Appendix A

SLR Output

SLR Summary Output

#	Database	Authors	Title	Journal	Vol (No)	Year of Publication	Pages	Overview	Findings
1	Science Direct	Sharma, K., Park, J.H.	Blockchain Based Hybrid Network Architecture for the Smart City	Future Generation Computer Systems	86	2018	pp. 650-655	Hybridised network architecture facilitates integrated network with the support of software-defined networking and a blockchain middle-layer	Blockchain solution must be a secure, scalable distributed architecture that connects computational storage resources and network endpoints. Architecture divided into core network and edge network. Proof of work scheme protects privacy and security.
2	Science Direct	Li, Y., Yang, W., He, P., Chen, C., Wang, X.	Design and Management of a Distributed Hybrid Energy System Through Smart Contract and Blockchain	Applied Energy	248(15)	2019	pp. 390-405	Peer-based exchange of real-time energy demand information to inform a non-cooperative, priority-based hierarchical framework for distribution.	Smart contracts utilising a decentralised identifier that leverage blockchain transactions ensure a seamless, secured, and efficient distributed energy system.
3	Science Direct	Li, Z., Bahramirad, S., Paaso, A., Yan, M., Shahidehpour, M. (2019)	Blockchain for Decentralized Transactive Energy Management System in Networked Microgrids	The Electricity Journal	32(4)	2019	pp. 58-72	Blockchain integration supports distributed data storage and management and can be customised to meet the socioeconomic requirements of transactive energy management	Self-enforcing smart contracts manage energy and financial flows among the transacting microgrids, optimising energy transactions, and ensuring secure, efficient exchanges
4	Science Direct	Reyna, A., Martin, C., Chen, J., Soler, E., Diaz, M.	On Blockchain and its Integration with IoT. Challenges and Opportunities	Future Generation Computer Systems	88	2018	pp.173-190	By introducing self-executable, quantifiable smart contracts, blockchain intermediation offers an autonomous, decentralised solution to negotiating triggers and fulfilment	IoT-blockchain interactions enable an immutable record of interactions, storing all data associated with these transactions in a decentralised network. However, a hybridised approach would allow real-time IoT interactions, with limited-resource devices serving as end-nodes that communicate with a central gateway. Lightweight nodes can be used to confirm the authenticity of transactions without having to download the entire blockchain (e.g. Ethereum). Fog computing could support distributed computing and formalise the connections between end devices and databases.

#	Database	Authors	Title	Journal	Vol (No)	Year of Publication	Pages	Overview	Findings
5	Science Direct	Casado-Vara, R., Chamos, P., De La Prieta, F., Prieto, J., Corchado, J.M.	Non-Linear Adaptive Closed-Loop Control System for Improved Efficiency in IoT-Blockchain Management	Information Fusion	49	2019	pp.227-239	Due to the significant amount of data generated by the IoT, high-efficiency servers are needed to process information and to facilitate the response protocol.	An adaptive, closed-loop control system is proposed which includes a non-linear control model designed to optimise the number of blocks in queue on the miners' network and accelerate searchers via hashmaps.
6	Science Direct	Hammi, M.T., Hammi, B., Bellot, P., Serhrouchni, A.	Bubbles of Trust: A Decentralized Blockchain-Based Authentication System for IoT	Computers and Security	78	2018	pp.126-142	Within the IoT things need to recognise and authenticate each other and ensure data integrity without human intervention. A revised security and integrity system is needed to preserve efficiency and authentication	The bubbles of trust methodology groups IoT nodes by their smart contracts reducing the number of authentications and improving the processing efficiency. Transaction signatures authenticate the individual objects and the data integrity is protected. Bubbles operate as forms of walled gardens to prevent interference
7	Science Direct	Yang, J., Lu, Z., Wu, J.	Smart-Toy-Edge-Computing-Oriented Data Exchange Based on Blockchain	Journal of Systems Architecture	87	2018	pp.36-48	Edge computing technology allows smart toys to generate valuable data; however, a secure and reliable data exchange mechanism has not been developed because of the isolation of smart toy data platforms	Exchange prototype (hyperledger Fabric v1.0) provides a tamper-resistant, reliable, and distributed ledger for writing smart contracts in risky environments. Allows for P2P data exchange between smart toy and other IoT nodes.
8	Science Direct	Dorri, A., Kanhere, S.S., Jurdak, R.	MOF-BC: A Memory Optimized and Flexible Blockchain for Large Scale Networks	Future Generation Computer Systems	92	2019	pp.357-373	Blockchain immutability ensures resilience against data modification; however, in the IoT, the data storage increases the storage size and raises privacy concerns. Aged transactions can be forgotten or summarised to reduce storage requirements	The Memory Optimised and Flexible BC solution resolves the key storage concerns and applies a Generator Verifier (signed hash) which changes for each transaction to provide privacy and minimizing information storage needs. Generalised solution to be implemented on top of any existing or future blockchain. Can reduce memory consumption by up to 25%

#	Database	Authors	Title	Journal	Vol (No)	Year of Publication	Pages	Overview	Findings
9	Wiley	Pahl, C., El Ioni, N., Helmer, S., lee, B.	A Semantic Pattern for Trusted Orchestration in IoT Edge Clouds	Internet Technology Letters	2(3)	2019	pp.1-17	For IoT optimality, edge cloud architecture provides an outlying layer between the centralised clouds and the IoT and sensor space. Trust orchestration is based upon trust ontology for reasoning of essential trust properties	By establishing intermediary trust between the object (e.g. IoT) and the subject (e.g. the agent), a trust-based orchestration framework is established that can be used to systematically regulate intermediary relationships. Blockchain intermediation serves to store identity, the orchestration contract, and the data provenance in separate blocks, allowing for in-out controls in the software layers.
10	Wiley	Tedeschi, P., Piro, G., Murillo, J.A.S., Ignajatov, N., Pilc, M., Lebloch, K., Boggia, G.	Blockchain as a Service: Securing Bartering Functionalities in the H2020 SymboloTe Framework	Internet Technology Letters	2(1)	2019	pp. 1-7	In the distributed IoT, access and interoperability create challenges across distributed platforms. By creating a blockchain intermediary solution to grant access to key resources, security and generality can be protected.	A smart contract solution based upon a central service layer provided by blockchain technologies for validating and granting access between parties to shared resources. Blockchain becomes the immutable, decentralised, and objective consensus mechanism capable of securing the transaction through cryptographic signing procedures.
11	Wiley	Pinno, O.J.A., Gregio, A.R.A., Bona, L.C.E	ControlChain: A New Stage on the IoT Access Control Authorization	Concurrency and Computation: Practice and Experience	3(1)	2019	pp. 1-8	IoT vulnerability to security infiltration has the potential to expose users to a broad range of vulnerabilities. Current access control systems fail to fulfil the comprehensive security needs necessary to negotiate network communication and smart data exchange.	A central, blockchain-based control authorisation architecture can leverage the Ethereum network to provide a user-friendly, fully decentralized, Scalable, fault tolerant, and compatible solution for IoT security needs. Middleware layer that centralises data security, whilst allowing outside companies to develop their own service technologies.

#	Database	Authors	Title	Journal	Vol (No)	Year of Publication	Pages	Overview	Findings
12	Wiley	Ouaddah, A., Elkalam, A.A., Ouahman, A.A.	FairAccess: A New Blockchain-Based Access Control Framework for the Internet of Things	Security and Communication Networks	9(18)	2016	pp. 5943-5964	For users to gain sufficient confidence in the management of personal information resources, some form of decentralised access control system is needed to transfer responsibility to individuals.	As the IoT is a collaborative environment, authorisation inherits collaborative principles, or coordinate environments. By differentiating between management and access controls, administration can be decentralised and provide varying service-level controls to varying individuals or groups. Smart contract utilises scripting language to express access control policies. Authorisation token (digital signature) entitles the transaction originator to gain access to a specific resource. Digital keys provide proof of ownership, allowing both public and private access to be assigned.
13	IEEE	Gallo, P., Pngnumkul, S., Nguyen, U.Q.	BlockSee: Blockchain for IoT Video Surveillance in Smart Cities	IEEE International Conference on Environment and Electrical Engineering	1	2018	pp. 1-6	Smart city surveillance needs ranging from sensor technologies to video monitoring require active, continuous data analysis; however, malicious attacks could lead to misappropriation and unauthorised use.	Blockchain video surveillance system provides validation and immutability for camera settings and surveillance videos, ensuring that only authorised users gain access to the feeds. Smart contracts and tokens restrict unauthorised access, whilst user profiles are validated and confirmed before access is granted. Heterogeneous network support.
14	IEEE	Fayad, A., Hammi, B., Khatoun, R.	An Adaptive Authentication and Authorization Scheme for IoT's Gateways: A Blockchain Based Approach	IEEE Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC)	1	2018	pp. 1-7	In spite of the critical role of authentication and authorisation in securing the IoT, most deployment systems employ separate methods to achieve both interdependent outcomes. An adaptive, combinative approach is needed to increase efficiency and network fidelity.	By creating a heterogeneous solution, any methods and parameters for authentication and authorisation can be used, allowing users to add in a new device through a lightweight initialization process. Whilst optimisation is needed to reduce the time to find the block on the blockchain and cost considerations must be taken into account, then the flexible authentication can exceed efficiencies of existing certificate-based authentication measures.

#	Database	Authors	Title	Journal	Vol (No)	Year of Publication	Pages	Overview	Findings
15	IEEE	Bruneo, D., Chillari, S., Distefano, S., Giacobbe, M., Minnolo, A.L. et al.	Building a Smart City Service Platform in Messina with the #SmartMe Project	IEEE 32nd International Conference on WAINA	1	2018	pp. 343-348	Definition of integrated IoT nodes into smart city framework is a critical antecedent to a more efficient, more interconnected smart urban solution. Ecosystem of infrastructure that requires a management core capable of resolving the cross-device communications	By developing the Stack4Things framework, a cloud-oriented, horizontal solution which offers IoT object virtualisation, customisation, and orchestration is presented that leverages fog-based orchestration to connect IoT ensembles. Tunable granularity via blockchain authentication allows both control and open access across multiple smart solutions via a central software-based interface
16	IEEE	Kravitz, D.W.	Transaction Immutability and Reputation Traceability: Blockchain as a Platform for Access Controlled IoT and Human Interactivity	IEEE 15th Annual Conference on PST	1	2017	pp. 3-12	Reputational credibility is a critical antecedent to efficient data exchange and transfer practices. By developing an intermediary middleware solution, cryptographic blockchain controls can be used to reduce the threat of loss and exposure.	By developing a cryptographic protocol that employs blockchain technologies to detect anomalies and to assess dynamically asserted identities at the network edge, then trusted behaviour data can be used to control access. Such data is dependent upon human-IoT interactions that employ an inviter-invitee protocol to maintain consistent communication channels.
17	IEEE	Lazaroiu, C., Roscia, M.	Smart District Through IoT and Blockchain	IEEE 6th International Conference ICRERA	1	2017	pp. 454-461	In order to realise a smart city solution capable of interconnecting automation with authentication, it is critical for smart grid and service solutions to incorporate a strong, immutable security solution. Blockchain creates a centralised solution for integrating multiple proprietary technologies in a single, authenticated system	Smart contracts are essential to recording and executing network transactions. Device activity is recorded independently utilising proprietary software and APIs, but then integrated with a middle layer of blockchain technology that is decentralised and based upon the peer-to-peer network concept. Distributed systems such as power and water can be managed autonomously by a local community by integrating smart meter technologies and smart contract terms and authorisations. The solution allows neighbourhood residents to assume ownership of their technologies, eliminating the need for larger scale service providers.

#	Database	Authors	Title	Journal	Vol (No)	Year of Publication	Pages	Overview	Findings
18	IEEE	Rahman, M.A., Rashid, M.M., Hussain, M.S., Hassanain, E., Alhamid, M.F., Guizani, M.	Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City	IEEE Access	1	2019	pp. 18611-18621.	Due to the complexity of the information processed through the smart city, there is a need for high-speed transaction processing capabilities that integrate blockchain networks with AI and cognitive computing capabilities	Through concurrent transactions and multi-signature digital wallets, transaction summaries can be used to reduce the amount of data processed. Edge devices running full blockchain nodes can employ decentralised messaging services to save IoT sensory data into a decentralised repository. Blockchain clients can process contractual agreements, with a proof of work standard to calculate the hash between the two transacting nodes and verify and commit the payment to the blockchain. System executions such as the opening of a lock can be delayed by permissions written to the smart device, ensuring that the contract is only executed once an appropriate trigger is received.
19	Sage	Qiao, R., Zhu, S., Wang, Q., Qin, J.	Optimization of Dynamic Data Traceability Mechanism in Internet of Things Based on Consortium Blockchain	International Journal of Distributed Sensor Networks	14	2018	pp.1-15	To improve the legitimacy and traceability of dynamic data, a transparency solution is needed that is based upon the whole life-cycle of data records and access. By establishing a secure key, encrypting data, and securely transmitting via blockchain nodes, dynamic traceability of the IoT can be realized.	The blockchain consensus mechanism provides a means of dynamic data monitoring and protection. Traditional security measures are centralised and fail to address the system vulnerabilities and insider attacks that may manifest at any given time. Dynamic data security offers a decentralised framework for IoT, establishing dynamic data blocks based upon multiple, decentralised nodes.

#	Database	Authors	Title	Journal	Vol (No)	Year of Publication	Pages	Overview	Findings
20	Sage	He, Q., Xu, Y., Liu, Z., He, J., Sun, Y., Zhang, R.	A Privacy-Preserving Internet of Things Device Management Scheme Based on Blockchain	International Journal of Distributed Sensor Networks	14	2018	pp.1-12	Managing access control policies or permissions can protect user resources and ensure user-driven, transparent access to resources in the IoT. By combining the blockchain with this control module, smart contracts can be used to automatically execute an agreed upon contract through a code programme. Users can retain their rights to audit and manage resources.	A privacy-preserving, IoT device management standard based upon the blockchain allows information sharing across organisations and systems. Stored data is verifiable and non-tampered. Time-bound key management mechanism can automatically revoke user attributes and keys. Non-repudiation is achieved through transaction-based digital signatures on each block. Encryption and fine-grained access control verifies the integrity of the data and prevents unauthorised access.
21	Sage	Hong, H., Hu, B., Sun, Z.	Toward Secure and Accountable Data Transmission in Narrow Band Internet of Things Based on Blockchain	International Journal of Distributed Sensor Networks	15(4)	2019	pp.1-10	Narrow-band IoT provides a wide-coverage area with low-energy consumption, massive connections, and inexpensive costs. By applying to smart city environments in the form of smart meters or asset trackers, NB-IoT is able to reconcile data from multiple sources and allow applications to make decisions about effective responses. Blockchain is needed to reduce the potential for double spending or inefficient, expectation-weighted decision-making.	Blockchain provides the middle transport layer of information processing from IoT-based nodes, sharing data with applications localised in the Cloud via authenticated transmissions. Identity authentication is based upon public key-cryptography and allows for lifetime data accountability allowing the system to detect any anomalies in real-time. Real-time status can be tracked and shared via the application, with timestamp authentication preserving the auditability of IoT readings and interpretations. Asymmetric key operations can be reduced after the initial authentication process, thereby reducing the computational demands on the system and basing future exchanges on symmetric keys and secret key negotiations.

#	Database	Authors	Title	Journal	Vol (No)	Year of Publication	Pages	Overview	Findings
22	Sage	Singh, S., Ra, I.H., Meng, W., Kauer, M., Cho, G.H.	SH-BlockCC: A Secure and Efficient Internet of Things Smart Home Architecture Based on Cloud Computing and Blockchain Technology	International Journal of Distributed Sensor Networks	15(4)	2019	pp.1-10	Layer-divided interconnected smart solution that is based upon efficiency, scalability, and availability. IoT-based devices form the smart home layer, blockchain offers decentralised cloud-based storage with a shared key for individual users or households. Permissions are either supported or rejected based upon administrative instructions and permissions.	Data packets are stored in the cloud according to a FIFO standard, allowing service providers to access the data efficiently and connecting the IoT nodes via a single central middleware layer of cloud-based blockchain. For any transaction, genesis transaction is verified by the overlay block managers and the signature of the transaction participants is validated. Sidechain networks can be formed to group IoT devices used for various cases. Cloud layer managed via third-party organisations to reduce environmental impact and maintain carbon-efficient cloud operation. Algorithmic-based service provision validated through blockchain register.
23	WoS	Biswas, K., Muthukkumarasamy, V.	Securing Smart Cities Using Blockchain Technology	IEEE International Conference on High Performance Computing and Communications	1	2016	pp. 1392-1393	The heterogeneity of resource-constrained devices creates vulnerabilities that can threaten the stability and reliability of the IoT infrastructure for Smart City applications. A revised security framework based upon blockchain technologies is needed to improve the overall security of the IoT	The proposed security framework includes four layered elements including the physical layer, the communication layer, the database layer, and the interface layer. Acknowledging the lack of a single standard for the IoT technologies (physical layer), the researchers propose a blockchain-supported database layer that is decentralised and maintains the transaction register capable of negotiating the smart contracts used for the smart city actions and trans-device negotiations.
24	WoS	Ren, Q., Man, K.L., Li, M., Gao, B.	Using Blockchain to Enhance and Optimize IoT-Based Intelligent Traffic System	IEEE International Conference on Platform Technology and Service (PlatCon)	1	2019	pp. 1-4	Blockchain has the potential to function as a decentralised technology that can be applied to an intelligent traffic system to allow vehicles to jointly collaborate without sending and receiving information from a central computing node. P2P data transmission allows individual vehicles to communication with other nodes and the information transmitted is then verified by the end-point nodes to approve lane acquisition. Based upon a consensus agreed upon smart contract.	By applying rights-based logic to the concept of intelligent traffic routing, lane property rights can be negotiated independently between vehicles operating smart IoT technologies. Through decentralised authentication, rights are requested and transferred autonomously via blockchain technologies that connect individual vehicles to the larger blockchain network via mesh, distributed technologies. Due to information throughput, network resources could be severely limited without an improved, decentralised architecture.

#	Database	Authors	Title	Journal	Vol (No)	Year of Publication	Pages	Overview	Findings
25	WoS	Zorzo, A.F., Nunes, H.C., Lunardi, R.C., Michelin, R.A., Kanhere, S.S.	Dependable IoT Using Blockchain-Based Technology	IEEE Eighth Latin American Symposium on Dependable Computing (LADC)	1	2018	pp. 1-9	To address the power and memory limitations of the IoT, there is a need for a layer-based model of blockchain integration that is capable of spanning multiple network protocols. Blockchain as a service maintains the full nodes outside of the IoT, whilst still providing device access to the third-party infrastructure.	There are three P2P architecture possibilities including distributed, gateway-based, and blockchain as a service. The hierarchical, gateway-based solution utilises supernodes to maintain a blockchain with individual device information, reducing traffic and decreasing device vulnerability. The BaaS protocol separates the nodes controlling the blockchain from the IoT, delegating trust on the basis of third-party guideines and API encryption. Smart grid applications and smart contracts require greater security and transparent authentication; however, without a standard blockchain framework for the IoT, proprietary solutions remain vulnerable to security threats. There is a need for improved analysis of the consensus layer and exploration of APIs for the application layer.
26	WoS	Paul, R., Baidya, P., Sau, S., Maity, K., Maity, S., Mandal, S.B.	IoT Based Secure Smart City Architecture Using Blockchain	IEEE 2nd International Conference on Data Science and Business Analytics	1	2018	pp. 215-220	The memory footprint for standard security protocols creates challenges for the IoT that requires lightweight computing to preserve its basic cryptographic properties. The blockchain could provide an efficient architectural solution capable of achieving a standard of basic requirements such as authenticity, integrity, confidentiality, availability, and non-repudiation.	The blockchain solution must be applied at strategic nodes within the IoT architecture to reduce computing and power consumption. By sharing symmetric keys between multiple nodes and then introducing a light weight key exchange algorithm, only one node needs to engage in higher processing functions. High processing nodes serve as validation mechanisms (e.g. admin), creating a canopy network that transfers blockchain storage to the admin system, whilst transferring access control to the high processing node. To meet the challenges of the IoT, a new security standard is needed that is light weight and capable of meeting the needs of rapid, high-reliability authentication. The blockchain provides this intermediary solution.