAK-256	SHA-256	Curl-P-27	SHA-256	• SHA-3 • HKDF • Ed25519
Consensus algorithm	PoW	PBFT	• PoW • PoS (Serenity)	PoW	• PoW • Tangle	DPoS	LibraBFT[b]
e-currency	bitcoin (BTC)	N/A	Ether (ETH)	N/A [c]	IOTA	EOS	Libra
TPS	7	3500	15–20	200–1000	500–800	4000	1000
Smart contracts	Bitcoin Script	Chain-code	Smart contract	Smart Filters [d]	Not supported[e]	Smart contract	Move composed Smart contract

[a] IOTA is blockless and based on DAG.
[b] Variant of BFT.
[c] Native currency is supported but not enabled by default.
[d] In MultiChain 2.0.
[e] IOTA does not natively support smart contracts, however a PoC released in 2020 supports smart contract as additional-layer.

also discussed the cost and security analysis for the operation of the devised framework.

Liu et al. in (Liu et al., (2019b)) designed a blockchain-driven autonomous transaction management system entitled “NormaChain” for the IoT based E-commerce. The three-layer shrading is used to improve the scalability of the blockchain network, high computational overhead, and transaction-throughput. PBFT was used as an underlying consensus algorithm. The transaction layer deals with transactions initiated by users, which are sent to the approval layer for processing. Once approved, the transactions are pushed to the transaction chain. Regulators have partial access to user’s transaction information for legal supervision, thus maintaining a proper balance between privacy and legitimacy of transactions. A novel decentralized public-key searchable encryption scheme (DPEKS) for decentralized supervision is devised which allows searching on encrypted data with privacy intact. The supervision layer keeps a record of scanning the transaction chain for a target illegal keyword list in the supervisory chain. NormaChain is robust against security attacks such as ciphertext attacks (CCA) and fraudulent access to the secret key. Normachain provides scalable-secure-traceable-legitimate-autonomous payment services, with characteristics such as data integrity and non-repudiation.

3.2. Smart electronic voting

In a smart city, e-governance aims to automate the governance process by using ICT. Voting is a governance process to elect representatives of the masses democratically at the national, state, or city level. Paper-based voting completely relies on the honesty of the government officials conducting the polling. Aside from this, there are many other disadvantages associated with ballot-based voting such as high cost, time-intensive, inconsistency, pre-poll rigging, spurious vote-tallying, easy insertion of bogus ballot papers, and low voter turnout. Electronic voting is polling based on using digital technology. Instead of using ballot papers, voters are authenticated for voting using biometrics through software platforms. However, such electronic voting is vulnerable to cyber and tampering attacks at the user-end and system level. Blockchain provides a network, which does not have a single point of failure, nor it is controlled by any central authority. Blockchain provides a private key for each user to digitally sign his transaction which subsequently gets added to the append-only digital ledger. These features of blockchain can be exploited in blockchain-based scalable e-Voting. In blockchain-oriented e-voting, each voter can be assigned a wallet with a private key for authentication during polling. During each polling, the wallet is credited with a coin that can be used only once for casting a vote to a favorable candidate (Kshetri and Voas, 2018). The system protocol can be designed such that voters could be validated, but remain anonymous during the final count.

Osgood et al. in (Osgood, (2016)) discussed the challenges involved in accomplishing blockchain-based e-voting. Remote voting is regarded as impractical because of cyber-security issues. The authors proposed a voting scheme that is hybrid of ballot paper-based and digital voting. Voters vote on paper ballots with QR codes. The scanned paper ballots are stored on the local blockchain in a secure machine. The scanned images of paper ballots are also digitally preserved. After the polling time is over, all the digital information along with offline blockchain is saved on DVD. Then, the voting machines are connected as a node to a “permissioned blockchain” for accumulating individual count into the final count. Later, the final blockchain is made public to all relevant authorities for verification and validation. The suggested system will improvise e-voting; however, it is still not flawless. The authors put the light on the challenges for the widespread adoption of the system in the US.

Shahzad et al. in (Shahzad and Crowcroft, (2019)) proposed a blockchain-based e-voting scheme, particularly in Pakistan as a case study. The work mainly focused on procedures followed during the voting pursuit, security of voters’ data, and transactions corresponding to vote-casting. The work consecrates consortium blockchain which is administered by a national authority such as the election commission of a country. After the physical and biometric identification of voters, they are permitted to cast votes. After the voting is concluded at a polling station, the result is asserted for that polling station. The process is repeated for each polling station within the constituency for the

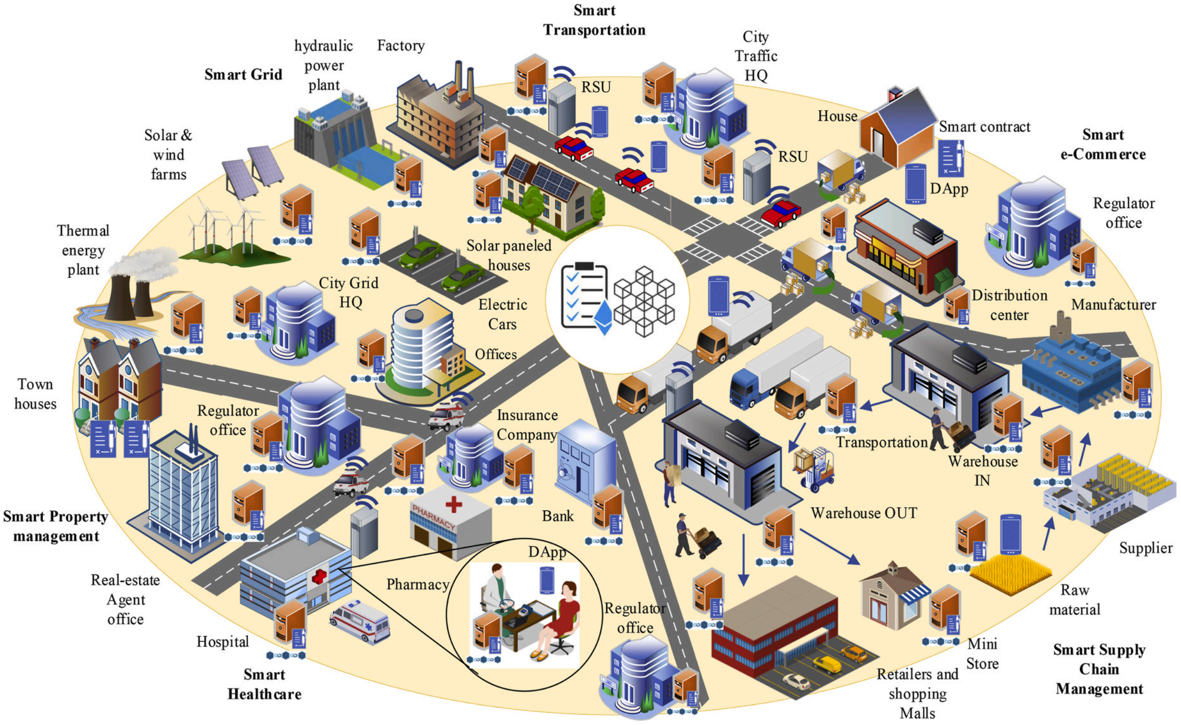


Fig. 3. Role of blockchain in various smart environments within the smart city; using smart contract and distributed ledger, corresponding transactions are identified, authenticated, authorized, and stored in immutable ledger for all entities according to the policy defined by various smart environments.

collective result of a particular constituency. Subsequently, the result of the national election is announced. The BSJC proof of completeness algorithm is proposed in the study to adjust the blockchain for e-voting. The block creation process is initiated concurrently with the start of polling time and terminated after cessation of polling time. The unique identity of the presiding officer (PO) is added using an effective hashing scheme during the creation and sealing of blocks for enhanced security. The work assumes seamless network connectivity without significant delay.

Researchers in (Ayed, (2017)) critically review different e-voting system designed by governments in several countries. A. B. Ayed proposed blockchain architecture for internet voting (i-voting) which provides authentication, anonymity, accuracy, and verifiability. The blockchain will have multiple branches. In the first block of each branch known as the foundation block, a special transaction representing the name of the candidate will be added. The vote cast for a candidate will be added in the form of the blocks in the branch initiated by the foundation block of the relevant candidate. The final count is done by counting the votes in each branch, including the orphan blocks in the branch. The vote is secured once it is cast and registered as a transaction in the blockchain network. However, the primary limitation of the proposed system is malicious behavior at the user-end while casting the vote.

Based on characteristics of transparency and immutability, Blockchain-based e-voting protocol can be regarded as rigging-proof. Although Blockchain provides a secure, fast-paced, transparent counting, and accountability system for voting. The key challenges for its prevalent adoption are low public acceptability, technological issues like scalability and storage problems of the employed blockchain scheme, end-user privacy and anonymity concerns, resistance from beneficiaries of the inefficient voting system, e.g., corrupt politicians, and inadequate digital skills of the general populace.

3.3. *Smart transportation*

Intelligent Transport System (ITS) incorporates the use of advanced technologies such as computing devices, sensor networks, wireless communications, electronics alongside modern management strategies and traffic management techniques to make transportation systems efficient, safe, fast, convenient, economical, profitable, and connected. The smart transport system involves traffic signal control systems, integration of Speed Detection Camera System (SDCS), automatic number plate recognition, CCTV systems for real-time monitoring, and traffic ticket management systems.

The BFT feature of blockchain can solve the problem of communication and collaboration in automobiles, road-side connected devices and infrastructure, smartphones (owned by pedestrian) in a fully distributed manner for smart transport systems. The "double spending" resistance of blockchain will help in a monetary transaction without central intermediaries, thus establishing an in-build financial system for ITS.

Blockchain can be used in the ride-sharing transport ecosystem. It can create an eco-system that will be P2P thus disrupting the monopoly of commercialized corporate-based transport services like uber, careem, and lyft. This will lead to a more distributed economy.

Yuan et al. in (Yuan and Wang, (2016)) proposed seven-layered blockchain-based ITS (B-ITS) framework. In the physical layer, the vehicles can be registered in the blockchain using IoT as communicating & computing devices. The data layer concerns the secure addition of data in the form of blocks using SHA256, Merkle trees, and time-stamping in the blockchain. The network layer deals with the broadcasting of blocks in P2P networks. The consensus layer is concerned with the validation and verification of blocks using different consensus algorithms to have a world state of the blockchain. The incentive layer deals with reward distribution to peers who have added a valid block to the blockchain. In the contract layer, autonomous smart contracts will be executed upon triggering of pre-defined conditions. The application layer considers the potential use cases and application scenarios of B-ITS. The authors discussed the BITS as a step forward for the Parallel transportation Management System (PTMS). However, the researchers did not mention the technical details for implementing the framework for practical real-world applications.

3.4. *Smart healthcare*

One of the primary objectives of the smart city is to provide state-of-the-art health care to the masses. The quality of care is the measure of competency of health care services in a smart city to achieve desired health outcomes at the individual and mass level (Glover et al., 2017). Blockchain can enhance the healthcare industry. Entire electronic health records (EHR) can be stored in the blockchain with blockchain-based-identity assigned to each patient. Information access, identity validation & privacy issues can be tackled using smart contracts, and blockchain-oriented access control technology (Ali et al., 2019b). Healthcare is an industry where different parties need access to the same information related to the medical history of a patient with diagnosis and treatments. The distributed architecture of blockchain can manage data-sharing, permissioned access between Medicare systems for clinical use. Moreover, blockchain can be used for supply chain management of medical products from manufacturing to distribution at pharmaceutical stores (Angraal et al., 2017), which leads to detection & prevention of counterfeiting of medicines by examining the provenance of medical products (Mettler, 2016).

Ekblaw et al. in (Azaria et al., (2016)) proposed a prototype "MedRec" for storing electronic health records for medical research using blockchain. MedRec provides a platform for real-time, system--interoperable data storage of healthcare records while addressing patient privacy and better quality & quantity of data for medical research. The distributed ledger protocol is entrenched the same as bitcoin POW. The medical record is stored using its cryptographic hash to prevent tampering.

Authors in (Linn and Koo, (2016)) addressed the key issues for using bitcoin styled public blockchain for healthcare data. The main concern is the storage-expansive nature of healthcare records which hinders scalability. The electronic health record is digitally signed by the provider or the patient upon creation for provenance proposes. The author proposes to store only indexing, meta-data, hash-pointers & encryption linked to the medical record on the blockchain while the complete health-record is stored off-blockchain.

3.5. *Smart grid*

Smart gird is a modern improvised power grid for optimized efficiency and reliability. Smart grid consists of smart appliances, sensing devices, smart meters, electricity generators, renewable energy resources, transmission lines responsible for the production and distribution of electricity with automated control (Emmanuel and Rayudu, 2016). Smart grid concerns with the addition of sensing, monitoring, communicating, analysis, visualization, computation, control, automation, diagnosis, and maintenance capabilities to the traditional dumb electrical delivery system. The smart Grid's primary objective is to meet demand with enough supply, prevent energy loss, enhancing grid reliability, affordability, sustainability, and operational efficiency.

Renewable energy sources (RES) such as wind and solar power generation have introduced the so-called prosumers in energy trading markets. Local power generation for local consumption has low transmission loss within the smart grid. Blockchain provides energy trading infrastructure within the smart grid in a peer to peer fashion without a centralized authority. Musleh et al. in (Musleh et al., (2019)) discussed blockchain applications in the smart grid such as real-time operational monitoring of the power grid, automated decentralized transmission and distribution of power, finding the optimal location for cost-effective charging for an electric vehicle, personalized and efficient energy trading between prosumers, cyber-physical security of the smart grid and effective consumption analytics. The authors presented a blockchain framework as a cyber layer for the smart grid. Application-specific blockchains, as well as an aggregator-based blockchain, are deployed for robust and reliable operation management.

Wu et al. in (Dang et al., (2019)) discussed the employment of blockchain in demand-side management of the smart grid. The study targets big industrial energy users and presents a novel power trade structure based upon the P2P blockchain network for the contract, day-ahead, adjustment, and balancing markets. They devised an optimal load management problem for a particular industrial user to minimize the operational cost.

Li*et al.* in (Li et al., (2018)) used consortium blockchain technology for secure energy trading in the IIoT nodes having close geographical proximity without a trusted intermediary. A credit-based payment scheme is introduced for the efficient and rapid trading process which provides an optimal loan pricing strategy even for broke consumers. Stackelberg game is applied for the selection of optimal pricing strategy to maximize the utility of credit-bank through appropriate interest rate and penalty rate. Smart contracts are employed for automated transactions for energy trade between prosumers based upon pre-defined preferences. Energy aggregators (EAGs) are responsible for pairing up appropriate sellers and buyers based on corresponding energy requests. The transactions are recorded and audited by these pre-qualified energy aggregators having moderate operational costs. The consensus between energy aggregators is achieved using PoW. The proposed scheme is scalable concerning numbers of partaking IIoT nodes and transaction confirmation time. The main drawback of the proposed scheme is relatively less privacy protection.

3.6. *Supply chain management*

Complex supply chains are essential for industries and businesses. A supply chain is described as a collaboration of more than two organizations controlling the flow of commodities, utilities, economy, knowledge from a source to the respective consumer. There is a demand for a transparent, traceable, risk-preventive supply chain mechanism that can accommodate all the information from raw materials to manufacturing details of the finished products as well as traceability from plant to consumer. The blockchain-based supply chain system can record all specific information of each product during its life-cycle at one shared distributed ledger in a secured manner. The relevant information can be accessible to respective entities.

S. A. Abeyratne et al. in (Abeyratne and Monfared, (2016)) planned a blockchain ready manufacturing-supply-chain system. They assign each product a unique digital identification tag. All the actors involved have authenticated access to the blockchain ledger. The software platform for data entry as well as to access the product profile was developed. A smart contract is deployed for each product governing the rules as the product passes through the supply chain. The ledger will provide indisputable evidence of proprietorship of an asset along with location and time stamping information through a secure user interface. However, the authors did not discuss the technical challenges involved in the adoption of blockchain in supply chain management.

Alahmadi et al. in (Alahmadi and Lin, (2019)) proposed blockchain empowered fairness protocol for the IIoT-based supply chain management. The protocol ensures reliable on-demand trade of physical goods between merchants and suppliers by transmitting immutable trade information through blockchain and enforcing penalties via a smart contract. A new smart contract is deployed for each trade contract while the non-repudiation property is enforced by digitally signing the transaction via private key. The trade process involves initialization, order placement, order placement, delivery, and judgment phase by a smart contract. The proposed scheme was implemented using the EVM and performance evaluation was performed for transaction-confirmation-time within the blockchain network.

Salah et al. in (Salah et al., (2019)) propounded a blockchain-based approach for efficient and effective trace-ability within agricultural and food supply chains. The study was focused on soybean crops, but the proposed scheme is generic to be applied to the agricultural supply chain (ASC) of any cultivation produce. Substantiation of essential criteria such as country of origin, contemporary phase of crop processing, yield monitoring, conformity to quality benchmarks, and compliance with country-specific regulatory policies was done by all involved stakeholders through a blockchain platform. Ethereum based smart contracts regulated the interaction between all stakeholders such as seed companies, farmers, grain elevators, grain processors, distributors, retailers, and customers for the soybean agriculture supply chain in a decentralized manner. However, the authors did not explain the key challenges involved such as dispute handling, automated payment, and fraud prevention within the agricultural supply chain.

3.7. *Smart property management*

Real estate is a lucrative business in today's global market because of its immobile, heterogeneous, and fundamental asset nature. Real estate deals with public, private, and commercial properties on an ownership or rental basis. Smart real estate management (SREM) refers to the use of innovative modern technologies for the effective commercial administration of real estate trading in a user-centric, secure, privacy-preserving, and sustainable way. The adoption of novel disruptive technologies in smart real estate (SRE) is essential for solving key challenges associated with the real state industry. Blockchain promise to create new business models in the real state industry by accommodating the needs of corresponding stakeholders such as consumers, real state agents, government, and regulators within a shared decentralized ledger. Blockchain is a seamless solution for the land registry problems to tackle property frauds. The geo-coordinates and polygonial description of land can be hashed and tied to owner id and stored in a distributed ledger. Moreover, the immutable blockchain allows tracing of the complete ownership history of a property as well as authentication and validation of corresponding transactions (Shedroff, 2018).

Avantaggiato et al. in (Avantaggiato and Gallo, (2019)) discussed the usage of MultiChain in real estate with corresponding challenges and opportunities. The authors proposed blockchain-based REchain architecture for real estate trading with Multichain as the underlying platform. Issuing refers to creating a digital abstraction of physical assets by authorized nodes with metadata indicating attributes of the property. Smart filters validate the transactions before adding them to append-only Streams. An owner puts his property on sale publishing. Potential buyers make purchase offers followed by acceptance of the bid by the owner and subsequent transfer of ownership to the new buyer after explicit agreement. The authors developed a customized MultiChain explorer to probe into real estate transactions. Since smart filters are less capable than smart contracts, the REchain has limited flexibility for the exertion of smart logic.

Evareium (Fernandez et al., 2018) is a mutually beneficial ecosystem for the digitized and effective management of real estate investment for enhanced value-creation. EVRM is Ethereum ERC20 based token within the Evareium platform and is backed by real estate assets. It allows investors to generate passive income without active engagement in the trading of real estate property. It is predicted that EVRM will acquire 10% of world GDP by 2027. Norta et al. in (Norta et al., (2018)) emphasized that blockchain enables time-efficient P2P trading of commercial property without intermediaries at a reduced cost. They proposed a Business-to-Business (B2B) crowdfunding platform on Evareium system for commercial real estate leveraging with quality goals such as security of the overall system, seamless information flow between platform sub-infrastructures, direct P2P engagement between stakeholders, sufficient liquid financial resources available for investment at any moment and verifiable recording of the key transactions on the

Table 5
Applications of blockchain in smart environments within a smart city.

Paper	Objective	Smart Environment	Consensus Protocol	Technologies Employed
Asgaonkar and Krishnamachari (2018)	To Solve the buyer and seller's dilemma for genuine delivery and payment of digital good.	Smart Electronic Commerce	N/A	• Double deposit Escrow • Smart Contract
Hasan and Salah (2018b)	To establish proof of delivery of a tangible good as it is transferred from the seller to the buyer through logistic intermediaries.	Smart Electronic Commerce	Proof of Delivery	• Smart Contract • Ethereum • IPFS
Liu et al. (2019b)	To design scalable and efficient autonomous transaction management system for IoT based E-commerce.	Smart Electronic Commerce	PBFT	• NormaChain • Ethereum
Osgood (2016)	To design a blockchain-based tamper-proof and auditable voting mechanism.	Smart Electronic Voting	N/A	• Permissioned Blockchain • Local Blockchain
Shahzad and Crowcroft (2019)	To propose a blockchain-based framework for trustable electronic voting.	Smart Electronic Voting	Proof of completeness	• Consortium Blockchain • Biometric authentication
Ayed (2017)	To design a decentralized internet-based electronic voting system.	Smart Electronic Voting	Longest Chain Rule	• N/A
Yuan and Wang (2016)	To propose the framework for a blockchain-based intelligent transportation system.	Smart Transportation	Proof of movement	• Layered architecture • Smart contracts
Azaria et al. (2016)	To propose a blockchain-based decentralized record management system to handle electronic health records in an interoperable manner.	Smart HealthCare	PoW	• Ethereum • Smart contracts
Linn and Koo (2016)	To design blockchain-enabled access-control manager for authentic and inter-operable retrieval of off-chain healthcare records.	Smart HealthCare	N/A	• Data Lake
Musleh et al. (2019)	To review the challenges and approaches associated with using blockchain for the smart grid. To present frameworks utilizing blockchain as a smart grid's cyber-physical layer.	Smart Grid	N/A	• N/A
Dang et al. (2019)	To present a blockchain-based novel market structure for various electricity trading markets. To study the optimal load management problem at demand-side	Smart Grid.	PoW	• N/A
Li et al. (2018)	To propose an optimal pricing strategy on credit-based loans scheme for P2P energy trading on a consortium blockchain.	Smart Grid	Proof-of-flow	• Consortium Blockchain • Smart Contract
Abeyratne and Monfared (2016)	To propose a decentralized manufacturing-supply-chain management system and discuss related requirements and challenges.	Supply Chain Management	N/A	• N/A
Alahmadi and Lin (2019)	To propose a distributed supply chain management system with the integrated industrial internet of things. To design a fair good exchange policy using the smart contract.	Supply Chain Management	Proof-of-Authority	• Ethereum • Smart Contract
Salah et al. (2019)	To propose a blockchain-enabled traceability scheme for the agriculture supply chain.	Supply Chain Management	N/A	• Ethereum • Smart Contract • IPFS
Avantaggiato and Gallo (2019)	To propose a decentralized real estate management system and highlight associated challenges and opportunities.	Smart property Management	PBFT	• REchain • MultiChain • Smart filters
Norta et al. (2018)	To propose a crowdfunding based investment platform for real estate trading.	Smart property Management	N/A	• Evareium • IPFS
She et al. (2019)	To design Homomorphic Consortium Blockchain for privacy-preserving of sensitive data within smart homes.	Smart Home	Distributed Consensus	• Consortium Blockchain • homomorphic encryption
(Dorri et al., 2017a, 2017b)	To design secure BIoT based privacy-preserving architecture for smart home with reduced network & processing overhead.	Smart Home	Distributed trust	• Private Immutable Ledger • overlay network • 6LoWPAN

blockchain in an immutable manner. The minimal transaction set and corresponding blockchain operation for the dynamic engagement of stakeholders were outlined to ensure traceability.

3.8. Smart home

Smart home refers to the sophisticated utilization of information and communications technology (ICT), ubiquitous computing, wireless sensor networks (WSN) for automated control and management such as lights control, climate regulation, fire-alarms control, and entertainment systems handling. It also includes a security system for intrusion detection, access control to prevent cyber-physical threats, and emergency alarm systems (Jose and Malekian, 2017). The home devices are connected to the Internet via a local network for remote monitoring and control by a wall-mounted terminal or mobile/desktop applications. Smart home promise to bring revolution in living standards with domestic comfort, reliability, privacy, and leisure with energy-efficiency (Khan et al., 2016), better Quality of Service (QoS), improved customer experience, and enhanced quality of life (QoL) as primary goals.

IoT in the Smart home system (SHS) communicate with each other and local server through the home local network and with remote servers through the home gateway and thus at risk of privacy leakage. To mitigate this, the network-level security of SHS is ensured through blockchain and smart contracts. She et al. in (She et al., (2019)) proposed a homomorphic consortium blockchain model for sensitive data privacy-preserving (HCB-SDPP) in traditional SHS. The consortium blockchain offers high scalability and interoperability with enhanced organizational jurisdiction (Yuen, 2020). The physical structure of HCB-SDPP consists of sensory nodes, gateway nodes, and verification nodes. Paillier encryption, which is a type of homomorphic encryption was used for privacy and security. Blockchain Channels were used to store separate ledgers for each community which encompasses several gateway nodes. A New block data structure based on Homomorphic Encryption (HEBDS) was also devised. The performance analysis based on data security, data availability, ledger storage security, and system robustness was performed and the HCB-SDPP scheme was found effective.

Dorri et al. in (Dorri et al., (2017a)) presents a novel lightweight blockchain-based hierarchical network architecture for smart home which has three tiers that are smart home, overlay, and cloud storage. The private Immutable Ledger is maintained for reduced network overhead at the IoT based on the local network within a smart home. The blocks in the local ledger also include a policy header, which stores policies for authentication and authorization of all types of transactions (Dorri et al., 2017b). The data can be accessed by the homeowner for remote monitoring or Service Providers (SP) for improved-personalized services through "access" and "monitor" transactions after authentication, whereas the transactions are processed by a high resource miner at a smart home. An overlay network constituted of Cluster Heads (CH) as selected by smart home managers (SHMs) maintains public blockchain while each CH possesses PK of relevant requesters and requestees. The distributed trust scheme employed by the overlay network reduces the processing overhead, but still maintains the privacy and security of the network.

3.9. Discussion

According to UN's "2018 Revision of World Urbanization Prospects", 55% of the global population (4.2 billion) lives in cities (DESA, 2018), which is estimated to increase by 68% to 6.2 billion by 2050. The excessive urbanization in today's global society presents immense challenges as well as prodigious opportunities. Blockchain is expected to take a significant role in solving key challenges within smart cities for social, government, technological, and economic development by establishing a new digital smart city ecosystem paradigm. In this context, we discussed state of art application areas such as electronic commerce, electronic voting, transportation, healthcare, power grid, supply chain management, real estate management and smarty home, where the blockchain can be applied for enhanced security (Hakak et al., 2020), privacy, authenticated access, sustainability, reliability, and integrity in a smart city. Table 5 shows the key objective issues solved in summarized research articles. The consensus protocol, blockchain platforms, and other related technologies applied in the studies are also mentioned.

In a smart city, data is generated by various smart environments at a high-volume, high-variety, high-velocity, and high-veracity. However, several issues related to data collection, privacy, and security impede the full potential benefit of this data. Federated Learning (FL) (Konečný et al., 2016; Khan et al., 2019, 2020d) is a privacy-preserving distributed machine learning technique to train a shared global model without sending the raw data to a centralized server. Users' devices train the local models on local data and only send the local model updates to the server. The shared global model is the aggregation of these local model updates. However, typical FL has issues such as low reliability, less-robustness, and lack of reward mechanism. Blockchain can be used for secure, reliable, auditable, and reward-driven federated learning (Majeed and Hong, 2019; Kim et al., 2020) to enhance smart city services at governance and industrial scale.

The main challenges associated with public blockchains include high latency, full openness, low usability, low throughput, and low scalability. Private and consortium blockchains have a trust-based model, low decentralization, and less security. Such limitations prevent the widespread adoption of blockchain in smart cities. However, as the new consensus algorithms and privacy-preserving techniques are emerging, blockchain is expected to provide different levels of decentralization with divergent access policies in a scalable fashion to offer more reliable and secure smart city services. Moreover, smart contracts can provide intelligence to the blockchain for anomaly detection or execution of business logic for enabling safe and reliable smart city services.

The record stored on blockchains with timestamps cannot be erased. This contradicts the data protection and privacy laws such as the European General Data Protection Regulation GDPR). 'Right to erasure' or 'right to be forgotten' (Mantelero, 2013) comes under article 17 of GDPR which states that the data subject has the right to the erasure of personal data without undue delay. In this regard, some novel solutions need to be proposed in the future. From the smart city perspective, the blockchain must be standardized to enable its widespread adoption into new smart city services for various industrial use cases. Some international standard organizations such as ISO, ITU, IEEE, and W3C are engaged to enable blockchain standardization at a global level. However, innovative guidelines for a smooth migration to blockchain for existing smart city services still need to be devised.

4. Case studies

Blockchain has been acclimated by renowned businesses, governments to enhance their business models and provide superior services. In this section, we discuss some eminent real-world blockchain-based endeavors as case studies.

4.1. Dubai blockchain strategy

The Dubai government has envisioned Dubai as the first smart city powered by blockchain by 2020 for the secure, impactful, efficient, and safe city experience. Smart Dubai Office in collaboration with Dubai Future Foundation has launched the Dubai Blockchain strategy in 2016. Dubai Blockchain strategy emphasizes the effective delivery of paperless public services, establishing a blockchain ecosystem for business, and making Dubai an international leader in devising cross border blockchain-oriented use cases (Smart Dubai, 2016). Bitcoin, blockchain & smart contracts are expected to play a pivotal role in realizing the vision. Dubai Blockchain strategy includes the thorough analysis of existing services to determine the potential for blockchain-based improvisation, technical analysis for building use-cases, designing business models, and finally creating a proof of concept for deducing feasibility of use cases & business models.

As part of the Dubai blockchain strategy, Dubai Land Department DLD) has accomplished a milestone by becoming the world's first government department to incorporate blockchain technology for its electronic transactions (Dubai has world's first,). The blockchain-based real estate platform includes validation of residency visas, real estate contracts, lease registration, tenant registration. The information on the ledger is also accessible via authentication to related authorities such as Dubai Electricity & Water Authority DEWA), telecommunication companies, and other property-based utilities. Digitization enables stakeholders to complete transactions electronically in a time-efficient manner without a physical visit to government organizations.

The Dubai Blockchain strategy aims to use blockchain for safe, trustworthy, and secure transactions in all sectors of the city. documents such as license renewal, visa applications, utility invoices, contracts & legal papers will be processed using blockchain digitally and expected to save 5.5 billion dirhams annually as well as to redistribute 25.1 million hours of productive work time (Dubai Blockchain Strategy,). Thus, blockchain is considered effective for government efficiency & economic growth.

4.2. Estonian blockchain technology

Estonia is currently regarded as the most progressive & digital nation on the globe. Estonia was already using blockchain technology in 2008 for its e-state policy even before Satoshi Nakamoto invented bitcoin. In Estonia, the technology was termed as "hash-linked time-stamping" before bitcoin. Estonia considers the blockchain the key tech to bypass destruction from cyber attacks. Since 2012, Estonia has been using blockchain for public services like national health, population, land, security, legislative, banking commercial & business registries (The world's first Data Em,). All such data is digitized, securely stored using blockchain, and accessible to authorized entities only. The citizen or e-residents can access their data through special digital identities. The accessibility logs are maintained using the blockchain, thus preventing misuse of public data.

Estonia has given the concept of the world's first "data embassy" which is a state of the art national cloud solution to host data and services (The world's first data,). The so-called "data embassy" can be operated from data centers outside Estonia for reliable operation during a potential invasion from hostile countries or devastating cyber attacks. The data embassy provides secure digital services to Estonian citizens as well as e-residents of Estonia. Blockchain ensures the data integrity for data embassies that use distributed systems for operations.

4.3. WWF blockchain-based seafood traceability

Skeptical fishing practices can cause irreversible damage to marine habitats and dis-balance the aquatic ecosystem. The worldwide fishing industry is struggling with over-fishing, desecration of local and international laws, dodging practices to taxation rules, and human rights abuse. As per the estimates made by the National Oceanic and Atmospheric Administration NOAA), unauthorized fishing costs $10 billion annually due to suppression in prices due to high supply in the market while the lost revenue accumulates to $23 billion per annum (Can Blockchain Technology,). Illegal fishing in the seafood industry can be combated using Blockchain. World Wildlife Fund WWF) with the help of tech organizations ConsenSys and TraSeable) & seafood processing facility Sea Quest Fiji Ltd.) is using blockchain to track the route of tuna fish from "bait to plate" in Pacific Ocean (How blockchain,). fishermen will use specially designed scannable electronic tags to register their catch on the blockchain. This will ensure apex transparency and integrity of data along the supply chain of seafood and empowers traders to discover malicious actions. Blockchain enables the consumers to find all relevant data such as provenance, legality, manufacturing information, and distribution details of an item just by scanning the code on an item. Consequently, the technology will allow consumers to refuse to buy illicitly caught seafood.

Moreover, Smart contracts are employed for rapid transactions and fasten agreements at the docks. Thus, reducing the docking time, lessening the wastage of food due to spoilage and corresponding financial loss. Thus, blockchain is being utilized to enact global peer to peer networks involving all stakeholders for providing robust, neutral, transparent, reliable, economical, and secure trade at the grass-root level of the seafood industry.

4.4. Walmart & IBM food safety solution

Walmart Inc. is a multinational retail corporation that runs discounted departmental stores, hypermarkets, and grocery stores as well as an e-commerce business. Walmart has captured the major retail market in China, which is one of the prominent economies in the world. Walmart in collaboration with IBM is working to develop a food safety solution that intents to upload supply chain information and data of its retail products to blockchain(Walmart is betting,). IBM has developed Food Trust Solution for the corresponding use-case of blockchain and Walmart is adopting it for its food safety solution. This will make the supply chain process can become digitized, smooth, traceable, and transparent. The stakeholders such as farmers, logistics companies, wholesalers, distributors, grocery markets can upload their data to the blockchain using specially designed applications. The data mainly concern with the identification of particular food items and the role of stakeholders involved in a specific supply chain process. The key benefit of digitization is that the source of food can be tracked promptly in less than 3 s while before the digitization it took approximately 7 days to track the origin of food through paper-based ledgers.

The tracing of food is useful to track the source of infectious, poisonous, or contaminated food in case of incidents such as the infamous *E. coli* outbreak in romaine lettuce and Strawberry needle sabotage in Australia.

In April 2018, the United States had a poisonous *E. coli* outbreak in romaine lettuce that caused people to be hospitalized with kidney failure. Some of the victims even died. Moreover, the *E. coli* outbreak disturbed the supply chains of romaine lettuce to restaurants and food markets.

The strawberry contamination scare in Australia started when masses found needles in the strawberries. The incidents enforce the farmers and retail businesses to dump the food, consequently causing huge financial loss. With the help of the blockchain, the provenance of such contaminated food can be tracked immediately & contained instead of closing the whole business for a particular food and depriving people of their livelihood.

4.5. Discussion

Blockchain is playing a key role in enabling smart city services; namely, 'Dubai Blockchain strategy' at the city level, 'Estonian blockchain technology' at the country level, 'WWF blockchain-based seafood traceability' and 'Walmart & IBM food safety solution' at organization and smart environment level. Table 6 summarizes these case studies. We conclude that blockchain can provide enhanced B2B, B2C, and Government to Citizens (G2C) services by establishing improved transparency, immutable audit logs, enhanced accountability, embedded security, and mutual trust. Because of such characteristics, blockchain will be a key technology in future smart cities. As per IDC, blockchain technology has already been adopted by governments and big corporations in various smart environments such as smart tourism, precise agriculture, smart education, smart grid, and smart healthcare (ID

Trackers, 2020). However, to enable more widespread adoption of blockchain in real-world smart cities, new congruent regulatory policies and feasible business models need to be devised. Besides, some certain challenges and requirements need to be met to make blockchain a mainstream technology. In the following sections, we outline some key requirements and challenges.

5. Requirements

This section discusses the key requirements that need to be met for making blockchain a mainstream technology in smart cities.

5.1. Data access and privacy

Data is considered as a valuable asset in designing efficient policies after rigorous analysis for smart cities. However, accessing data generated in the smart cities can be abusive in terms of data owner privacy. On the other hand, personalized data acquisition will play a very important role in providing customized services in smart cities such as smart health care, e-voting, and many more community-related services. Thus, control for sharing this sensitive data should be maintained by the data owner to ensure privacy, willingness, and level of access. Indeed, blockchain enables the collection, storage, and control of personal data. One way to promote the acquisition of data is to motivate the data owners by providing them incentives via smart contracts which can also serve the purpose of privacy. Furthermore, there have been a few recent studies in the literature to analyze and address the issues of privacy in blockchain-based systems. However, they are focused on presenting area-specific solutions such as an intelligent transportation system that cannot be adopted for general smart cities (Butt et al., 2019). Hence, a key requirement for accelerating innovations and growth in smart cities is designing novel data access and sharing mechanisms that support data owner's privacy.

5.2. Data format consistency

Smart cities include several sensors and actuators that constantly produce data. Data produced by these heterogeneous devices is generally required for analysis and decision-making purposes. Moreover, the data produced by these sensors do not comply with any single standard and thus can have heterogeneous formats. Thus, the analysis of such data with different formats becomes challenging. Furthermore, this inconsistency in data formats can add additional cost in terms of delay and pre-processing. Thus, blockchains for smart cities should be able to efficiently handle, analyze, and process data produced in heterogeneous formats.

5.3. Permanent data availability

Data storage in blockchain technology enables a key feature of the permanent availability of data. This is a key requirement to enable smart contracts between legal entities. However, the permanent availability of all data will be challenging given the huge scale of the network and the number of stakeholders involved in the smart cities. Thus, novel schemes are required to enable the permanent availability of data in smart cities.

5.4. Data storage

Blockchain enables decentralized data storage that enables scalability and protection from a single point of failure (Zahed Benisi et al., 2020). Although the decentralized storage mechanism of blockchains enhances the storage performance in smart cities, it poses novel challenges in terms of immense volume, variety, and velocity of data produced by millions of devices in the smart cities. One of the possible approaches is storing only the pointers on the blockchain and the rest of the blockchain for catering to the volume of data. Furthermore, consistency in terms of replicated data on different storage devices and the availability of this data is also a key requirement for processing and decision making. Therefore, an effective mechanism that can handle the aforementioned challenges in blockchain-enabled smart cities should be designed for data storage.

5.5. Sufficient bandwidth

Blockchain-enabled smart cities equipped with a huge number of resource-constrained sensors poses an important requirement of high bandwidth to control the blockchain framework. This includes the exchange of control data to achieve many tasks in the blockchain framework such as achieving consensus, appending blocks, accessing data

Table 6
Summary of the case studies.

Sr #	Case Study	Objectives	Companies/Organizations	Country/ Location	year
1.	**Dubai Blockchain strategy**	• Make Dubai first blockchain based smart city by 2020 • Provide blockchain-oriented government services • Establish blockchain acclimatized businesses and startups • Make Dubai international leader in blockchain global paradigm • Use blockchain for improvised tourism	• Dubai government • Dubai Future Foundation • Dubai Land Department • Smart Dubai Office • Dubai Electricity & Water Authority	Dubai	2016–2020
2.	**Estonian blockchain technology**	• Provide blockchain backed federal services • Deliver secure data facility to Estonian native citizen and E-citizens • Create Data Embassies secured by blockchain • Secure Estonia from potential cyber attacks of hostile countries	• Estonia government • Estonian Information Systems Authority RIA) • Guardtime - blockchain vendor	Estonia	2012-present
3.	**WWF Blockchain based seafood traceability**	• Trace the seafood from bait to plate • Prevent illegal fishing • Improvise associated environmental impact • Restrain economic loss of unauthorized fishing • Fasten the sea food trade using blockchain	• World Wildlife Fund • ConsenSys - US based tech innovator • TraSeable - US based tech implementer • Sea Quest Fiji Ltd. - A food processing company	South pacific	2018 - present
4.	**Walmart and IBM food safety solution**	• Track food from field to market • Fasten the supply chain operations • Reduce the economic impact of food wastage • Decrease the impact of food-borne diseases	• Walmart Inc. • International Business Machines Corporation IBM)	China	2016-present

storage. Insufficient network bandwidth can hinder the performance of the blockchain-enabled smart cities in terms of latency and scalability. Hence, the effective design of a network with sufficient bandwidth is required to fulfill the requirements both posed by the smart city devices and blockchain framework.

5.6. *Low latency*

Latency requirements in blockchain-enabled smart cities will play a key role in bringing real-time applications to fruition. Real-time applications such as online banking, self-driving cars, etc. cannot rely on current blockchain technology that handles only a few transactions per second. Moreover, the proliferation of novel heterogeneous latency constrained applications in the future network will require to have lightweight blockchain approaches that can meet these heterogeneous latency requirements. Thus, new mechanisms are required to achieve fast consensus and handle a high number of transactions in blockchain technology to handle the aforementioned requirement posed by these smart city applications.

5.7. *Interoperability*

Smart cities are envisioned to enable several services to facilitate their citizens. These services will be enabled by a variety of independent and isolated blockchain technologies in smart cities. However, reaping the benefits of blockchain-enabled smart cities require addressing a critical challenge of interoperability between multiple isolated blockchain technologies. Cross blockchain cooperation will play a vital role in deploying stable large scale networks. Hence, novel architectural approaches are required to fill the gap of interoperability in existing blockchains.

6. Open research challenges

This section presents several indispensable open research challenges hindering the implementation of blockchain technology into a smart city. We outline the key causes and guidelines for these challenges as can be seen in Table 7.

6.1. *Sustainability*

Sustainability refers to the design of blockchain-enabled smart cities without depletion of natural resources. An unprecedented proliferation of smart IoT devices in smart cities results in high energy consumption. Apart from that, blockchain consensus algorithms such as PoS having high computational complexity further increases energy consumption. To cope with the high energy consumption challenge, the use of energy-efficient design, renewable energy sources, and energy harvesting can be a viable solution. Therefore, several aspects that must be considered in the sustainable blockchain-enabled smart city include energy-efficient communication networks, renewable energy resources, energy-efficient storage for blockchain, energy-efficient consensus algorithms, and reputation-based consensus schemes (Wang et al., 2020c). Some of the energy-efficient consensus algorithms are PBFT, PoS, DPoS, Proof of activity, proof of importance, and proof of retrievability with prime focus on energy usage minimization (Zheng et al., 2017). Moreover, relatively less energy-demanding hardware such as application-specific integrated circuits (ASICs) for PoS-based blockchain can be used for sustainable smart city services (Sedlmeir et al., 2020). In general, less energy-intensive validation schemes are required to develop for achieving long-term sustainability of blockchain-based smart city services from economic, environmental, and social perspectives (Schinckus, 2020).

6.2. *Adaptive consensus algorithm*

Smart city advancements have significantly diverse requirements that must be considered in their design. Therefore, it is an open research area to adaptively enable different advancements of the smart city via blockchain. In a typical blockchain, a consensus algorithm provides rules of reaching consensus among several nodes involved in a blockchain network. The design of every blockchain consensus algorithm is characterized by node identity, energy consumption, data model, and application (Chalaemwongwan and Kurutach, 2018). PoW is characterized by high energy consumption, public node identity, transaction, and account-based model, and cryptocurrency application. Similarly, PoS has partial energy saving nature, public node identity, and account-based model. For instance, consider energy efficiency as a primary design objective of blockchain-enabled smart city advancements, there exist different consensus algorithms designed for similar applications but with different energy consumption. PoW and proof of activity having the same data model and cryptocurrency application but different energy consumption (i.e., proof of activity has lower energy consumption). Therefore, we must design a consensus algorithm having adaptive nature as per application design objectives. In (Alzahrani and Bulusu, (2018)), Alzahrani et al. proposed a game theoretic based consensus algorithm. In their consensus algorithm, a variable number of validators are determined dynamically based on game theory. Selecting only a valid number of honest validators results in a reduction of the likelihood of risk. On the other hand, an artificial intelligence-based consensus algorithm has been proposed in (Chen et al., (2018)) to combine the advantages of DPoS, PoS, and PoW. In (Chaudhry and Yousaf, (2018)), the authors presented crucial parameters for designing consensus algorithms for divergent applications such as blockchain type, adversary tolerance, scalability, communication model, throughput, bandwidth, and consensus finality. However, the designing and implementation of such consensus algorithms require further research.

6.3. *Scalability*

Scalability refers to the operation of the smart environments enabled by blockchain without losing QoS with an increase in the number of smart city devices. On the other hand, key design aspects of a typical blockchain network are fault tolerance, security, and decentralization. However, achieving these features simultaneously causes limitations on scalability which is one of the primary important parameters in smart city design. Every full node in a blockchain network requires to store a growing number of records as well as to participate in the validation process. Therefore, a typical blockchain is intrinsically arduous to scale because of its fully decentralized nature. It is expected that the number of smart IoT devices will reach 64B in 2025 (Exciting Internet of Things,). Such an unprecedented increase in smart IoT devices imposes challenges on the design of scalable blockchain-enabled smart city infrastructure. Therefore, it is necessary to enable the scalable operation of the blockchain-enabled smart city services by devising scalable consensus algorithms with consistency, availability, and partition tolerance (Carrara et al., 2020). Numerous solutions have been proposed to enable scalability in blockchain (Cong et al., 2018; Hazari and Mahmoud, 2019). In (Cong et al., (2018)), Cong et al. proposed a horizontal scalable solution to blockchain. Special blocks such as checkpoint blocks were considered to reach consensus rather than all transactions. PoW is a consensus algorithm that aims to maintain the integrity and immutability of a blockchain network. However, the conventional PoW protocol seriously hinders the scalability of blockchain in terms of transactions per second. To mitigate the scalability issues of the conventional PoW protocol, a PoW based on parallel mining is proposed for the blockchain network in (Hazari and Mahmoud, (2019)). However, this solution relies on the manager node that has the issue of a single point of failure.

Table 7
Summary of the research challenges along with their causes and possible guidelines.

Challenges	Causes	Guidelines
Sustainability	• Depletion of energy resources by smart city devices • Higher energy consumption of various consensus algorithms	• Use of renewable energy resources • Use of energy harvesting • Energy efficient consensus algorithms
Adaptive Consensus Algorithm	• Requirement diversity of various smart city applications • Specific design objective dependent nature of various blockchain consensus algorithms	• A game theoretic-based adaptive consensus algorithm • Artificial intelligence-based consensus algorithm
Scalability	• Unprecedented increase in Smart IoT devices • Storage requirement of all records by every node in blockchain network by traditional consensus algorithms	• Horizontal scalability • PoW based on parallel mining
Latency	• Validation of transactions • Scalability • Forking effect due to propagation delay	• Closest Neighbors Selecting (CNS) based propagation scheme • An acknowledgment-based scheme to avoid forking
High Performance Computing Memories	• Scalability limitations • Huge data storage • Centralized off-chain storage is unreliable • Decentralized off-chain storage are publicly accessible	• On-node high performance computing memories • Off-node high performance computing storage • Use decentralized off-chain storage such as IPFS • Do encryption before uploading to decentralized off-chain storage
Secure Economical Models	• Significant diversity in smart services requirements • Existence of wide variety of players in a smart city • Diverse security requirements of different smart city slices	• Blockchain-based brokering mechanism for smart city slices • Dynamic pricing models
Identity and Privacy	• Links between public blockchain addresses and transactions can breach user real identity • Centralized digital identity management systems are not secured city • SSI and DID have human dependency • User data in public blockchain is usually accessible to every one	• Use new address for each new transaction • Use mixers for cryptocurrency based applications • Decentralized Self-sovereign identity provide the user full control over her identity and data • Devise secure decentralized recovery mechanisms for SSI and DID • Distributed consent management for data sharing • Zero-knowledge proofs-based double-blind data sharing for anonymous data sharing • on chain encryption and encryption techniques for privacy of user data
Smart contract immutability and chain-boundedness	• Smart contract once deployed are immutable • Deploying a new contract for each upgrade has trust and discrepancy issue. • Smart contract cannot initiate deterministic external requests	• Sperate data and logic • Delegate-call from proxy-contract to logic-contract • Use event-triggered-oracle-data-feeds for deterministic external information

6.4. Latency

Latency represents transaction processing time, whereas throughput indicates a maximum number of transactions within a certain predefined time. Both latency and throughput constraints significantly affect the scalability of smart cities. In a blockchain-enabled smart city, delay happens due to computation at decentralized computing nodes. Other than computation at local nodes, communication of data among nodes further added to delay. Both of these delays determine the latency and throughput of the blockchain network. Therefore, various solutions must be proposed to enable smart cities by blockchain with low latency and higher throughput. Latency due to propagation delay causes forking. For instance, a successful miner broadcasts a block to a network. A miner other than a broadcasting miner may broadcast its block in a network before receiving a block of the other miner. This forking effect causes possession of multiple blocks by miners. To avoid the forking effect, propagation delay must be minimized. In (Bi et al., (2018)), a Closest Neighbors Selecting (CNS) scheme is used to reduce the propagation delay in the blockchain network. Another way to avoid the forking effect is the use of acknowledgment upon receiving a new block to indicate whether forking occurred or not(Kim et al., 2020). Following the forking occurred, the operation of block generation restarts. This process continues until the block update happens without forking. The forking effect causes the probabilistic confirmation of transactions because there is a rollback possibility in a case when a long chain does not include the relevant block in the future. For example, it is advised to wait for at least 6 block confirmations in bitcoin, which accumulate to an hour delay. To mitigate the forking effect (Hari et al., 2019), proposed a 'deterministic transaction confirmation' scheme named 'ACCEL'. The ACCEL has low-latency but high throughput. It exploits upper-bound on end-to-end delay for PoS-based blockchain to prevent forking. Smart city services that are based on PoS-driven blockchain can adopt the ACCEL.

6.5. High-performance computing memories and storage

A remarkable increase in smart IoT devices is expected in the foreseeable future of smart cities. Providing blockchain-based smart services to these devices poses a significant challenge of high storage requirements. Every device in a blockchain network must maintain a complete set of transactions. Such type of higher storage requirement of blockchain nodes limits the scalability of the blockchain network. On the other hand, scalability is one of the essential requirements of smart cities. Therefore, to enable the scalable operation of blockchain-enabled smart cities, it is indispensable to use high-performance computing memories with higher storage capability and low power consumption. Other than the use of high-performance computing memories located at a blockchain node, storage can be performed off the blockchain network. Enabling such type of storage via high-performance computing memory other than blockchain network nodes at a centralized location poses security and robustness challenges. Malfunctioning of the centralized memory results in the interruption of the blockchain-based smart city services. Another disadvantage of using external memory is an increase in cost and complicity associated with its management. Instead of centralized storage, blockchains may use off-chain decentralized storage and file system such as IPFS and Swarm. However, IPFS and Swarm are publicly accessible which hinders their use for sensitive data. Nevertheless, data can be encrypted before uploading to IPFS, however, this adds more encryption-decryption-delay. Asides, the sharing of encryption-decryption keys in a decentralized but secure manner is another issue.

6.6. Secure economical models

Future smart cities are expected to use 5G and beyond telecommunication networks along with other emerging computing paradigms to provide numerous smart services with significantly diverse requirements. To enable these smart services with dynamic requirements network slicing (Khan et al., 2020e) is a viable solution. Network slicing is based on the creation of logical networks over the top of physical network infrastructures. The network slicing operator must buy different physical resources from service providers and selling them to smart citizens. Enabling network slicing in smart cities requires novel and secure economical models that simultaneously improve the user QoE and service provider's profit. Numerous standalone economic models exist for driving players of a smart city. However, we need to devise novel economical models for smart city services for a full filling of a wide variety of customer expectations. These applications and user-dependent expectations include latency, operational efficiency, privacy, security, service provider's profit, users QoE, among others. To offer smart cities with a variety of services via network slicing, the use of blockchain to provide a secure brokering mechanism for network slicing is indispensable. Blockchain-Based brokers purchase resources from the numerous resource providers (Xie et al., 2020) while selling it to smart citizens of different verticals in a secure way (Nour et al., 2019).

6.7. Identity and privacy

In public blockchains, each transaction can be viewed by anyone. Each participating device can be identified using its public address. Although the public address is pseudonymous, curious malicious actors that have some background information can exploit the links between public addresses and transactions user's real-world identity. In cryptocurrency-enabled smart city applications, the privacy issue can be mitigated by generating a new disposable address for each new payment as well as using mixers that collect and redistribute coins to relevant stakeholders.

Currently, the identity of the user in smart city services is provided using digital identity management systems administrated by central authorities. Self-sovereign Identity (SSI) and Decentralized ID (DID) enable users to fully control their digital identity without an intermediate centralized third party. This allows users to control how their personally-identifiable information and data are shared. In the IoT-enabled smart city services, blockchain-enabled SSI and DID can be used for identification, authentication, and authorization of users in a decentralized manner. However, SSI and DID pose several issues such as human dependency (i.e., a user may lose the private key). Devising secure recovery mechanisms for SSI and DID is a crucial challenge.

User data and user-pseudonymous-identity in the public blockchain is usually accessible to everyone and thus creates privacy concerns and identity threats. Innovative privacy methods such as zero-knowledge proofs-based distributed consent management and double-blind data sharing can be applied for selective data sharing in mutually anonymous multi-party transactions in a privacy-preserving manner in various smart city services (Bhaskaran et al., 2018). While symmetric on-chain encryption and other encryption techniques may be applied to the transaction data itself. One of the limitations is that all these techniques add more latency to the network.

6.8. Smart contract immutability and chain-boundedness

Smart contracts are immutable that help to establish trust between the contracting parties. However, the smart contract code (e.g., on Ethereum Platform) is usually not upgradeable even in case of bugs, vulnerabilities, or new business-logic specifications. The updated code of the smart contract is usually deployed in a new instance with a new contract address which may have discrepancy issues. However, one way around for an upgradeable smart contract is to delegate-call from proxy-contract to new logic-contract (Pustišek et al., 2020). The proxy-contract holds the data while the logic-contract executes the new logic. The logic-contract address is updated in proxy-contract for each update. The user of smart city service is unaffected by the update as his data is safe in proxy-contract. Yet, the proxy-contact-delegation-call method has trust and decentralization issues. The researchers are devising partially upgradeable strategies for a smart contract that do not allow updates of core functionalities of a smart contract, but some parts are still upgradable.

Another pressing issue in the smart contract is chain-boundedness as there is no mechanism for a smart contract to initiate external requests. The only deterministic-way the smart contract interacts with external real-world information is through event-triggered-oracle-data-feeds for deterministic information. However, the decentralization, determinism, authenticity, trust, and security of oracles are important open research issues.

7. Conclusion

Blockchain has emerged as a disruptive technology for secure P2P interaction in an untrusted environment with disintermediation. In this paper, we have explored the role of blockchain in smart cities. We chronologically investigated the genesis of blockchain technology as well as its inception and further enhancements. For this, we discussed the constituent technologies in blockchain technology. We reviewed the prevailing blockchain platforms and consensus algorithms available in the blockchain ecosystem for engaging in smart city applications. We provided the technical diligence of potential applications for blockchain utilization as a discussion. We outlined important factors influencing the selection of a blockchain platform. We critically reviewed the literature utilizing blockchain in prominent smart city applications. We presented real-world case studies that effectively employed blockchain to provide reliable and secure services in smart cities. We discussed the fundamental data-centric requirements for the employment of blockchain in smart cities. We presented the open research challenges preventing blockchain to become a key technology in innovating smart cities.

We conclude that blockchain will be a key technology in the era of a data-driven world. Innovations in blockchain technologies and their implementation in smart cities, to improve the quality of life, is a popular area in contemporary research communities. However, there are still many challenges and requirement constraints to be explored and resolved for employing blockchain in sustainable urban development initiatives. This survey can help researchers to identify and tackle the challenges involved in designing and developing blockchain-based solutions for IoT-based smart cities.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Abeyratne, S.A., Monfared, R.P., 2016. Blockchain ready manufacturing supply chain using distributed ledger. Int. J. Renew. Energy Technol. 5 (9), 1–10.

Ahmed, S., Shah, M.A., Wakil, K., 2020. Blockchain as a trust builder in the smart city domain: a systematic literature review. IEEE Access 8, 92977–92985. https://doi.org/10.1109/ACCESS.2020.2993724.

Al Nuaimi, E., Al Neyadi, H., Mohamed, N., Al-Jaroodi, J., 2015. Applications of big data to smart cities. Journal of Internet Services and Applications 6 (1), 25.

Alahmadi, A., Lin, X., 2019. Towards secure and fair IIoT-enabled supply chain management via blockchain-based smart contracts. In: IEEE International Conference on Communications (ICC), Shanghai, China, pp. 1–7.

Ali, M.S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., Rehmani, M.H., 2019a. Applications of blockchains in the internet of things: a comprehensive survey. IEEE Communications Surveys Tutorials 21 (2), 1676–1717.

Ali, G., Ahmad, N., Cao, Y., Ali, Q.E., Azim, F., Cruickshank, H., 2019b. BCON: blockchain based access CONtrol across multiple conflict of interest domains. J. Netw. Comput. Appl. 147, 102440.

Alladi, T., Chamola, V., Parizi, R.M., Choo, K.R., 2019. Blockchain applications for industry 4.0 and industrial iot: a review. IEEE Access 7, 176935–176951. https://doi.org/10.1109/ACCESS.2019.2956748.

Alm, J., Lindblad, J., Meddeb, J., Nord, P., Söderberg, K., Wall, J., 2019. Toward a Framework for Assessing Meaningful Differences between Blockhain Platforms.

Alzahrani, N., Bulusu, N., 2018. Towards true decentralization: a blockchain consensus protocol based on game theory and randomness. In: International Conference on Decision and Game Theory for Security. Springer, Seattle, WA, USA, pp. 465–485.

Anderson, J.C., Lehnardt, J., Slater, N., 2010. CouchDB: the Definitive Guide: Time to Relax. O'Reilly Media, Inc.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., et al., 2018. Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the 13th EuroSys Conference. ACM, Porto, Portugal, pp. 1–30.

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

Asgaonkar, A., Krishnamachari, B., 2018. 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 arXiv:1806.08379.

Atzei, N., Bartoletti, M., Cimoli, T., 2017. A survey of attacks on ethereum smart contracts (sok). In: Principles of Security and Trust. Springer, pp. 164–186.

Avantaggiato, M., Gallo, P., 2019. Challenges and opportunities using MultiChain for real estate. In: IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom). Sochi, Russia, pp. 1–5.

Ayed, A.B., 2017. A conceptual secure Blockchain-based electronic voting system. Int. J. Netw. Secur. Appl. 9 (3), 1–9.

Azaria, A., Ekblaw, A., Vieira, T., Lippman, A., 2016. MedRec: using blockchain for medical data access and permission management. In: IEEE 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, pp. 25–30.

Bansod, G., Raval, N., Pisharoty, N., 2015. Implementation of a new lightweight encryption design for embedded security. IEEE Trans. Inf. Forensics Secur. 10 (1), 142–151.

Beck, R., Czepluch, J.S., Lollike, N., Malone, S., 2016. Blockchain-the gateway to trust-free cryptographic transactions. In: Proceedings of the 24th European Conference on Information Systems (ECIS). Istanbul, Turkey, pp. 1–15 research Papers. 153.

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

Bi, W., Yang, H., Zheng, M., 2018. An Accelerated Method for Message Propagation in Blockchain Networks arXiv:1809.00455.

Biswas, K., Muthukkumarasamy, V., 2016. Securing smart cities using blockchain technology. In: IEEE 18th International Conference on High Performance Computing and Communications, Sydney, Australia, pp. 1392–1393.

Bitcoin Core Developers. Bitcoin core. https://bitcoin.org.

Bitcoin market capitalization. https://coinmarketcap.com/currencies/bitcoin/. (Accessed 20 March 2020).

Bitcoin Wiki, 2018. Script. https://en.bitcoin.it/wiki/Script.

Blackshear, S., Cheng, E., Dill, D.L., Gao, V., Maurer, B., Nowacki, T., Pott, A., Qadeer, S., Rain, D.R., Sezer, S., et al., 2019. Move: a language with programmable resources. https://developers.libra.org/docs/assets/papers/libra-move-a-language-with-programmable-resources.pdf.

Blockchain Market by Component (Platform and Services), Provider (Application, Middleware, and Infrastructure), Type (Private, Public, and Hybrid), Organization Size, Application Area (BFSI, Government, IT & Telecom), and Region - Global Forecast to 2025, 2020. https://www.marketsandmarkets.com/Market-Reports/blockchain-technology-market-90100890.html. (Accessed 10 July 2020).

Buterin, V., 2014. DAOs, DACs, DAS and More: an Incomplete Terminology Guide. Ethereum Blog.

Buterin, V., Griffith, V., 2017. Casper the Friendly Finality Gadget arXiv preprint arXiv:1710.09437.

Buterin, V., et al., 2014. A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum White paper. https://github.com/ethereum/wiki/wiki/White-Paper.

Butt, T.A., Iqbal, R., Salah, K., Aloqaily, M., Jararweh, Y., 2019. Privacy management in social internet of vehicles: review, challenges and blockchain based solutions. IEEE Access 7, 79694–79713.

Cai, W., Wang, Z., Ernst, J.B., Hong, Z., Feng, C., Leung, V.C., 2018. Decentralized applications: the blockchain-empowered software system. IEEE Access 6, 53019–53033.

Can blockchain technology solve the problem of illegal fishing. https://www.investopedia.com/news/can-blockchain-technology-solve-problem-illegal-fishing. (Accessed 15 January 2020).

Carrara, G.R., Burle, L.M., Medeiros, D.S.V., de Albuquerque, C.V.N., Mattos, D.M.F., 2020. Consistency, availability, and partition tolerance in blockchain: a survey on the consensus mechanism over peer-to-peer networking. Annals of Telecommunications 75 (3–4), 163–174.

Castro, M., Liskov, B., et al., 1999. Practical byzantine fault tolerance. In: Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI), vol. 99, pp. 173–186. Berkeley, CA, USA.

Chalaemwongwan, N., Kurutach, W., 2018. State of the art and challenges facing consensus protocols on blockchain. In: IEEE International Conference on Information Networking (ICOIN). Chiang Mai, Thailand, pp. 957–962.

Chaturvedi, K., Rao, S., 2019. Distributed elections using site-push majority winner monitoring. IEEE Systems Journal 14 (2), 1682–1691.

Chaudhry, N., Yousaf, M.M., 2018. Consensus algorithms in blockchain: comparative analysis, challenges and opportunities. In: 2018 12th International Conference on Open Source Systems and Technologies (ICOSST). IEEE, pp. 54–63.

Chen, J., Duan, K., Zhang, R., Zeng, L., Wang, W., 2018. An AI Based Super Nodes Selection Algorithm in Blockchain Networks arXiv:1808.00216.

Chen, F., Xiao, Z., Cui, L., Lin, Q., Li, J., Yu, S., 2020. Blockchain for internet of things applications: a review and open issues. J. Netw. Comput. Appl. 172, 102839.

Cho, H., 2018a. Asic-resistance of multi-hash proof-of-work mechanisms for blockchain consensus protocols. IEEE Access 6, 66210–66222.

Cho, H., 2018b. Asic-resistance of multi-hash proof-of-work mechanisms for blockchain consensus protocols. IEEE Access 6, 66210–66222.

Christidis, K., Devetsikiotis, M., 2016. Blockchains and smart contracts for the internet of things. IEEE Access 4, 2292–2303.

Cong, K., Ren, Z., Pouwelse, J., 2018. A blockchain consensus protocol with horizontal scalability. In: IFIP Networking Conference (IFIP Networking) and Workshops. IEEE, Zurich, Switzerland, pp. 1–9.

Conti, M., Sandeep Kumar, E., Lal, C., Ruj, S., 2018. A survey on security and privacy issues of bitcoin. IEEE Communications Surveys Tutorials 20 (4), 3416–3452.

Cui, L., Xie, G., Qu, Y., Gao, L., Yang, Y., 2018. Security and privacy in smart cities: challenges and opportunities. IEEE Access 6, 46134–46145.

Dang, C., Zhang, J., Kwong, C., Li, L., 2019. Demand side load management for big industrial energy users under blockchain-based peer-to-peer electricity market. IEEE Transactions on Smart Grid 10 (6), 6426–6435.

Deirmentzoglou, E., Papakyriakopoulos, G., Patsakis, C., 2019. A survey on long-range attacks for proof of stake protocols. IEEE Access 7, 28712–28725.

DESA, U.N., 2018. 2018 Revision of World Urbanization Prospects. https://www.un.org/development/desa/publications/2018-revision-of-world-urbanization-prospects.html. (Accessed 20 March 2020).

Dhillon, V., Metcalf, D., Hooper, M., 2017. Recent developments in blockchain. In: Blockchain Enabled Applications. Springer, pp. 151–181.

Diffie, W., Hellman, M., 1976. New directions in cryptography. IEEE Trans. Inf. Theor. 22 (6), 644–654.

Dinh, T.T.A., Wang, J., Chen, G., Liu, R., Ooi, B.C., Tan, K.-L., 2017. Blockbench: a framework for analyzing private blockchains. In: Proceedings of the 2017 ACM International Conference on Management of Data. ACM, Chicago, USA, pp. 1085–1100.

Dinh, T.T.A., Liu, R., Zhang, M., Chen, G., Ooi, B.C., Wang, J., 2018. Untangling blockchain: a data processing view of blockchain systems. IEEE Trans. Knowl. Data Eng. 30 (7), 1366–1385.

L. N. documentation, Lto Network, Europe's Leading Hybrid Blockchain Platform: the New Standard for Data Security and Collaboration.

Dorri, A., Kanhere, S.S., Jurdak, R., 2017a. Towards an optimized BlockChain for IoT. In: 2017 IEEE/ACM Second International Conference on Internet-Of-Things Design and Implementation (IoTDI), Pittsburgh, PA, USA, pp. 173–178.

Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P., 2017b. Blockchain for IoT security and privacy: the case study of a smart home. In: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, pp. 618–623.

Dubai blockchain strategy. https://www.smartdubai.ae/initiatives/blockchain. (Accessed 20 February 2020).

Dubai has world's first government entity to conduct transactions through Blockchain network. Gulf News. http://gulfnews.com/business/property/dubai-has-world-s-firstgovernment-entity-to-conduct-transactions-through-blockchain-network-1.2101819. (Accessed 20 February 2020).

Dwork, C., Naor, M., 1992. Pricing via processing or combatting junk mail. In: Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology. Springer, Santa Barbara, California, pp. 139–147.

Eckhoff, D., Wagner, I., 2018. Privacy in the smart city—applications, technologies, challenges, and solutions. IEEE Communications Surveys Tutorials 20 (1), 489–516.

Emmanuel, M., Rayudu, R., 2016. Communication technologies for smart grid applications: a survey. J. Netw. Comput. Appl. 74, 133–148.

EOSIO, 2018. EOS.IO, Technical White Paper V2. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md.

Exciting internet of things statistics. https://techjury.net/stats-about/internet-of-things-statistics/. (Accessed 15 January 2020).

Feng, Q., He, D., Zeadally, S., Khan, M.K., Kumar, N., 2019. A survey on privacy protection in blockchain system. J. Netw. Comput. Appl. 126, 45–58.

Fernandez, C., Hickmott, S., Norta, A., 2018. Tokenizing commercial property with smart contracts. https://www.evareium.io/img/Evareium%20EVRM%20DSO%20White%20Paper%20H218A.pdf.

Fernández-Caramés, T.M., Fraga-Lamas, P., 2018. A review on the use of blockchain for the internet of things. IEEE Access 6, 32979–33001.

Ferrag, M.A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., Janicke, H., 2019. Blockchain technologies for the internet of things: research issues and challenges. IEEE Internet of Things Journal 6 (2), 2188–2204.

FutureScape, I.D.C.. Worldwide IT industry 2018 predictions. https://www.idc.com/getdoc.jsp?containerId=US43171317.

Gaži, P., Kiayias, A., Russell, A., 2018. Stake-bleeding attacks on proof-of-stake blockchains. In: IEEE Crypto Valley Conference on Blockchain Technology (CVCBT). Zug, Switzerland, pp. 85–92.

Gharaibeh, A., Salahuddin, M.A., Hussini, S.J., Khreishah, A., Khalil, I., Guizani, M., Al-Fuqaha, A., 2017. Smart cities: a survey on data management, security, and enabling technologies. IEEE Communications Surveys and Tutorials 19 (4), 2456–2501.

Gimein, M., 2013. Virtual Bitcoin Mining Is a Real-World Environmental Disaster. https://www.bloomberg.com/news/articles/2013-04-12/virtual-bitcoin-mining-is-a-real-world-environmental-disaster. (Accessed 20 March 2020).

Glover, W., Li, Q., Naveh, E., Gross, M., 2017. Improving quality of care through integration in a hospital setting: a human systems integration approach. IEEE Trans. Eng. Manag. 64 (3), 365–376.

Greenspan, G., 2015. Multichain Private Blockchain. white paper.

Haber, S., Stornetta, W.S., 1990. How to time-stamp a digital document. In: Conference on the Theory and Application of Cryptography. Springer, Berlin, Heidelberg, pp. 437–455.

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

Hari, A., Kodialam, M., Lakshman, T.V., 2019. Accel: accelerating the bitcoin blockchain for high-throughput, low-latency applications. In: IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, pp. 2368–2376. https://doi.org/10.1109/INFOCOM.2019.8737556.

Hasan, H.R., Salah, K., 2018a. Blockchain-based proof of delivery of physical assets with single and multiple transporters. IEEE Access 6, 46781–46793.

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

Hazari, S.S., Mahmoud, Q.H., 2019. 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), Las Vegas, NV, USA, pp. 916–921.

Hildenbrandt, E., Saxena, M., Rodrigues, N., Zhu, X., Daian, P., Guth, D., Moore, B., Park, D., Zhang, Y., Stefanescu, A., et al., 2018. Kevm: a complete formal semantics of the ethereum virtual machine. In: IEEE 31st Computer Security Foundations Symposium (CSF), Oxford, United Kingdom, pp. 204–217.

How blockchain is strengthening tuna traceability to combat illegal fishing?. https://theconversation.com/how-blockchain-is-strengthening-tuna-traceability-to-combat-illegal-fishing-89965. (Accessed 20 February 2020).

Hyperledger Fabric licence, 2017. https://github.com/hyperledger/fabric.

Hyperledger project, 2015. https://www.hyperledger.org/.

Ibba, S., Pinna, A., Seu, M., Pani, F.E., 2017. Citysense: blockchain-oriented smart cities. In: Proceedings of the XP2017 Scientific Workshops. ACM, Cologne, Germany, pp. 1–12.

IDC Trackers, 2020. Worldwide Smart Cities Spending Guide. https://www.idc.com/tracker/showproductinfo.jsp?prod_id=1843. (Accessed 10 July 2020).

Jakobsson, M., Juels, A., 1999. Proofs of work and bread pudding protocols. In: Secure Information Networks. Springer, pp. 258–272.

Jentzsch, C., 2016. Decentralized Autonomous Organization to Automate Governance. White paper.

Jose, A.C., Malekian, R., 2017. Improving smart home security: integrating logical sensing into smart home. IEEE Sensor. J. 17 (13), 4269–4286.

Kabra, N., Bhattacharya, P., Tanwar, S., Tyagi, S., 2020. Mudrachain: blockchain-based framework for automated cheque clearance in financial institutions. Future Generat. Comput. Syst. 102, 574–587.

Khan, M.A., Salah, K., 2018. Iot security: review, blockchain solutions, and open challenges. Future Generat. Comput. Syst. 82, 395–411.

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

Khan, L.U., Tran, N.H., Pandey, S.R., Saad, W., Han, Z., Nguyen, M.N.H., Hong, C.S., 2019. Federated Learning for Edge Networks: Resource Optimization and Incentive Mechanism arXiv:1911.05642.

Khan, L.U., Yaqoob, I., Tran, N.H., Kazmi, S.M.A., Dang, T.N., Hong, C.S., 2020a. Edge-computing-enabled smart cities: a comprehensive survey. IEEE Internet of Things Journal 7 (10), 10200–10232.

Khan, L.U., Yaqoob, I., Imran, M., Han, Z., Hong, C.S., 2020b. 6G wireless systems: a vision, architectural elements, and future directions. IEEE Access 8, 147029–147044.

Khan, K.M., Arshad, J., Khan, M.M., 2020c. Investigating performance constraints for blockchain based secure e-voting system. Future Generat. Comput. Syst. 105, 13–26.

Khan, L.U., Saad, W., Han, Z., Hong, C.S., 2020d. Dispersed Federated Learning: Vision, Taxonomy, and Future Directions arXiv:2008.05189.

Khan, L.U., Yaqoob, I., Tran, N.H., Han, Z., Hong, C.S., 2020e. Network slicing: recent advances, taxonomy, requirements, and open research challenges. IEEE Access 8, 36009–36028.

Kim, H., Park, J., Bennis, M., Kim, S., 2020. Blockchained on-device federated learning. IEEE Commun. Lett. 24 (6), 1279–1283.

King, S., Nadal, S., 2012. PPcoin: Peer-To-Peer Crypto-Currency with Proof-Of-Stake. https://www.peercoin.net/assets/paper/peercoin-paper.pdf.

Konečný, J., McMahan, H.B., Yu, F.X., Richtárik, P., Suresh, A.T., Bacon, D., 2016. Federated Learning: Strategies for Improving Communication Efficiency arXiv:1610.05492.

Kshetri, N., Voas, J., 2018. Blockchain-enabled e-voting. IEEE Software 35 (4), 95–99.

Lamport, L., 1984. Using time instead of timeout for fault-tolerant distributed systems. ACM Trans. Program Lang. Syst. 6 (2), 254–280.

Lamport, L., Shostak, R., Pease, M., 1982. The byzantine generals problem. ACM Trans. Program Lang. Syst. 4 (3), 382–401.

D. Larimer, Delegated Proof-Of-Stake (DPoS), Bitshare whitepaper.

Larimer, D., 2014. Delegated Proof of Stake. https://how.bitshares.works/en/master/technology/dpos.html. (Accessed 20 March 2020).

Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., Zhang, Y., 2018. Consortium blockchain for secure energy trading in industrial internet of things. IEEE Transactions on Industrial Informatics 14 (8), 3690–3700.

Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q., 2020. A survey on the security of blockchain systems. Future Generat. Comput. Syst. 107, 841–853.

Libra Association, 2019. An introduction to Libra. https://libra.org/en-US/whitepaper/.

Lin, F., Qiang, M., 2019. The challenges of existence, status and value for improving blockchain. IEEE Access 7, 7747–7758.

Lin, C., He, D., Huang, X., Choo, K.-K.R., Vasilakos, A.V., 2018. BSeIn: a blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. J. Netw. Comput. Appl. 116, 42–52.

Linn, L.A., Koo, M.B., 2016. Blockchain for health data and its potential use in health it and health care related research. In: ONC/NIST Use of Blockchain for Healthcare and Research Workshop, Gaithersburg, Maryland, United States, pp. 1–10.

Liu, Z., Luong, N.C., Wang, W., Niyato, D., Wang, P., Liang, Y., Kim, D.I., 2019a. A survey on blockchain: a game theoretical perspective. IEEE Access 7, 47615–47643.

Liu, C., Xiao, Y., Javangula, V., Hu, Q., Wang, S., Cheng, X., 2019b. NormaChain: a blockchain-based normalized autonomous transaction settlement system for IoT-based E-commerce. IEEE Internet of Things Journal 6 (3), 4680–4693.

Liu, Y., He, D., Obaidat, M.S., Kumar, N., Khan, M.K., Raymond Choo, K.-K., 2020. Blockchain-based identity management systems: a review. J. Netw. Comput. Appl. 166, 102731.

Ma, H., Huang, E.X., Lam, K.-Y., 2020. Blockchain-based mechanism for fine-grained authorization in data crowdsourcing. Future Generat. Comput. Syst. 106, 121–134.

Magazzeni, D., McBurney, P., Nash, W., 2017. Validation and verification of smart contracts: a research agenda. Computer 50 (9), 50–57.

Majeed, U., Hong, C.S., 2019. Flchain: federated learning via mec-enabled blockchain network. In: 20th Asia-Pacific Network Operations and Management Symposium (APNOMS). Matsue, Japan, pp. 1–4.

Mantelero, A., 2013. The eu proposal for a general data protection regulation and the roots of the 'right to be forgotten'. Comput. Law Secur. Rep. 29 (3), 229–235.

McGhin, T., Choo, K.-K.R., Liu, C.Z., He, D., 2019. Blockchain in healthcare applications: research challenges and opportunities. J. Netw. Comput. Appl. 135, 62–75.

R. Merkle, reportSecrecy, Authentication, and Public Key Systems, Ph. D. Thesis, Stanford University.

Merkle, R.C., 1980. Protocols for public key cryptosystems. In: 1980 IEEE Symposium on Security and Privacy, Oakland, California, USA, 122–122.

R. C. Merkle, Method of providing digital signatures, US Patent 4,309,569 (Jan. 5 1982).

Mettler, M., 2016. Blockchain technology in healthcare: the revolution starts here. In: IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom), Munich, Germany, pp. 1–3.

Mohanty, S.N., Ramya, K., Rani, S.S., Gupta, D., Shankar, K., Lakshmanaprabu, S., Khanna, A., 2020. An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy. Future Generat. Comput. Syst. 102, 1027–1037.

Musa, S., 2018. Smart cities-a road map for development. IEEE Potentials 37 (2), 19–23.

Musleh, A.S., Yao, G., Muyeen, S.M., 2019. Blockchain applications in smart grid–review and frameworks. IEEE Access 7, 86746–86757.

Nakamoto, S., 2008. Bitcoin: A Peer-To-Peer Electronic Cash System.

Nakamoto, S., 2010. Re: Transactions and Scripts: DUP HASH160…EQUALVERIFY CHECKSIG, Bitcointalk. https://bitcointalk.org/index.php?topic=195.

Nakamoto, S., Finny, H., Garzik, J., et al., 2009. Bitcoin core. https://bitcoin.org/en/download.

Nguyen, D.C., Pathirana, P.N., Ding, M., Seneviratne, A., 2020. Blockchain for 5G and beyond networks: a state of the art survey. J. Netw. Comput. Appl. 166, 102693.

Nogueira, A., Casimiro, A., Bessani, A., 2017. Elastic state machine replication. IEEE Trans. Parallel Distr. Syst. 28 (9), 2486–2499.

Norta, A., Fernandez, C., Hickmott, S., 2018. Commercial property tokenizing with smart contracts. In: International Joint Conference on Neural Networks (IJCNN), Rio de Janeiro, Brazil, pp. 1–8.

Nour, B., Ksentini, A., Herbaut, N., Frangoudis, P.A., Moungla, H., 2019. A blockchain-based network slice broker for 5G services. IEEE Networking Letters 1 (3), 99–102.

Osgood, R., 2016. The Future of Democracy: Blockchain Voting. COMP116: Information security, pp. 1–21.

O'Dwyer, K.J., Malone, D., 2014. Bitcoin mining and its energy footprint. In: 25th IET Irish Signals Systems Conference (ISSC) and China-Ireland International Conference on Information and Communications Technologies (CIICT). Limerick, Ireland, pp. 280–285.

Pahl, C., El Ioini, N., Helmer, S., 2018. A decision framework for blockchain platforms for IoT and edge computing. In: International Conference on Internet of Things, Big Data and Security (IoTBDS). Funchal, Madeira, Portugal, pp. 105–113.

Popov, S., 2018. The Tangle, IOTA Whitepaper. https://iota.org/IOTA_Whitepaper.pdf.

Pustišek, M., Turk, J., Kos, A., 2020. Secure modular smart contract platform for multi-tenant 5g applications. IEEE Access 8, 150626–150646.

Rathore, S., Wook Kwon, B., Park, J.H., 2019. BlockSecIoTNet: blockchain-based decentralized security architecture for IoT network. J. Netw. Comput. Appl. 143, 167–177.

Razaghi, M., Finger, M., 2018. Smart governance for smart cities. Proc. IEEE 106 (4), 680–689.

Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M., 2018. On blockchain and its integration with IoT. Challenges and opportunities. Future Generat. Comput. Syst. 88, 173–190.

Salah, K., Nizamuddin, N., Jayaraman, R., Omar, M., 2019. Blockchain-based soybean traceability in agricultural supply chain. IEEE Access 7, 73295–73305.

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

Schneider, F.B., 1990. Implementing fault-tolerant services using the state machine approach: a tutorial. ACM Comput. Surv. 22 (4), 299–319.

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

Shahaab, A., Lidgey, B., Hewage, C., Khan, I., 2019. Applicability and appropriateness of distributed ledgers consensus protocols in public and private sectors: a systematic review. IEEE Access 7 (2019), 43622–43636.

Shahzad, B., Crowcroft, J., 2019. Trustworthy electronic voting using adjusted blockchain technology. IEEE ACCESS 7, 24477–24488.

Sharma, P.K., Park, J.H., 2018. Blockchain based hybrid network architecture for the smart city. Future Generat. Comput. Syst. 86, 650–655.

She, W., Gu, Z., Lyu, X., Liu, Q., Tian, Z., Liu, W., 2019. Homomorphic consortium blockchain for smart home system sensitive data privacy preserving. IEEE Access 7, 62058–62070.

Shedroff, N., 2018. Self-managing real estate. Computer 51 (1), 104–104.

Shu, Y., Zhang, L., Zhao, W., Chen, H., Luo, J., 2006. P2p-based data system for the east experiment. IEEE Trans. Nucl. Sci. 53 (3), 694–699.

Singh, A., Parizi, R.M., Han, M., Dehghantanha, A., Karimipour, H., Choo, K.-K.R., 2020. Public blockchains scalability: an examination of sharding and segregated witness. In: Advances in Information Security. Springer International Publishing, pp. 203–232.

Smart Cities Market, 2020. Growth, trends, and forecast (2020 - 2025). https://www.mordorintelligence.com/industry-reports/smart-cities-market. (Accessed 10 July 2020).

Smart Dubai, 2016. Dubai Blockchain Strategy. Dubai Government.

Sookhak, M., Tang, H., He, Y., Yu, F.R., 2019. Security and privacy of smart cities: a survey, research issues and challenges. IEEE Communications Surveys Tutorials 21 (2), 1718–1743.

Szabo, N., 1994. Smart contracts. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

Szabo, N.. The idea of smart contracts, Nick szabo's papers and concise tutorials 6. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_idea.html.

Tang, H., Jiao, Y., Huang, B., Lin, C., Goyal, S., Wang, B., 2018. Learning to classify blockchain peers according to their behavior sequences. IEEE Access 6, 71208–71215.

The world's first Data Embassy – Estonia. https://e-estonia.com/wp-content/uploads/2019sept-facts-a4-data-embassy.pdf. (Accessed 20 February 2020).

The world's first data embassy – Estonia. https://www.oecd.org/gov/innovative-government/Estonia-case-study-UAE-report-2018.pdf. (Accessed 20 February 2020).

Tu, W., 2018. Data-driven QoS and QoE management in smart cities: a tutorial study. IEEE Commun. Mag. 56 (12), 126–133.

Vukolić, M., 2015. The quest for scalable blockchain fabric: proof-of-work vs. BFT replication. In: International Workshop on Open Problems in Network Security (iNetSec). Springer, Zurich, Switzerland, pp. 112–125.

Walmart is betting on the blockchain to improve food safety. https://techcrunch.com/2018/09/24/walmart-is-betting-on-the-blockchain-to-improve-food-safety. (Accessed 20 February 2020).

Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., Wang, F., 2019a. Blockchain-enabled smart contracts: architecture, applications, and future trends. IEEE Transactions on Systems, Man, and Cybernetics: Systems 49 (11), 2266–2277.

Wang, S., Ding, W., Li, J., Yuan, Y., Ouyang, L., Wang, F., 2019b. Decentralized autonomous organizations: concept, model, and applications. IEEE Transactions on Computational Social Systems 6 (5), 870–878.

Wang, H., Ma, S., Dai, H.-N., Imran, M., Wang, T., 2020a. Blockchain-based data privacy management with nudge theory in open banking. Future Generat. Comput. Syst. 110, 812–823.

Wang, Q., Zhu, X., Ni, Y., Gu, L., Zhu, H., 2020b. Blockchain for the Iot and Industrial Iot: A Review, Internet of Things 10, 100081, special Issue of the Elsevier IoT Journal on Blockchain Applications in IoT Environments.

Wang, E.K., Liang, Z., Chen, C.-M., Kumari, S., Khan, M.K., 2020c. Porx: a reputation incentive scheme for blockchain consensus of iiot. Future Generat. Comput. Syst. 102, 140–151.

Z. Wang, H. Jin, W. Dai, K.-K. R. Choo, D. Zou, Ethereum smart contract security research: survey and future research opportunities, Front. Comput. Sci. 15 (2).

Wojciechowski, P.T., Kobus, T., Kokociński, M., 2017. State-machine and deferred-update replication: analysis and comparison. IEEE Trans. Parallel Distr. Syst. 28 (3), 891–904.

Wood, G., 2014. Ethereum: a secure decentralised generalised transaction ledger. Ethereum project yellow paper 151, 1–32.

Wu, T., Liang, X., 2017. Exploration and practice of inter-bank application based on blockchain. In: 12th IEEE International Conference on Computer Science and Education. ICCSE, Houston, TX, USA, pp. 219–224.

Wu, M., Wang, K., Cai, X., Guo, S., Guo, M., Rong, C., 2019. A comprehensive survey of blockchain: from theory to IoT applications and beyond. IEEE Internet of Things Journal 6 (5), 8114–8154.

Wu, D., Wang, H., Seidu, R., 2020. Smart data driven quality prediction for urban water source management. Future Generat. Comput. Syst. 107, 418–432.

Xie, J., Tang, H., Huang, T., Yu, F.R., Xie, R., Liu, J., Liu, Y., 2019. A survey of blockchain technology applied to smart cities: research issues and challenges. IEEE Communications Surveys Tutorials 21 (3), 2794–2830.

Xie, S., Zheng, Z., Chen, W., Wu, J., Dai, H.-N., Imran, M., 2020. Blockchain for cloud exchange: a survey. Comput. Electr. Eng. 81, 106526.

P. Xu, Q. Wu, W. Wang, W. Susilo, J. Domingo-Ferrer, H. Jin, Generating Searchable Public-Key Ciphertexts with Hidden Structures for Fast Keyword Search, arXiv preprint arXiv:1512.06581.

Yang, M., Yang, Y., 2010. An efficient hybrid peer-to-peer system for distributed data sharing. IEEE Trans. Comput. 59 (9), 1158–1171.

Yang, J., Han, Y., Wang, Y., Jiang, B., Lv, Z., Song, H., 2020. Optimization of real-time traffic network assignment based on IoT data using DBN and clustering model in smart city. Future Generat. Comput. Syst. 108, 976–986.

Yaqoob, I., Salah, K., Uddin, M., Jayaraman, R., Omar, M., Imran, M., 2020. Blockchain for digital twins: recent advances and future research challenges. IEEE Network 34 (5), 290–298.

Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y., 2021. Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Comput. Appl. 1–16.

Youb, C., Mehlman, S., Zimits, M., Youb, B., 2019. Method for creating commodity assets from unrefined commodity reserves utilizing blockchain and distributed ledger technology. US Patent App 15/916, 128.

Yu, Y., Li, Y., Tian, J., Liu, J., 2018. Blockchain-based solutions to security and privacy issues in the internet of things. IEEE Wireless Communications 25 (6), 12–18.

Yuan, Y., Wang, F.-Y., 2016. Towards blockchain-based intelligent transportation systems. In: IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Rio de Janeiro, Brazil, pp. 2663–2668.

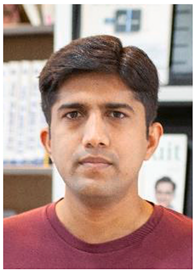
Yuen, T.H., 2020. PAChain: private, authenticated & auditable consortium blockchain and its implementation. Future Generat. Comput. Syst. 112, 913–929.

Zahed Benisi, N., Aminian, M., Javadi, B., 2020. Blockchain-based decentralized storage networks: a survey. J. Netw. Comput. Appl. 162, 102656.

Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H., 2017. An overview of blockchain technology: architecture, consensus, and future trends. In: IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, pp. 557–564.

Zheng, Z., Xie, S., Dai, H.-N., Wang, H., 2018. Blockchain challenges and opportunities: a survey. Int. J. Web Grid Serv. 14 (4), 352–375.

Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X., Weng, J., Imran, M., 2020. An overview on smart contracts: challenges, advances and platforms. Future Generat. Comput. Syst. 105, 475–491.



Umer Majeed is currently pursuing his Ph.D. degree in Computer Engineering at Kyung Hee University (KHU), South Korea. He is working as a researcher in the intelligent Networking Laboratory under a project jointly funded by the prestigious Brain Korea 21st Century Plus and Ministry of Science and ICT, South Korea. He received BS degree in Electrical Engineering from the National University of Science and Technology (NUST), Pakistan in 2015. He received the best paper award in 35th IEEE International Conference on Information Networking (ICOIN), Jeju Island, South Korea, in 2021. His research interest includes Blockchain, Mobile Edge Computing, Internet of Things, Machine Learning, and Wireless Networks.

Latif U. Khan is currently pursuing his Ph.D. degree in Computer Engineering at Kyung Hee University (KHU), South Korea. He is working as a leading researcher in the intelligent Networking Laboratory under a project jointly funded by the prestigious Brain Korea 21st Century Plus and Ministry of Science and ICT, South Korea. He received his MS (Electrical Engineering) degree with distinction from the University of Engineering and Technology (UET), Peshawar, Pakistan in 2017. Before joining the KHU, he has served as a faculty member and research associate in the UET, Peshawar, Pakistan. He has published his works in highly reputable conferences and journals. He is the author of the book "Network Slicing for 5G and Beyond Networks", Springer International Publishing, 2019. His research interests include analytical techniques of optimization and game theory to edge computing and end-to-end network slicing.

Ibrar Yaqoob (S′16-M′18-SM′19) is currently working with the Department of Electrical Engineering and Computer Science, Khalifa University, UAE. Previously, he worked as a research professor at the Department of Computer Science and Engineering, Kyung Hee University, South Korea, where he completed his postdoctoral fellowship under the prestigious grant of Brain Korea 21st Century Plus. Prior to that, he received his Ph.D. (Computer Science) from the University of Malaya, Malaysia, in 2017. He worked as a researcher and developer at the Centre for Mobile Cloud Computing Research (C4MCCR), University of Malaya. His numerous research articles are very famous and among the most downloaded in top journals. He has been listed among top researchers by Thomson Reuters (Web of Science) based on the number of citations earned in the last five years in six categories of Computer Science. He is currently serving/served as a guest/associate editor in various Journals. He has been involved in several conferences and workshops in various capacities. His research interests include big data, blockchain, edge computing, mobile cloud computing, the Internet of Things, healthcare, and computer networks.

S. M. Ahsan Kazmi is with the Institute of Information Security and Cyber Physical System, Innopolis University, Innopolis, Tatarstan, Russia, where he is currently working as an Assistant Professor. He received his master's degree in communication system engineering from the National University of Sciences and Technology (NUST), Pakistan, in 2012, and the Ph.D. degree in Computer Science and Engineering from Kyung Hee University (KHU), South Korea. His research interests include applying analytical techniques of optimization and game theory to radio resource management for future cellular networks. He received the best KHU Thesis Award in engineering in 2017 and several best paper awards from prestigious conferences.

Khaled Salah (Senior Member, IEEE) received the B.S. degree in computer engineering with a minor in computer science from Iowa State University, USA, in 1990, and the M.S. degree in computer systems engineering and the Ph.D. degree in computer science from the Illinois Institute of Technology, USA, in 1994 and 2000, respectively. He joined Khalifa University, United Arab Emirates, in August 2010, and is teaching graduate and undergraduate courses in the areas of cloud computing, computer and network security, computer networks, operating systems, and performance modeling and analysis. Prior to joining Khalifa University, he worked for ten years with the Department of Information and Computer Science, King Fahd University of Petroleum and Minerals (KFUPM), Saudi Arabia. He is currently a Full Professor with the Department of Electrical and Computer Engineering, Khalifa University. He has over 190 publications and three patents. He has been giving a number of international keynote speeches, invited talks, tutorials, and research seminars on the subjects of blockchain, IoT, fog and cloud computing, and cybersecurity. He was a recipient of the Khalifa University Outstanding Research Award 2014/2015, the KFUPM University Excellence in Research Award of 2008/09, and the KFUPM Best Research Project Award of 2009/10, and also a recipient of the departmental awards for the Distinguished Research and Teaching in prior years. He serves on the Editorial Boards of many WOS-listed journals, including IET Communications, IET Networks, Elsevier's JNCA, Wiley's SCN, Wiley's IJNM, J.UCS, and AJSE. He is the Track Chair of the IEEE GLOBECOM 2018 on Cloud Computing. He is also an Associate Editor of IEEE Blockchain Newsletter and a member of the IEEE Blockchain Education Committee.

Choong Seon Hong (S′95-M′97-SM′11) received the B.S. and M.S. degrees in electronic engineering from Kyung Hee University, Seoul, South Korea, in 1983 and 1985, respectively, and the Ph.D. degree from Keio University, Tokyo, Japan, in 1997. In 1988, he joined KT, Gyeonggi-do, South Korea, where he was involved in broadband networks as a member of the Technical Staff. Since 1993, he has been with Keio University. He was with the Telecommunications Network Laboratory, KT, as a Senior Member of Technical Staff and as the Director of the Networking Research Team until 1999. Since 1999, he has been a Professor with the Department of Computer Science and Engineering, Kyung Hee University. His research interests include future Internet, intelligent edge computing, network management, and network security. Dr. Hong is a member of the Association for Computing Machinery (ACM), the Institute of Electronics, Information and Communication Engineers (IEICE), the Information Processing Society of Japan (IPSJ), the Korean Institute of Information Scientists and Engineers (KIISE), the Korean Institute of Communications and Information Sciences (KICS), the Korean Information Processing Society (KIPS), and the Open Standards and ICT Association (OSIA). He has served as the General Chair, the TPC Chair/Member, or an Organizing Committee Member of international conferences, such as the Network Operations and Management Symposium (NOMS), International Symposium on Integrated Network Management (IM), Asia-Pacific Network Operations and Management Symposium (APNOMS), End-to-End Monitoring Techniques and Services (E2EMON), IEEE Consumer Communications and Networking Conference (CCNC), Assurance in Distributed Systems and Networks (ADSN), International Conference on Parallel Processing (ICPP), Data Integration and Mining (DIM), World Conference on Information Security Applications (WISA), Broadband Convergence Network (BcN), Telecommunication Information Networking Architecture (TINA), International Symposium on Applications and the Internet (SAINT), and International Conference on Information Networking (ICOIN). He was an Associate Editor of the IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT and the IEEE JOURNAL OF COMMUNICATIONS AND NETWORKS and an Associate Editor for the International Journal of Network Management and an Associate Technical Editor of the IEEE Communications Magazine. He currently serves as an Associate Editor for the International Journal of Network Management and Future Internet Journal.