# Block Chain for Financial Application using IOT

**Dr. B. Subba Reddy[1], P. Sai Hamshika[2], S. Aishwarya[2], V. Ashritha[2]**

[1]Professor and Head of the Department, [2]UG Scholar, [1,2]Department of Information Technology

[1,2]Malla Reddy Engineering College for Women (A), Maisammaguda, Medchal, Telangana

**ABSTRACT**

The Internet of Things (IoT) has become a popular computing technology paradigm. It is increasingly being utilized to facilitate human life processes through a variety of applications, including smart healthcare, smart grids, smart finance, and smart cities. Scalability, interoperability, security, and privacy, as well as trustworthiness, are all issues that IoT applications face. Blockchain solutions have recently been created to help overcome these difficulties. Therefore, this paper describes the concept of providing security for payment processing involved in IOT devices and their service usage by applying Blockchain technology. Blockchain is a secured distributed cryptographic hashing technique which maintains transaction in a transparent and unalterable format. It maintains block of chained transaction and keeps on validating old and new transaction and if old hash matched then only transaction will be consider as successfully verified. All users' transaction will be privacy protected and this same technique applied in this project to secure payment process happen between users and company services. All data in this project saved inside Blockchain and authentication and privacy will be performed by using DSA (digital signature algorithm) and SHA hashing technique.

**Keywords:** Internet of Things, DSA (digital signature algorithm), Service providers, service users.

## 1. INTRODUCTION

In recent years, the Internet of Things (IoT) has emerged as a new and significant technology of the computing paradigm. The market demand for smart devices is projected to be worth trillions of pounds annually soon, and almost all businesses will use some sort of technology to improve their financial operations [1]. However, as critical applications of the IoT rapidly increase (for instance, smart healthcare, smart grids, smart cities, and smart finance), they face numerous security and privacy challenges. In fact, in October 2016, the US internet was brought down by cyberattacks. These attacks targeted the servers of Dyn, a corporation that controls and operates the largest infrastructure of the internet's domain-name system (DNS). The company estimated that attacks were launched from tens of millions of IP addresses and that attacks have become larger. These attacks were due to malicious software called Mirai that infected web traffic obtained from IoT devices, including home routers, baby monitors, webcams, and video recorders for digital use. The Mirai attacks had a much wider scope than the most distributed denial of service (DDoS) attacks that have historically been able to reach more than 100,000 malicious endpoints, according to Dyn's estimate [2].

As IoT attacks become more sophisticated, the threat vector grows. Therefore, blockchain technology plays a critical role in addressing security challenges and the issues involved in using the IoT [3,4]. A blockchain system involves a type of large database leveraged with several new computational technologies and protocols. Blockchain stores data on servers that commonly consist of huge arrays of computers with the storage space and computing power required to support multiple users simultaneously accessing the database [5]. The first version of the blockchain, known as Bitcoin, was invented in 2009 by Satoshi Nakamoto [6]. Bitcoin was set up as a stable, decentralized global

currency, which could be used as an exchange for financial transactions. The blockchain concept uses a decentralized public ledger designed to permanently record transactions without any need for authorization from a third party [6].

Vitalik Buterin created the first cryptocurrency 'smart contract' in 2013. This system enables citizens to directly share value without intermediaries. Further, a smart contract's ability to enforce or self-execute contractual provisions is one of its most important aspects. Furthermore, smart contracts have considerably assisted the growth of blockchain. The combination of automatically executed contracts in a trusted environment with no centralized control has the potential to revolutionize the way business is conducted today. In addition, smart contracts and improving trust in the IoT's mechanisms while lowering expenses, whereas data security in the IoT is ensured by time series data and encryption. The blockchain network collects a lot of information and uses the right techniques to secure data at a higher level [3]. Smart contracts are increasingly being used by businesses to minimize costs and improve efficiency [7].

Blockchain technologies, such as distributed ledger technology, have provided benefits to organizations requiring high levels of trust in the execution of their core transactions. In fact, the blockchain is a distributed ledger technology that differs from standard distributed ledger technology in terms of storage mechanisms and data types. As a result, blockchain technology realizes privacy and security requirements, ensuring the validity and security of the data. Besides, record sets are a new thing in a ledger that preserves connected devices. In the blockchain, there is no such thing as a master or slave; each device has equal authority and a copy of the entire chain. A private or public blockchain can be used to implement a blockchain ledger. The use of a general ledger has enabled the benefits of blockchain to be extended beyond financial services to all aspects of daily life, and blockchain technologies have recently been explored in areas such as healthcare, transport, and energy. Companies' blockchain market value could hit $20.3 billion by 2025 from $4.6 billion in 2018, with finance and manufacturing dominating the blockchain market [8].

Consensus mechanisms are required for the integrity of the information stored in blockchains as well as defense against double attacks, and they are thus an essential component of blockchain technology. The goal is to create consensus in a dispersed network with no central authorities and participants who may or may not trust one another. Therefore, multiple consensus processes are possible with blockchain, and data privacy is achieved by cryptography and segmentation [3].

Asymmetric encryption algorithms are used to encrypt data on the blockchain. In blockchains, this asymmetric encryption is used for data encryption and digital signatures. Data encryption in the blockchain ensures transaction data security and decreases the risk of data loss or falsification. The transaction data is sent over the network and digitally signed to show the signatory's identity and whether the transaction has been identified. It is not essential to reveal the genuine identity of the node associated with the participant in the blockchain system. This feature is problematic because it indirectly aids criminal operations such as money laundering, but it does safeguard the participants' privacy and security.

Blockchain technology's decentralization and data encryption make it ideal for developing distributed security systems. IoT security is enhanced by blockchain. Electronics 2022, 11, 630 3 of 35 blockchain's decentralization creates a safe environment for the IoT and creates a fully distributed system [9]. Blockchain technologies are used in multiple situations in many fields involving IoT applications such as data storage, management of identities, timestamps, sensors, supply chain management and applications to daily life, including smart healthcare and smart homes. The use of blockchain technologies is a promising solution for several problems in IoT applications, thus attracting the attention of both academia and industry aimed at developing and integrating blockchain technologies into IoT applications [10].

## 2. LITERATURE SURVEY

Since the establishment of Bitcoin in 2009, one thing that has raised hopes of many is the technology running under the hood, Blockchain. 9 years on and blockchain has made its way into an array of other technologies with Financial and IOT being at the forefront of this development. The blockchain is a distributed ledger which helps in facilitating and verifying transactions between mutually distrusted parties without the need of central authority. Ethereum, the world's largest Blockchain has a market cap of 21 billion $ and 333.1 million confirmed transactions [1] (As of writing this paper). Furthermore, it has more than 4.5 million unique addresses [2] (As of Writing this paper). With 69 % of banks experimenting with blockchain, it shows how important this technology is to the financial world [3].

The Internet of Things (IoT) and Blockchain are two topics which are causing a great deal of exposure and elation, not just in the technical environment but in the far-ranging business world, too. However, the idea that putting them together could lead to something even greater than the sum of its individual parts is something which is starting to gain attention. Put them together and in theory, you have an empirical, secure and immutable method of recording data processed by "smart" devices in the IoT. Simplified business workings, better customer experience and cost efficiencies are made possible due to blockchain based IoT solutions. It is often said that IoT needs Blockchain and vice-versa. Four ways IoT can exploit blockchain technology:

- Trust building.
- Cost reduction.
- Accelerated data exchanges.
- Scaled security.

But with great potential comes great risks. Attacks on Crypto currencies are an all-time high [4][5] and it is due to surpass all other types of cyber-attacks [6]. This is the case with public Blockchain where computing power is very high, imagine hackers gaining access to some private organizations one and stealing valuable information. The infamous DAO attack which costs 60 million USD and forced developers to Hard Fork Ethereum is a prime example of a looming threat to Blockchain and crypto currencies [7]. Miners are devising new ways to rake in more profits by mining blocks with easier mathematical complexities; one such method is presented in [8]. With Smart contracts taking much of space on Ethereum Blockchain and more than 99 percent of it hasn't been executed less than 100 times, it is headed towards a major scalability problem [9].

### Blockchain in Financial Applications

*Suhaliana bt Abd Halim, Norul & Rahman, Md Arafatur & Azad, Saiful & Kabir, Muhammad Nomani. (2018). Blockchain Security Hole: Issues and Solutions. 739-746.*

In this paper, the author has started with an overview of blockchain technology and later in the paper described some of the issues but, the author missed out on some key issues. In addition to this, the description of each issue is obscure with negligible references. Further, in the paper, he has proposed solutions to the problems presented in the paper which are as follows

Pegged side chain: It is the concept of integrating two blockchains by peg mechanism to facilitate bidirectional transfer between the chains. This solution is fundamentally for scalability and privacy problem, one of which isn't addressed in this paper at all. When we are integrating two blockchains, fundamental problems more or less remain the same. By adopting this approach developers have added a layer of complexity (SPV) in the already complex system which will further hinder the performance of blockchain. Furthermore, integrating two blockchain also mean that there will be more than one asset at disposal, so one will have to significantly change the architecture to identify any malicious transactions.

Two-factor authentication: This solution suggests that private keys should be broken down in parts and stored in different devices. It addresses the problem of transaction malleability and privacy. It can be very useful if implemented. For example, a person stores one part of the key in his/her mobile phone and another part in their wallets. What if the person mobile is hacked or cloned? Then the hacker will have part of user's private key and time has proven that wallets can be hacked too. In this way, two-factor authentication can be easily circumvented.

Proposed solution: In the proposed solution the author has combined two solutions and tried to create a more secure blockchain. The problem here is that it does more harm than good. Firstly, it will only increase the complexity of Blockchain as pegged blockchain is introduced furthermore, there is a need for additional software to check this authentication. Which will ultimately take a toll on the efficiency of the blockchain? Also, the author hasn't performed any comparative study of his proposed method without which its viability cannot be assessed.

*A. Kaushik, A. Choudhary, C. Ektare, D. Thomas and S. Akram, "Blockchain — Literature survey," 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, 2017, pp. 2145- 2148.*

This paper gives an overview of blockchain technology. It explains what blockchain technology is and what the process of transferring currency through a blockchain is. Furthermore, the author compares decentralization and centralization and states why decentralization is better than its counterpart. Later on, Author has given a gist of attacks like 51% attack, double spending attack, Brute force attack and Finney attack which is another form of double-spending attack. One important thing to note here is that Side channel attacks are discussed here, which is often overlooked but is a cause of serious concern.

Author hasn't provided any solution to the issues presented in the paper. For instance, a concern of wallets is discussed but the methods that can be implemented in order to prevent identity theft aren't discussed at all. Also, the author has missed out on some crucial issues like DDoS attacks etc. In the last section, Different constraints of blockchain like are discussed which are as follows

Hashing: Hashing function is a piece of code which converts data into ciphertext. The author describes all the qualities an algorithm needs to possess, in order to be a good hashing Algorithm.

Digital Signature: It is the process of appending a piece of unique information along the intended file such that the sender is easily identified.

**Blockchain in IoT**

*Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy. arXiv preprint arXiv:1712.02969.*

Security and Privacy is the major concern of IoT devices today. Maybe because of the Massive scale and distributed nature of IoT. This paper presents the solution of concern using lightweight scalable blockchain (LSB). According to the author, the IoT applications and devices suffer from:

- High resource demand for solving the Proof of Work.
- Long latency for transaction confirmation.
- Less flexibility, this is a result of broadcasting transactions and blocks to the whole network.

In LSB, a time-based consensus algorithm approach can be used in place of PoW and PoS. Consensus algorithm is used because it selects a block at random and has higher fault tolerance as compared to the Byzantine fault tolerance system. To increase fault tolerance while selecting block generators, each Overlay Block Manager (OBM) must wait for a random time called waiting-period, before

generating a new block. Since different OBMs have different waiting-period, an OBM may select a new block that was previously created by another OBM that contains transactions of that OBM. This OBM must remove all these transactions that are already stored in the blockchain by the other OBM from its collection. By making OBMs wait for a random time the probability of duplicate blocks that can be generated simultaneously also reduces hence reducing redundancy. The author addressed the following attacks on LSB.

51% vulnerability: The attacker controls over 51% of OBM and tries to hack into the consensus algorithm by generating fake blocks or add more blocks than the number of blocks that are allowed. This attack can be detected during block verification.

*Appending Attack:* Attacker hacks into an OBM and generates blocks with fake transactions. An OBM can detect fake blocks during the verification process.

*https://www.corero.com/blog/870-the-rise-of-iot-botnetthreats-and-ddos-attacks.html*

Due to a large number of devices added daily by the Internet of Things (IoT), business methods and growth are brought about by organizations of all sizes as they are recognizing the importance of IoT. The IoT solutions have exponentially increased in number, creating real challenges, them being, an IoT model that is secure for performing tasks like information storage, communication between devices, processing and sensing. One of the main reasons for security is the DDoS attack [37]. This affected millions. Since blockchain is a public ledger, the users participating can see the blocks and the data stored in these blocks. This is one of the major advantages of blockchain. Since blockchain is not centralized, transaction approval and rules are not set by a single authority. Also, since everyone participating must reach a general agreement to accept transactions, a trust is developed.

## 3. PROPOSED METHODOLOGY

In this work, there are two users called Service Providers and Service users.

- Service providers: this user will register with the application and then login to application to perform activities such as Adding Services with IOT devices and view account balance and subscribe users. User will subscribe to service providers to access their IOT devices data. Sensors will sense data and send to IOT devices and IOT devices will send to Blockchain for storage.
- Service Users: this user will register with application and then login to application to perform activities such as Viewing List of Service Providers, Subscribing to IOT services, View data of sensors and IOT by sending request to Blockchain.

### 3.1. Digital signature

A digital signature is a mathematical scheme for presenting the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a claimed sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity).

Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures.

Digital signatures employ asymmetric cryptography. Asymmetric cryptography, also known as public key cryptography (PKI), uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical (asymmetric). One key in the pair can be shared with everyone; it is called the public key. The other key in the pair is kept

secret; it is called the private key. Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption.In many instances they provide a layer of validation and security to messages sent through a non-secure channel. Digital signatures are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type.

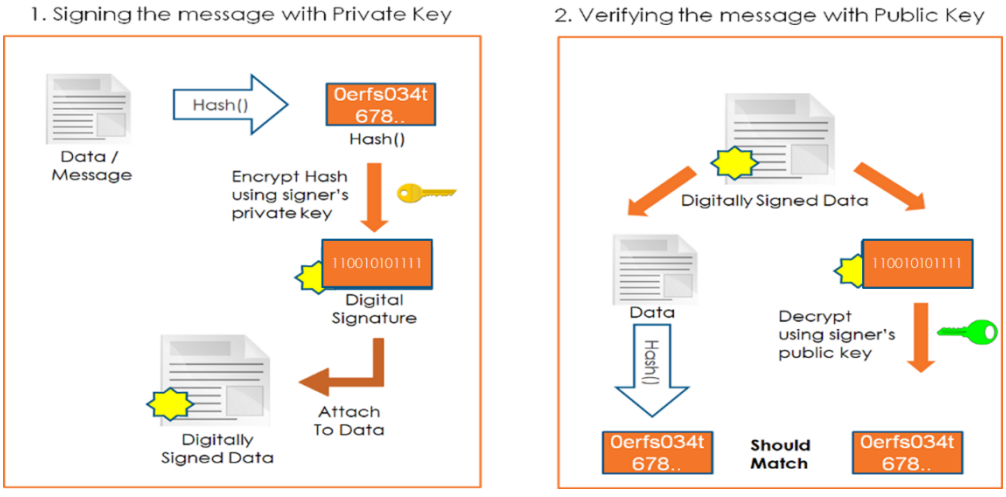
Let's dive into this concept from blockchain perspective with the help of an example

Public key cryptography is a cryptographic system where you have 2 keys — public key (Pu) and a private key (Pr). You give out your public key to the entire world and keep the private key to yourself. e.g., Your Ethereum address is a public key, and your private key is stored either in your browser / mobile / hardware wallet. Consider public key like a bank account number, for someone to send you money (Ether), they just need to know your public (account) address. However, only you can access the funds in your account because you are the only one who knows your private key, say similar to your bank account password.

Public key cryptography has algorithms that let you encrypt, decrypt, sign and verify messages using your pair of keys. Let's explore how these steps flows with an example

*Signing the message with private key:* To create a digital signature, signing software (such as an email program) creates a one-way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The encrypted hash — along with other information, such as the hashing algorithm — is the digital signature. The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves time since hashing is much faster than signing.

*Verifying the message with public key:* This would involve two steps, generate hash of the message and signature decryption. By using the signer's public key, the hash could be de-crypted. If this de-crypted hash matches a second computed hash of the same data, it proves that the data hasn't changed since it was signed. If the two hashes don't match, the data has either been tampered with in some way (integrity) or the signature was created with a private key that doesn't correspond to the public key presented by the signer (authentication)




### 3.2 Practical Applications

- Digital Signatures are used in software programs, such as browsers, which need to establish a secure connection over an insecure network like the internet. Users and systems

need to be certain that a public key is authentic, that it belongs to the person or entity claimed and that it has not been tampered with or replaced by a malicious third party.

- The United States Government Printing Office (GPO) publishes electronic versions of the budget, public and private laws, and congressional bills with digital signatures.
- Digital Signatures can reduce the time to close the contracts that require many parties to validate and sign them. E.g. Mortgage Contracts require number of parties to validate the contract & sign it at different stages of mortgage life cycle. Parties involved — Buyer, Lender, Seller, Attorneys, Real Estate Agents, Title Representatives, Closing Agents With the immutable nature of blockchain, the contract validity can be trusted at any point in time, so that all these parties can sign these contracts at their convenience (no need to be present at the same time)
- Digital Signatures can be used for B2B communications & transactions, that can validate the source & can be sent to only intended party without any middlemen

### 3.3 Digital Signature Algorithm (DSA)

A digital signature (DS) is the detail of an electronic document that is used to identify the person transmitting data. DS makes it possible to ascertain the non-distortion status of information in a document once signed and to check whether or not the signature belongs to the key certificate holder. The detail's value is a result of the cryptographic transformation of information through the use of a private and public key.

DS is treated as a substitute for handwritten signature to the extent permitted by law. From the standpoint of applications, it

- Allows value control in respect to the document being transmitted. Whenever a document gets exposed to a malicious modification, the signature is invalidated since it conforms solely to the initial document status.
- Guarantees protection from falsification. The existing signature algorithms render falsification infeasible in most cases.
- Ensures non-repudiation of origin — any signature is generated using a private key that is known only to its owner, who is, therefore, unable to repudiate his/her signature added to the document.
- The latter factor also enables the authorship of a document to be supported by evidence in the event of a dispute.

### 3.4 DSA

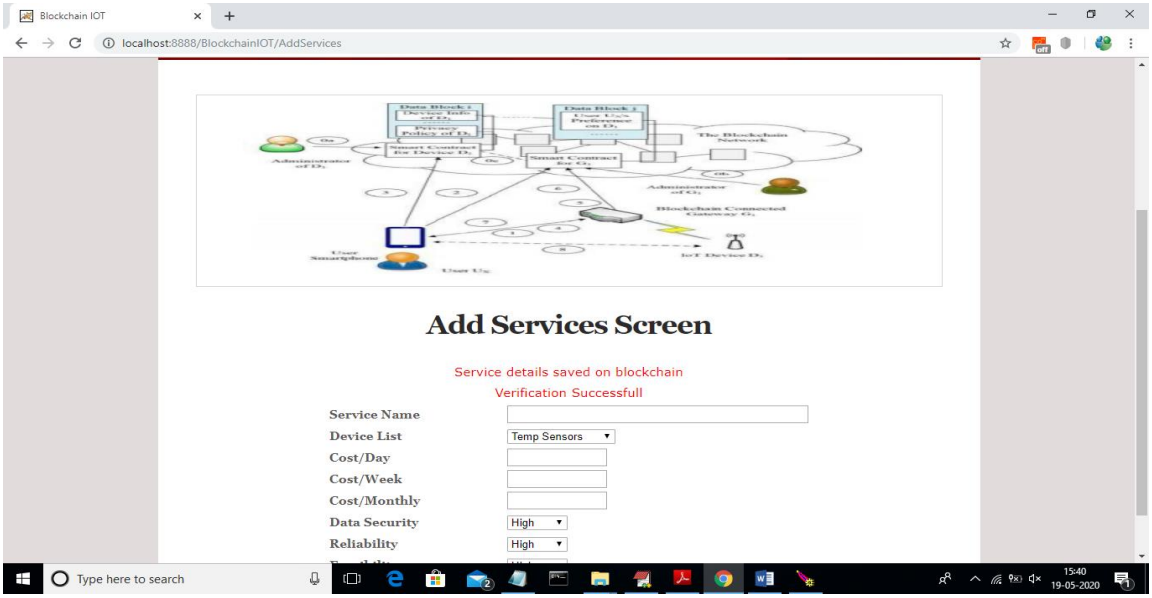
This public-key encryption algorithm is designated to create an electronic signature. A signature is created "in private," but it can be verified "in public." In other words, there is only one subject that can create a signature added to a message, but anyone is in a position to check whether or not the signature is correct. Security features of this algorithm stem from the computational complexity of taking logarithms in the finite fields.

The DSA algorithm is a modification of the ElGamal encryption algorithm and offers a number of benefits:

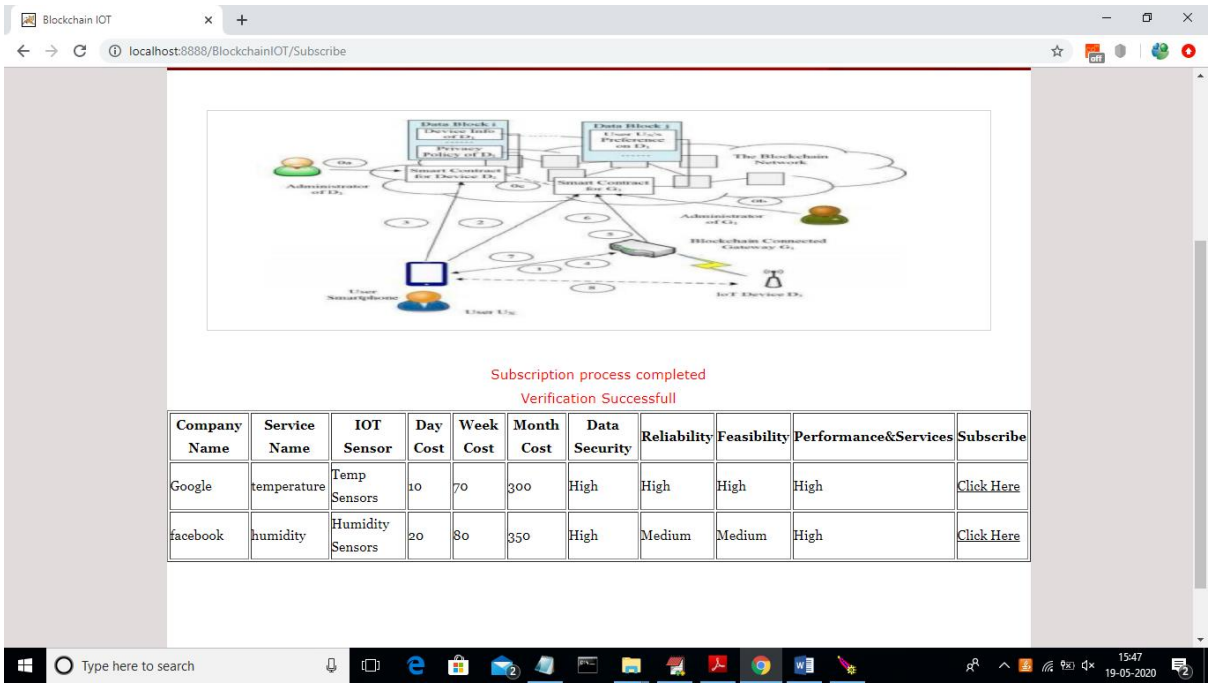
- Shorter signature length despite the identical strength levels.
- Lower signature computation speed.
- Reduced required storage space.

## 4. RESULTS

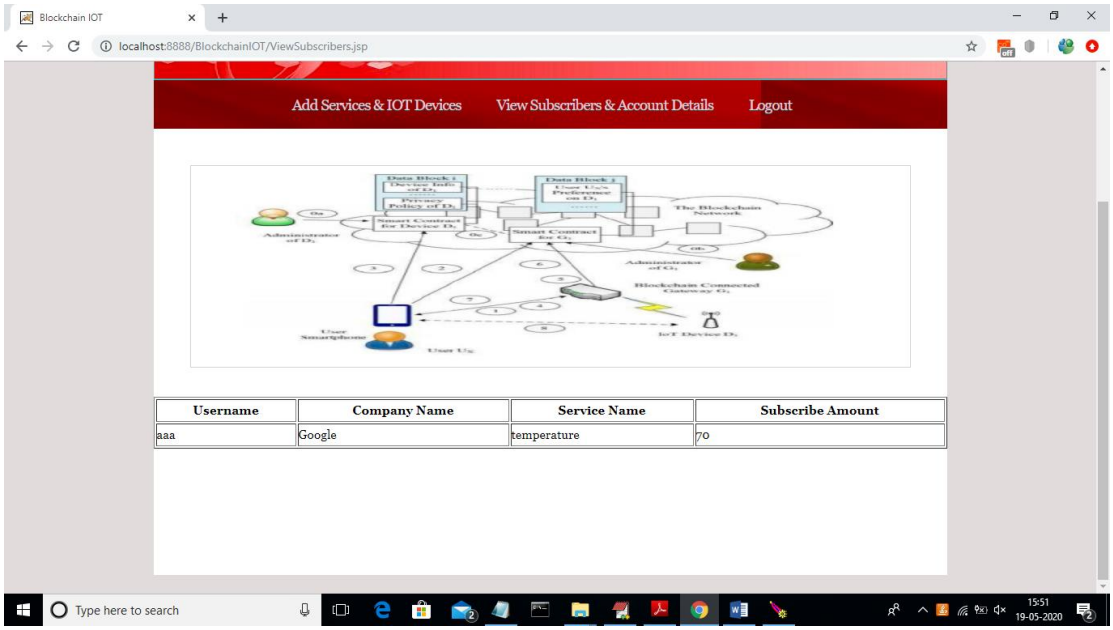
In below screen service provider is adding some service and now clicks on 'Submit' button to add service




In above screen service details added to Blockchain. Now logout and signup new user to subscribe service




In above screen we can see subscription process complete. Now user can click on 'View Subscribed IOT Sensors Data' link to view last 10 records of sensor data. Here we don't have any sensor so we are generating sensor values randomly.




In above screen we can see which user is subscribing to which company and its services and the balance amount in that company account.

## 5. CONCLUSION

This paper described the concept of providing security for payment processing involved in IOT devices and their service usage by applied Blockchain technology. Blockchain is a secured distributed cryptographic hashing technique which maintains transaction in a transparent and unalterable format. It maintained block of chained transaction and keeps on validating old and new transaction and if old hash matched then only transaction will be considered as successfully verified. All users' transaction will be privacy protected and this same technique applied in this project to secure payment process happened between users and company services. All data in this project saved inside Blockchain and authentication and privacy will be performed by using DSA (digital signature algorithm) and SHA hashing technique.

## REFERENCES

[1]. Ahmed, E.; Yaqoob, I.; Hashem, I.A.T.; Khan, I.; Ahmed, A.I.A.; Imran, M.; Vasilakos, A.V. The role of big data analytics in Internet of Things. Comput. Netw. 2017, 129, 459–471.

[2]. Kshetri, N. Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommun. Policy 2017, 41, 1027–1038.

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

[4]. Moin, S.; Karim, A.; Safdar, Z.; Safdar, K.; Ahmed, E.; Imran, M. Securing IoTs in distributed blockchain: Analysis, requirements and open issues. Future Gener. Comput. Syst. 2019, 100, 325–343.

[5]. Wang, X.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Niu, X.; Zheng, K. Survey on blockchain for Internet of Things. Comput. Commun. 2019, 136, 10–29.

[6]. Global, T.F. History of Blockchain. 2019. Available online: https://www.tradefinanceglobal.com/blockchain/history-of-blockch ain/ (accessed on 22 January 2022).

[7]. Buterin, V. A next-generation smart contract and decentralized application platform. White Pap. 2014, 3, 1–36.

[8]. The 5 Best Blockchain Platforms for Enterprises and What Makes Them A Good Fit. 2019. Available online: https://medium.com /swishlabs/the-5-best-blockchain-platforms-for-enterprises-and-what-makes-them-a-good-fit-1b44a9be59d4 (accessed on 7 January 2022).
[9]. Lu, Y. The blockchain: State-of-the-art and research challenges. J. Ind. Inf. Integr. 2019, 15, 80–90.
[10]. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain technologies for the internet of things: Research issues and challenges. IEEE Internet Things J. 2018, 6, 2188–2204.
[11]. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. 2018, 82, 395–411.
[12]. Makhdoom, I.; Abolhasan, M.; Abbas, H.; Ni, W. Blockchain's adoption in IoT: The challenges, and a way forward. J. Netw. Comput. Appl. 2019, 125, 251–279.
[13]. Hassan, M.U.; Rehmani, M.H.; Chen, J. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. Future Gener. Comput. Syst. 2019, 97, 512–529.
[14]. Cui, P.; Guin, U.; Skjellum, A.; Umphress, D. Blockchain in IoT: Current Trends, Challenges, and Future Roadmap. J. Hardw. Syst. Secur. 2019, 3, 338–364.
[15]. Viriyasitavat, W.; Anuphaptrirong, T.; Hoonsopon, D. When blockchain meets internet of things: Characteristics, challenges, and business opportunities. J. Ind. Inf. Integr. 2019, 15, 21–28.
[16]. Suhaliana bt Abd Halim, Norul & Rahman, Md Arafatur & Azad, Saiful & Kabir, Muhammad Nomani. (2018). Blockchain Security Hole: Issues and Solutions. 739-746.
[17]. Website: https://cointelegraph.com/news/how-pegged-sidechains-cansolve-the-problem-of-transacting-across-blockchains, Last Accessed: January 9, 2022.
a. Kaushik, A. Choudhary, C. Ektare, D. Thomas and S. Akram, "Blockchain — Literature survey," 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, 2017, pp. 2145- 2148.
[18]. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy. arXiv preprint arXiv:1712.02969.
[19]. Website: https://credits.com/en/Home/New_Ins/4056, Last Accessed: January 9, 2022
[20]. Website- https://www.corero.com/blog/870-the-rise-of-iot-botnetthreats-and-ddos-attacks.html, Last Accessed: January 9, 2022.
[21]. Website- https://www.fraedom.com/496/blockchain-technologykeeps-data-secure/, Last Accessed: January 9, 2022.
[22]. Jindal, F., Jamar, R., & Churi, P. FUTURE AND CHALLENGES OF INTERNET OF THINGS.