Postprint of: Dar M. A., Askar A., Bhat S. A., Blockchain based Secure Data Exchange between Cloud Networks and Smart Hand-held Devices for use in Smart Cities, 2022 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Jeju Island, Korea, Republic of, 21-24.02.2022, pp. 457-460, https://dx.doi.org/10.1109/ICAIIC54071.2022.9722646

Blockchain based Secure Data Exchange between Cloud Networks and Smart Hand-held Devices for use in Smart Cities

Muneer Ahmad Dar[†], Aadil Askar[‡] and Sameer Ahmad Bhat[§,✠]

[†]National Institute of Electronics and Information Technology (NIELIT), Jammu & Kashmir,India.
[‡]Dept. of Self Development Skills, King Saud University, Riyadh, Saudi Arabia.
[§]Gulf University for Science and Technology (GUST), Mehref, Kuwait.
✠ Gdansk University of Technology, Pomerania Gdansk, Republic of Poland.
Email: muneer@nielit.gov.in, aadil@ksu.edu.sa, bhat.s@gust.edu.kw

***Abstract*—In relation to smart city planning and management, processing huge amounts of generated data and execution of non-lightweight cryptographic algorithms on resource constraint devices at disposal, is the primary focus of researchers today. To enable secure exchange of data between cloud networks and mobile devices, in particular smart hand held devices, this paper presents Blockchain based approach that disperses a public/free key to save it on a block within a Blockchain. The proposed system generates public-private key pair to encrypt data digitally to allow data communication. This empowers communication devices to encipher data using keys stored in the Blockchain i.e. the public key. Generated cipher text can be decrypted/deciphered only with the respective private keys, meaning that only the communicating devices can obtain their own plain text in a data exchange process. Smart mobile employed in smart city can then encipher the data using the keys and store them on the cloud. The proposed system is able to decrease the number of overheads that relate to key generation, key delivery and key storage whilst providing solutions for data processing, information exchange and data over-collection, respectively. Thus, the study proposes a robust and secure solution to exchange keys and secure data communication based on Blockchain technology.**

***Index Terms*—Blockchain, Cryptographic Algorithms, Digital Signature, Digital Signatures, Smart City.**

I. Introduction

With the inflation in score of population moving towards cities, the usage of technological solutions is of paramount priority of various governments across the world. The smart cities are coming up, which provides every kind of facility to its citizens. The technological solutions, be it digital transactions, smart healthcare, smart education and lot more, the data over-collection and securing the private/ confidential data of citizens is of paramount importance. The EU group which looks for the information security of smart cities has come up with various protection measures that must be implemented in a smart city [1]. They recommend encryption of data that is transmitted, incorporation of intrusion detection system, Installation of VPNs, installation of alarms and surveillance and many other measures. Thus the user in a smart city is always on radar of intruders who always try to steal their critical data. With the introduction of Blockchain technology, many issues pertaining to the smart city can be resolved. The paramount advantage of Blockchain is its scattered way of authentication and use of encryption that makes use of both public and private keys. With no centralized power, the Blockchain provides a vital security for the financial transactions. The distributed ledger concept of Blockchain has raised bitcoin in the form of digital crypto currency which is procured by millions. Thus the advantage of Blockchain can be exploited for the proficient, flexible and above all secure implementation of smart cities. Various countries have already used the Blockchain technology for the betterment of their citizens. Table I provides the list of initiatives [2].

TABLE I
Blockchain initiatives by various countries

Country Name	Blockchain Applied On
Sweden	The transactions related to real estate are maintained using Blockchain
Estonia	Patients Medical record is maintained using Blockchain
Ghana	The property documents are maintained using Blockchain
Russia	Shareholders transactions and secure transactions are maintained using Blockchain
Korea	Banking
Singapore	Blockchain based trading
Dubai	City Logistics, Paperless government System

II. Review of BlockChain Technology

The technique used by bitcoin introduced by Nakamoto is the most widely used append only distributed database for crypto-currency [4]. As demonstrated in the Fig 1, the Blockchain comprises of blocks. Each block has the following data members with the description as in Tabel II under:

The order of the Blockchain is controlled by the preceding blocks' hash value. The main advantages of Blockchain are distinguishability, directness and understanding, decentralized, verifiable, and many more. Transactions made between nodes i.e. users inside the Blockchain network will be obtained by certain nodes with the consensus protocol Proof-of-Work (PoW) as an illustration as in miners. Then the nodes compete for possibilities for generating the new block by listing the

TABLE II
BLOCKCHAIN BLOCK STRUCTURE.

Block Data	Description
Version Number	For keeping track of modifications and updates that have occurred during the protocol's lifetime.
Previous Block Hash	Hash of preceding block
Merkle Root	It provides a unified hash value that allows you to validate anything that is contained within that block.
Time Stamp	A sequence of signs or encoded information that can be accurate to a fraction of a sec, if a specific event occurred, normally with a date and time of the day.
Difficulty Number	The difficulty of mining a block, or the difficulty of finding a hash below a specified goal, is a measure of how tough it is to mine a Bitcoin block.
Random Number	The generation of random numbers enables us to generate private keys— which are a component of your key pair.
Transaction Data	As soon as a transaction is entered in the Blockchain, its data, including as the price, the product, and control, are recorded and validated across all nodes within seconds, allowing it to be settled across the whole network.

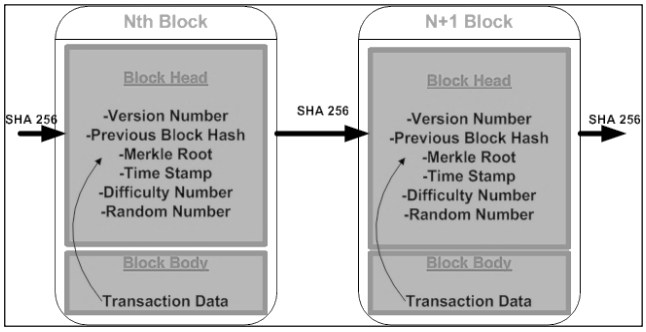

Fig. 1. Blockchain Structure.

previous block head hash values by increasing their parent block head random numbers. by growing the number of parent block Heads.

The miner will only construct a totally new block including transaction completed since the previous block is formed, depending on the difficulty number, if the hash value fulfills the criteria of the challenge number (ie, a system parameter for regulating block generation rate for Blockchain). The block is then sent to all network participants in the Blockchain system via the new block. Once the hash value confirms the supplied challenging number, all nodes will include the new block and link the new Blockchain to the local Blockchain sync to the global Blockchain. In addition, a Digital Signature Algorithm (DSA) is employed for communications security, and a Merkle Hash Tree for transaction information protection purposes is utilized. The Blockchain is therefore ready to offer us with a distributed, reliable and trustworthy consensus environment in the longer term.

A digital signature is a mathematical technique that confirms the validity of digital messages or documents throughout the communications process [5]. For a legitimate digital signal, the recipient is certain that a recognized and verified sender has generated the message. In the meanwhile, neither the sender nor the receiver can deem the transmission of the communication, nor the transmission of the message. In other words, the receiver can immediately determine whether the message has been altered or deleted during transmission. The proposed technique uses a secure communications mechanism based on ECDSA's cryptographic algorithm in order to ensure data security throughout communication. ECDSA, but at the other hand, is a kind of DSA combining the DSA with the Cryptography Elliptical Curves, which Neal Koblitz presented [6] and Victor Miller offered [7], and it is both hybrid.

A Merkle Hash Tree [8] is a kind of binary tree constructed as building pieces with hash values. As shown in Fig 2: The information included within a leaf node is the hash value value of a business, but it is the hash of the mixture of the child nodes of a leaf node in which it is recorded. This technique employs the safe SHA256 hash algorithm [9], an irregular computational process, and a cryptographic scheme with pseudo-randomness. It is used to secure transactions on the Blockchain of the scheme. As immediately as the load varies little, its output will thus be very changeable. This allows users to check if the processes or the data in the block body remain valid or not on the Blockchain network, i.e. nodes, due to this feature. Consider an example to better grasp what this means: Any change in the block contents of a block may be detected by MHT by considering each operation's has value as new point in the MHT.

III. EXISTING RESEARCH

In order to investigate and apply the technology Blockchain, Bitcoin's success led intellectuals to explore several fields, such as Smart Contracts [11], Finance [9], Management of HR [14], Supply Chain [15] and Internet of Things [11], [17]. In [11], for example, the authors stated that the Blockchain technology should be lightly installed for a smart IoT dwelling. Multiple IoT equipment is connected to one single network in every residence (e.g. smartphones, PCs and sensors). Under Bitcoin's success scholars have been driven to research and utilize Blockchain technology in many fields, including Smart Agreement [11] and Finance [4], the supply chain [15], and human resources management [14], and [11], [17]. In [11], for example, the authors suggested that the Blockchain technology be light installed in the intelligent IoT dwelling. Several IoT users are interconnected to the very same network in each home, such as smart devices like phones, personal PCs and sensors to collect data. The suggested model provides for only approved users to access and manage home devices and safeguarded and unable to modify the messages received by authorized users by the malicious users. The creators of [12] have established a new spread- out information managing policy that enables users to monitor their records so that third-party infringements can be avoided. The platform mixes cryptocurrency and off-Blockchain stores to build a framework for private data administration.

Since, the Blockchain acknowledges the users as their proprietors; therefore users are not needed to have confidence

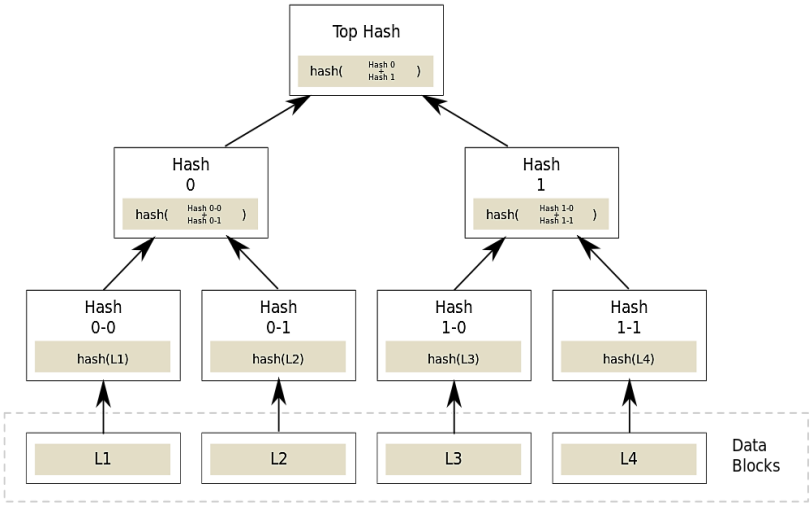

Fig. 2. Merkle Hash Tree [10]

in any third party. The authors have expanded [12] with the addition of a new approach, dubbed a Proof of Credibility Score (PCS), to improve the cryption algorithm for mining procedures. The suggested PCS technique uses the interconnection between nodes to determine the credibility score differently from [12] where the trust value of the node is gathered for how many beneficial acts the Node has taken. The numerical findings have then shown that the security measures can be upgraded with the proposed scheme Blockchain of credibility.The scalability of the Blockchain is a major difficulty as the application grows. The authors in [18] offered to tackle this problem with a BigchainDB system in NoSQL database format. The Blockchain pipeline is used to scale the system to the distributed database by adding Blockchain features. In MC, transactions at mobile nodes should be taken into account to enable the direct interchange and sharing of peer-tope data. This is particularly critical if connecting devices have really no internet connection. Presently some Android applications, such as Easy-Miner [12] and Scrypt-Miner PRO and LTC, are developing for mining on Mobile equipments for the Bitcoin relevance. They are still demo versions, though, and have not yet finished. Especially because Bitcoin applications are employed for crypto-currency applications alone, there are still a lack of the platform for broader Blockchain activities.

IV. Proposed Architecture

A digital signature is an authentication method. It consists of a public key pair and digital certificate, to authenticate or verify either recipient's or sender's identity. Elliptic curve cryptography generates smaller keys compared to digital signing algorithms that generate average length keys. Elliptic curve cryptography implements the algebraic structure of elliptic curves over finite fields, and it is a public key cryptography. Elliptic curve cryptography helps to generate definite or random sequences, such as pseudo-random numbers, digital signatures, and more.

A. Elliptic Curve Digital Signature Algorithm (ECDSA)

Elliptic Curve Digital Signature Algorithm (ECDSA) is based on public key cryptography (PKC). It is a Digital Signature Algorithm (DSA), uses key derrived from Elliptic Curve Cryptography (ECC). ECDSA signed certificates are used to encrypt connection requests of an HTTPS website that informs about the applied encryption by an image of a physical padlock displayed by the browser. ECDSA could be also found implemented in security systems, such as secure messaging apps, including Bitcoin security. While serving at Transport Layer Security (TLS), ECDSA encrypts connection requests between web browsers and a web application.

Compared to another popular algorithm- RSA, ECDSA offers high level security with short key lengths, is the primary feature of ECDSA. Apparently, ECDSA executes at low computational power requirements compared to RSAm, which is a less secure competing equation. Elliptic Curve Digital Signature Algorithm (ECDSA) is an elliptic curve-based encryption and digital signature scheme. ECDSA can be used to apply digital signature, however more efficiently. ECDSA bases on an elliptic curve, and the curve is analyzed for a point. After analzying, a point is chosen on the curve, and then next step is to multipy the selected point by another number. This just creates a new point on the same curve. As a result of multiplication, the key lies in the fact that finding the the new point on the curve is really a complex and hard task. Even if the original point is known, the new point cannot be found. This complexity of ECDSA highlights it's robustness against methods used to decrypt the data exchanged during the communication processes.

The proposed methodology allows a member in the suggested technique to join, relocate and consider leaving any subset. The proposed scheme, like Bitcoin, Ethereum applications sets up key encrypted duos without centralized authority for the Elliptic Curve Digital Signature Algorithm (ECDSA) - based data exchange. Unlike the Bitcoin Blockchain, which takes about an hour to make a transaction in Bitcoin (to actu-

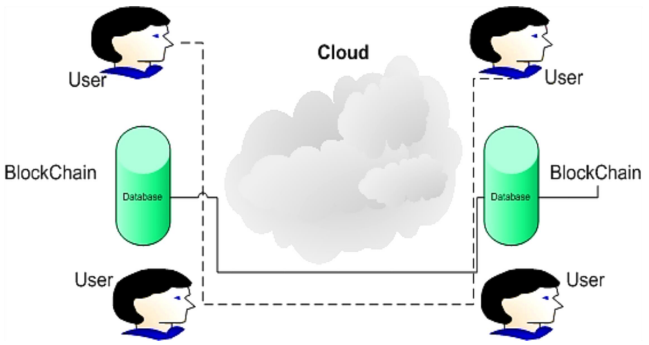

Fig. 3. Proposed Architecture.

ally create 6 blocks), Blockchain inside the scheme proposed adds blocks directly after they are received. And the proposed solution may prove to be significantly effective for the mobile devices used in the proposed scheme.

Fig. 3 shows a straightforward operating process of our proposed model. For the Blockchain, the open or public keys of all members eligible to establish a secure communication will be stored on a Cloud network. Any member may use an open/public key stored by other members on the Blockchain of the associated sub-network so as to connect with the other group members. A mobile device closer to a cloud may find easy access to a number of the available resources on Cloud, and conversely devices faraway from Cloud service may have limited access. As more and more mobile devices connect to nearest available cloud service, the availability of services needs to be ensured.. However, the services need to qualify and fulfill the increased demand for computational resources, communication channels bandwidth, and large storage resources.

V. Conclusion

Currently available mobile devices are often categorized under resources constraint devices, as it is hard to execute computationally complex algorithms on such hardware platforms. As millions of citizens show trends to maintain social connectedness in a smart city, there is a need to adopt lightweight security architectures. Not only would such architectures protect the privacy of users, but also could run or execute at a low computational cost. Therefore, this study provides advantages of using technological innovations in Blockchain and proposes model for secure data exchange between the mobile devices used in smart cities. The model proposed shows a conceptual model and gives an insight of how implementing Blockchain can decrease the computational complexity of the algorithms to allow them run on hardware constraint devices. In our future studies, we plan to test the proposed system on the available different resource restricted platforms so as to investigate in details the hardware and software complexities posed to processes that implement Blockchain technology.

References

[1] Smart Cities Cyber Security Management, Consultancy Report. Available at https://securingsmartcities.org/wp-content/uploads/2017/09/SSC-SCCCM.pdf

[2] PWC – PWC's Global Blockchain Survey, 2018. Available at https://www.pwccn.com/en/research-and-insights/publications/global-Blockchainsurvey-2018/global-Blockchain-survey-2018-report.pdf

[3] Gupta, S.: 'Using Blockchains in smart cities', Meetings of The Mind, 2018. Available at https://meetingoftheminds.org/using-Blockchain-in-smartcities-29319

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", https://bitcoin.org/bitcoin.pdf , 2008.

[5] Wikipedia contributors, "Digital signature — Wikipedia, the free encyclopedia," https://en.wikipedia.org/w/index.php?title=Digital signature&oldid=876680165, 2019, [Online; accessed 08-September-2021].

[6] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of computation,vol. 48, no. 177, pp. 203–209, 1987.

[7] V. S. Miller, "Use of elliptic curves in cryptography," in Conference on the theory and application of cryptographic techniques. Springer, 1985, pp. 417–426.

[8] R. C. Merkle, "A digital signature based on a conventional encryption function," in Conference on the theory and application of cryptographic techniques. Springer, 1987, pp. 369–378.

[9] N. T. Courtois, M. Grajek, and R. Naik, "Optimizing sha256 in bitcoin mining," in International Conference on Cryptography and Security Systems. Springer, 2014, pp. 131–144.

[10] Merkle Tree, Wikipedia, the free encyclopedia https://en.wikipedia.org/wiki/Merkle˙tree [Online; accessed 08-September-2021].

[11] A. Dorri, et al., "Blockchain for IoT security and privacy: The case study of a smart home," in IEEE International Conference on Pervasive Computing and Communications Workshops, pp.618-623, Hawaii, USA, Mar. 2017.

[12] G. Zyskind, O. Nathan, and A.S. Pentland, "Decentralizing privacy: Using Blockchain to protect personal data," in IEEE Security and Privacy Workshops, pp. 180-184, San Jose, USA,May 2015.

[13] D. Fu and L. Fang, "Blockchain-based trusted computing in social network," in IEEE International Conference on Computer and Communications, pp. 19-22, Chengdu, China, Oct. 2016.

[14] X. Wang, L. Feng, H. Zhang, C. Lyu, L. Wang, and Y.You, "Human resource information management model based

[15] on Blockchain technology," in IEEE Symposium on Service-Oriented System Engineering, pp. 168-173, San Francisco, USA,Apr. 2017.

[16] H. M. Kim and M.Laskowski, "Towards an ontology-driven Blockchain design for supply chain provenance," Open-Access Online Library, Aug. 2016.

[17] Global M-commerce Market 2016-2020. Technavio's Report.

[18] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockChain for IoT," in IEEE/ACM Second International Con-ference on Internet-of-Things Design and Implementation, pp. 173-178, Pittsburgh, USA, Apr. 2017.

[19] T. McConaghy, R. Marques, A. Mller, D. De Jonghe, T.McConaghy, T, G. McMullen, and A. Granzotto, "BigchainDB:a scalable Blockchain database," White Paper, BigChainDB,2016.

[20] M. A. Dar, S. Nisar Bukhari and U. I. Khan, "Evaluation of Security and Privacy of Smartphone Users," 2018 Fourth International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, 2018, pp. 1-4, doi: 10.1109/AEEICB.2018.8480914.

[21] Dar, Muneer & Khan, Ummer & Bukhari, Syed. (2019). Lightweight Session Key Establishment for Android Platform Using ECC. 10.1007/978-981-13-3122-0˙33.

[22] M. A. Dar and J. Parvez, "Security Enhancement in Android using Ellipic Curve Cryptography," Int. J. Secur. its Appl., vol. 11, no. 6, pp. 27–34, 2017.