# Survey on Blockchain Based Privacy Preserving Digital Ledger for Medical Data sharing

RENE THOMAS
MTECH SCHOLAR
Govt. Engineering College
Manathavady
Kerala, India-670645

ANITHA V S
Head of the Dept, CSE
Govt. Engineering College
Manathavady
Kerala, India-670645

Abstract—Blockchain-based privacy-preserving digital ledgers can be treated as a catalyst for security aspects in various internetworking domains and the digital frugality. It is a remark-able incorruptible methodology to knit the entire world in the network of certainty, accountability and lucidity. The technology behind digital currencies(cryptocurrencies) like bitcoin. It is a decentralized and distributed digital ledger of all transactions across peer to peer a network where it acts like a key that will enable every human being to be connected to this network and conduct business with each other in more limpid, hitch and secure way without involving an intermediary support to intensify the transaction. Blockchain-based medical data sharing system can be used to ensure Confidentiality, Integrity, and Availability. It maintains anonymity through the tactics of private or public ECDSA keys. Authentication, Authorization and Audit (AAA), fundamental security aspects for protecting information, designing and managing new systems and networks highlights the existence of blockchain based digital ledger in almost every industry.

In this paper, we survey and compare the existing digital transaction techniques what makes blockchain made so popular and inevitable technology and how blockchain made digital entities more secure. Finally detailed study current blockchain technologies and how blockchain become the defender of data dissemination issues.

Index Terms—Blockchain, cryptocurrency, Peer -to-peer, digital ledger, elliptic curve digital signature algorithm (ECDSA), integrity, Authentication, Authorization,Audit

## I. INTRODUCTION

Todays enterprise is all under attacks. Computer or digital assets and the various threats related to them are rapidly increasing in their size, shape and sophistication and representing the x-risk or the existential risk to the organizations around the globe. In this decade, life without digital transaction become an inevitable factor. So survey on digital assets, old and new banking-schemes, highly organized perpetrators who are trying to penetrate online transactions, reviews of emerging and proliferating technologies that make these attacks so interminable and effective is something which need to be considered. This survey deals with various digital ledgers, how blockchain is changing our society etc. finally review their implication to various security organizations, and the emendation techniques used in particular, in addition with these the how we can preserve digital assets, and perpetuate business or related organizations by privacy preserving digital transaction.

Everyone accepts money in the form of a payment thereby the mode of payment is more important. After barter system is expired the money in the form of paper came into existence. Then revolution of mobile changed the world with mobile payment in each and every sectors. Mobile payment always need to use some intermediary to transfer money. Due to the lack of proper awareness, probability of attacks over the network through these systems are increasing day by day. Finally by the end of 20th century concept of virtual currency is evolved and this diverges the digital world and banking systems. It lead to the innovation of the distributed decentralized ledger blockchain.

Digital security is nothing but where the identity is protected over the network and use assorted tools to secure our identity, digital assets and everything in the online environment. In this survey paper I would like to allot privacy preserving digital transaction ledger in digital security and specifically in cryptomining. Cryptomining is simply the mining of crypto coins or cryptocurrencies. Even though it's a bit intensive procedure in terms of it's computation, the mining will actually made this process success without having any complex or expensive software's or hardware's in hand. Blockchain is an example of well processed technology which needs cryptomining.

Blockchain [11]technology is one among the emanating trail for public organizations, industries, business, networks and even in the field of cyber security. It act as a cryptographically secure, shared and distributed ledger. The blockchain based privacy preserving digital ledger is a revolutionizing technol-ogy, by enabling ventures for an expeditious developments, diminished production cost, proliferating unprecedented innovations or renovations. The term blockchain was first elucidated in the original source code for bitcoin. Bitcoin is an example of virtual currency which uses blockchain technology. The participants of this transactions access peer to peer network can affirm transactions, without the need for a centralized certifying authority. The information stowed here are not modified by any party, it is coded in such a way that which prevents fudging of data. Which means information's can be transmitted through a huge network say supply chains and it

can be added to by users on networks without compromising security.

## II. RELATED WORK

In this section the main focus is on desperate topics related to digital transactions, various possible attacks to the existing systems, technology behind digital currencies and how these technologies are helpful in other prominent innovations and tactics. Basic intention of this survey is to make aware everyone, the importance of digital transactions it could be a contract, money, files or anything on anytime in an everywhere accessible fashion. The concern is all about how we can actually overcome the general problem in such way that it will never compromise any integrity or security aspects in the systems. For that we can use blockchain technology, Let's consider different aspects in relation with blockchain.

### A. DIGITAL TRANSACTION

Transaction is act like an instance of either purchase or vend anything like a deal, a contract etc. Digital transaction is one which consists of single or more than one participants without the need of cash in hand. The major digital transaction types are:

DTM: : DTM is Digital Transaction Management is something which uses Cloud Service Provider (CSP) to share and store data across the network anywhere at anytime other than financial transaction.

Financial Transaction: : It is used to transfer money over the internet for various purpose. It need some trusted intermediary. For example consider the following [5]:

Why we need digital transaction?

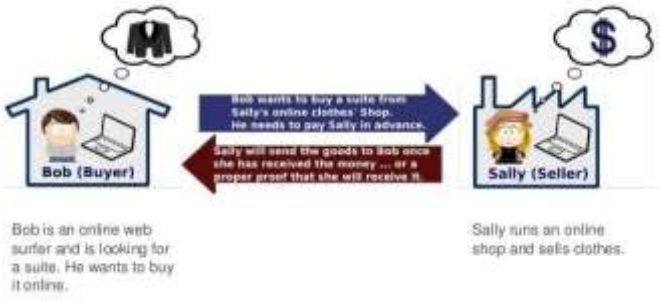


Fig. 1. Online Shopping using Digital Transaction

In figure name Fig. 1, it is clear that how most commonly used online shopping is related with digital transaction. Here bob the buyer wants to buy some cloths through online shopping site. So he request sally the seller for cloths. Sally the merchant send the cloths as soon as she received money or a proof to accept money later or anything like that. This is how the digital transaction takes place in the form of financial transaction with cloth and money exchange and there are 'n' no of sites are available for online shopping as well.

how digital transaction takes place?

The figure 2 explains simple representation on how the digital transaction is taken place through seven steps. In the first step the bob decided to buy some cloths online so he use an intermediary say pay pal. The moment Paypal receives request from bob, intermediary request payment from bob's credit card or anything which carries some money and accepts Paypal transaction. Then the other intermediary request for bob's banks for the payment. Bank will transfer the money to merchant account's. The time sally receives money then the merchant will send clothes to bob.

The figure 2 explains simple representation on how the digital transaction is taken place through seven steps. In the first step the bob decided to buy some cloths online so he use an intermediary say pay pal. The moment Paypal receives request from bob, intermediary request payment from bob's credit card or anything which carries some money and accepts Paypal transaction. Then the other intermediary request for bob's banks for the payment. Bank will transfer the money to merchant account's. The time sally receives money then the merchant will send clothes to bob.

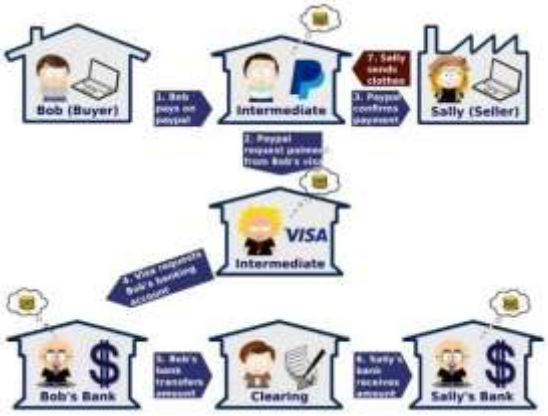


Fig. 2. Working of Digital Transaction

### B. ANALYSIS OF VARIOUS DIGITAL TRANSACTIONS

1) Bank Cards: Bank cards are basically a type of digital payment. This is one among most commonly used digital payment. Getting a bank card involves certain steps and and user must confirm these steps in order to make sure the transaction is secure and valid at the same time.

Steps involved in getting a bank card

– Issuing the bank card from the existing bank account
– Activation of the bank card

Types of Bank Cards

– Prepaid Card
– Debit Card

2) Aadhaar Enabled Payment System (AEPS): The AEPS, basically a payment method using AADHAAR. This can be used as world wide payment system if you have one valid account which generated from the aadhaar card.

Steps Involved in AEPS

– Find a micro automated teller machine (atm)
– provide specific atm with your name in the aadhaar card
– select the transaction mode

– provide finger print lock
– Take the slip for further reference
– transaction completed.

3) Unstructured supplementary service data (USSD): The USSD, the third universal application, the unstructured supplementary service data. It is basically a mobile based banking system.

Steps required for activation of USSD

– Select an deposit or any account which supports USSD
– Personal smart phone which supports facility of GSM

GSM means a global system for mobile communication.

Steps involved in Registration

– Find a branch in order to link specified mobile number and the specific bank account
– Receive Mobile Money Identifier (MMID) and its Mobile Personal Identification Number (MPIN)
– Remember your MMID and MPIN for further procedures.

4) Unified payment interface (UPI): The UPI is one among the digital payment system which we are using for online transaction of money. It even used for many other applications as well in order exchange or purchase your necessary items using money online. The main requirement of having such a system is a mobile with internet facility and the other is bank account details which is basically used in registration purpose. In India almost 28 applications and banks supports this facility online.

Steps involved in registration

– Go to the app store and download appropriate bank's application
– Select unique id for registration
– Select your bank
– Give account details for the first time
– Set pin for validating the transaction
– Completion of registration

Steps involved in sending money on UPI

– Choose send money option in the application
– Enter payees any of the address used in virtual payment
– Type the amount you need
– Conclude with remarks
– confirm the details
– Hit or press send option

5) Wallets: E-wallets or simply wallets are electronic prepaid payment system. We can consider the wallets a mobile facility. Mainly used for online purchasing and any kind of stores which we can swipe with a smart phone or equivalent one. Now next concern is nothing but an individuals details must be linked with the wallet in order to access and proceed further needs and clarifications.

steps involved in using Consumer wallets

– Consume or download the app on your mobile phone
– Register with mobile phone
– Add money from debit or credit by net banking services
– Wallet is ready to be proceed

Steps involved in using Merchants wallets

– Shopkeeper or stake holder must purchase or down-load the app
– Shopkeeper or stake holder must purchase or down-load the app
– Register the personal device with it
– Declaration as a merchant
– Proceed the payment

6) Point of Sale (POS): There are mainly three types of POS [?] or point of sale payment systems are available. They are the physical POS, Mobile POS or MPOS. Physical cards are nothing but the physical cars swiping. It is actually the PSTN or public switched telephone network with land line GPRS or the general packet radio services enabled. This is one of the most interesting payment system in which we can provide variety of applications in various sectors which enhance future growth in payment systems.

Working of the Physical version of point of sale

– swipe the card using a mobile phone
– Type the pin and then type the amount
– Receive receipt for future reference

Working of MPOS

– Plug in the M swipe
– Launch the application
– Swipe your customer's card
– Receive the message to mobile phone.
– Obtain the customer's signature
– Enter the card holder's email and the mobile number

Out of these six major online payment systems each and every systems has their own disadvantages and advantages and all of them need an intermediary to transfer goods or money from one to another.

## C. BLOCKCHAIN

Blockchain is a technology that came it existence in 2008 for bitcoin and now act as a trust-less intermediary with maximum possible anonymity and in short a digital asset technology that work with each and every application that we needed today. Internet of Things (IoT) is one among the core part where blockchain can apply. There are lot more applications are used to implement blockchain and improve security without compromising any privacy in the transaction. The blockchain itself is a tortuous computational mathematical function to create secure and definite record for your business. Major advantage of blockchain technology is it is decentralized distributed ledger so the term intermediary has no direct or indirect use in this technology.

Usually the blockchain database consists of two kinds of records, the transactions and the blocks. The block is where in which we can hold, the valid transactions of our digital assets. Once it stores the transaction in it and then encrypted with suitable encryption algorithm. A block of data is somewhat permanently recorded set of data. The data is first hashed, represented in a solid format, where it could easily compared for any changes. The comparison is something more than a valid plagiarism check so the result is accurate. Any small changes in the data complexity change the hashed version,

which makes the comparison super easy. While every transaction being processed, allowing users computer to verify the validity of each transaction. Hashed data is then encrypted and the private key allows the producer of the data to encrypt the data and serves as the digital signature whereas a public key allows everybody else, with the key to decrypt it.

A blockchain consists of 3 types of blocks which are represented using different colors. The green block is what we call it as green block or the Genesis block. It is the first block created by man who behind this bitcoin and blockchain technology in 2008 itself. This block is also represented by block 0. The block 0 is a combination of it's hash value with leading zeros in the left hand side , the times tamp value as it is digitally signed, the coinbase parameter, the raw block data represented using hexadecimal number, then it's prev block, merkle root, input, output, nounce, bits, no of transactions, sequence, script length etc. The second is the main block or one which use black color. It is the longest block in the blockchain. It shows a continuously growing list of blocks. Last but the least is orphan block. These are basically the detached blocks. Even though orphan blocks are valid transactions, their parents may not be there in the block chain just like that. when two different miners produce blocks at similar times thereby they can attacked by an intruder then it is termed as orphan blocks.Figure 3 shows how the block in a blockchain looks like.

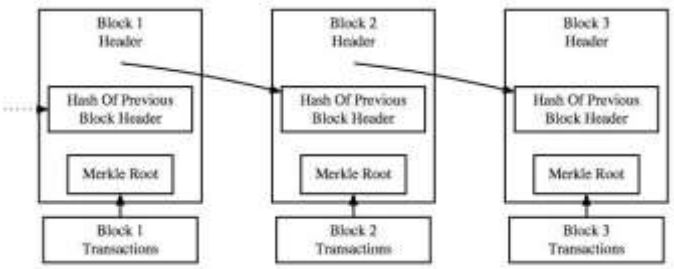


Fig. 3. Structure of a block

The blockchain mainly concentrated on Elliptic Curve Dig-ital Signature Algorithm (ECDSA) [9] in order to provide maximum security. In digital signature algorithm (DSA) it ensures data integrity, authentication of data origin. non-repudiation etc. In the extended version of DSA, ECDSA uses elliptic curve cryptography which is a combination key generation , signature generation and finally the signature verification. These three steps enhances the crypto-systems and improve it's authenticity and all other features. Blockchain uses consensus algorithm, where consensus which is nothing but a series of procedures which are used to check it's validity and aftereffect causing the confirmed transaction. The consensus algorithm is an algorithm used to approve the digital ledger using consensus. Examples of consensus algorithm includes the proof of work, proof of stake etc. The main advantage of having such algorithm is to achieve reliability inside the nodes in the network. Here node must agree each transactions in order to arrange them in the blockchain as they are mined in mining pool.

transactions in order to arrange them in the blockchain as they are mined in mining pool.

a) Benefits of Blockchain over Centralized Banking System:

Security: A blockchain assets provide an enhanced level of security, increasing the security of the system from hacking and fraud.

Easy to Use: It provides an easy mechanism to allow users to securely transfer the assets between parties and facilitates easy audit of user accounts.

Flexibility: Using a blockchain does not mean that the system will need to be a public ledger or open system if this is undesirable.

Privacy: The system may remain totally private if desirable.

Accounting: Blockchain provides a powerful accounting and auditing layer.

Malleable Technology: Blockchain assets are currently unregulated, helping minimizing management costs and expand the possible user base and distribution channels.

D. BSCIOT

BSCIOT or Blockchain based smart-contracts are used for IoT [6] enhancements which leads to many applications in order to provide maximum anonymity and outcome based production in several industries. One of the example for Blockchain based smart-contracts for internet of things is health care as a service. This is used in the medical field. In health care first a person wants to make a contract with an original equipment manufacturer (OEM). This contract is actually digitally signed for the specific matter say for example if you want this for weight loss in a stipulated period of time. You first assure your request with OEM. OEM will give this to every devices who wants to participate in the network of communication.

Here each every nodes say the devices will be proactive. This is will be beneficial suppose if someone or any device did some alterations with some malicious intention then it will automatically monitored and this will be detected. Once it is detected the authority will be announce some intruder is started working with the system. This is done by using blockchain technology is association with the smart contracts developed for internet of things. Here a hash function is used in order to make this hashing properly and this made the system difficult to decrypt in future.

The main advantages and disadvantages of having blockchain based smart contracts for IoT is described below:

Advantages

– It ensure maximum of services & resources.
– It helps to create a proper market environment between the participants who wants to participate in the service and device agreements.
– It allows us to automatically verify the algorithms to enhance the techniques inside the smart contracts.

Disadvantages

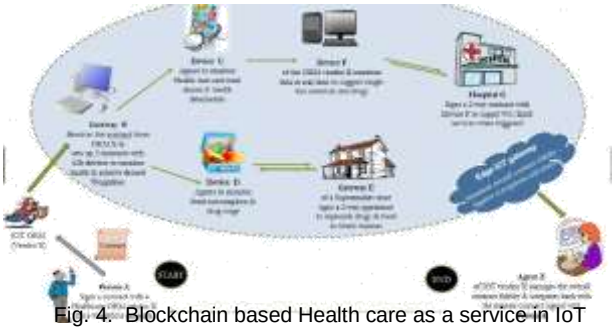

Fig. 4. Blockchain based Health care as a service in IoT

– Deployment issues in IoT with blockchain
– routing attacks

### E. BLOCKCHAIN AS A SOFTWARE CONNECTOR

Here the software connector [13] act as the fundamental building blocks of each and every software based interactions in our day to day software based life. Wherever you go you need to have the proper placements for the software connectors. Here the software connector could be anything like for example, basically it is termed as an architectural element which is used for several purpose according to the client request. It models either the interactions among the components or something like rules that are used to govern those interactions existed inside the system.

In blockchain based software connector our primary concern is on software connectors like repositories. Repositories in the sense like git hub, so we can use this to store and share anywhere anytime purpose. It enhances the overall idea of being a storage unit. The blockchain will automatically use some anonymous id which are trust less and hence it provide security without compromising any security concerns either inside the inside even if it may lack some in the network based or cloud based strategies. For the transaction based system it uses the ripple based protocol.

### F. BEBDA

Here BEBDA is Blockchain based approach to enhance big data authentication in distributed environment [1]. In this approach, in order to enhance big data authentication the main concern is all about with kerberos based authentication tools. This is mainly focused for linux based system users. While linux system users have various types of tools are used for several authentication tool. These tools may or may not be secure enough to hold further transaction based systems or data integrity. It handles almost every security issues in the big data authentication. It provides better security for the kerberos. Main application is in the cyber forensics. Cyber forensics use this technology in order to find the vulnerabilities in the system which are used for several cyber crimes. Public key based cryptography is used for this simple level authentication services. This makes the system to promise high levels of data with tamper proof. The MD5 algorithm that means the message digest algorithm is used.

| ALGORITHM USED FOR HASH FUNCTION | MESSAGE (Bits) |
|---|---|
| SHA-0 | <2^64 |
| SHA-1 | < 2^64 |
| SHA-256 | < 2^64 |
| SHA-384 | < 2^128 |
| SHA-512 | < 2^128 |
| MD5 | <2^64 |

Fig. 5. Hash Function Comparison

| Algorithm used | Rounds |
|---|---|
| SHA-0 | 80 |
| SHA-1 | 80 |
| SHA-256 | 64 |
| SHA-384 | 80 |
| SHA-512 | 80 |
| MD5 | 80 |

TABLE I
HASH FUNCTION COMPARISON

### G. MEDSHARE

In MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain [12] the blockchain is used in order to prevent the data loss and repetition of the data. As a matter of fact first we need to identify the need for the particular system. This is system helps to add and share data with anonymity and authenticity inside a medical based application. Insufficient source to store the data and issues while the records sharing can be clarified with the block based system. In this approach each record will be recorded as different blocks in the network. So that data will be secure enough to share without having any failure in the data transfer or anything like that. Even though it uses smart contracts based IoT system this is more reliable in the network scenario.

## III. COMPARISON OF RELATED WORK

During comparison of related works that I have already discussed above, first comparison is in between the technologies used for various digital transactions techniques. The technologies can be differ in terms of their hash functions uses, consensus algorithms used, etc.

Hash function is used to secure the smart contracts, Internet of things, the medical records and the authentication tool. First we have to compare the hash function based on their messages per bits. This is explained in figure 6.

Hash function compassion is now compare in terms of the rounds in which the algorithm is repeated. This is explained in the figure 5.

Since the comparison shows security is higher for SHA-384 algorithm but the computational speed is higher for SHA-

| Property | PoW | PoS | PBFT | Ripple |
|---|---|---|---|---|
| Node Identity Management | Identity Open | Identity Open | Permissioned Identity | Identity Open |
| Energy Savings | Partial Savings for electricity during mining | No savings | Can save power | No mining so energy is saved. |
| Example | Bitcoin | PeerCoin | Hyperledger Fabric | Ripple |

Fig. 6. Consensus Algorithm comparison

| Authors | Advantages | Disadvantages |
|---|---|---|
| KONSTANTINOS CHRISTIDIS | Tamper Proof Systems | Deployment Issue |
| XIEWI XU | High performance in terms of security, privacy, scalability, sustainability | Computational Power is low |
| NAZRI ABULLAH | Secure Data authentication | Chance for routing attacks |
| EMMANUEL BOATNEG | It ensure secure authentication, high performance and applicable for almost every sector with reduced attacks | Deployment issue for coming technologies |

Fig. 7. Comparison on Survey Papers

256. so what matters is here we have to deal with multiple computations simultaneously, so its important to have higher the speed the rate of transaction will be more beneficial and it is used for various applications over the network. So the SHA-256 can be treated as best among them.

Now let's compare the different consensus algorithm used in various blockchain systems, and based on that the we can decide the need for having a proposed system which ensure the maximum possible benefits for various tasks. This comparison is shown in figure 6.

Lastly comparison can be done with respect to the survey papers used for the comparison in this paper. During this comparison the main concern is on advantages and disadvantages of various papers. Comparison is done on figure 7.

Advantages of having intermediary systems without Blockchain

– Time Savings
– Reduced risk of loss and theft
– Low commissions
– User friendly
– Convenience
– Light but deep pockets
– Discounts and freebies
– Easy expense tracking & documentation
– Reduced risk of losing money

Disadvantages of having intermediary systems without Blockchain

– Increased risk of identity theft
– Losing phone means losing all your money
– Adapting is difficult for tech problems
– Adapting is difficult for tech problems
– High chances of overspending
– The risk of being hacked
– The problem of transferring money between different payment systems
– Restrictions
– The lack of anonymity
– The necessity of Internet access

## IV. Attacks in the Existing System

In this section, we give an overview of the two routing [3] attacks we describe in this paper: (i) partitioning attacks (ii) BGP Hijack (iii)Delay attacks. The main attack is attack in the blockchain. In the partition attack, the miners in the mining pool first started the mining with the corresponding transaction and thereby the bitcoin connections were all established. Then the attacker will monitor the traffic assessments and then divide the traffic into two different portions say left hand side and the right hand side traffic. During the partition timing, attacker will start the mining maliciously and attack the system in such a way that no other party will be able to understand the attacks before it's over. The other type of attack in on BGP hijacking. In this BGP hijacking, this is the boarder gateway protocol attack. During transaction, it's carried over the network with different autonomous system. Each autonomous system uses boarder gateway protocol for their communication. Once this transaction started the attacker will be able to hijack the traffic using the BGP and this is one of the main routing attack in the network. Next is Delay attack, in the delay attack the intruder will penetrate into the system and started mining maliciously and the attacker will hold the system for a 20 minutes. And after this 20 minutes, the miner may or may not be loss the data or loss the transaction and it causes many issues in the system.

## V. Blockchain Based Privacy Preserving Medical Data sharing Digital Ledger

Distribution of electronic records is an inevitable factor in digital era. Nowadays the dissemination, public engage- ment and exploitation of various digital records results drastic ethi-cal issues to the world of security. Blockchain based systems can be treated as a catalyst for security aspects in various internet-working domains and the digital economy. Blockchain is a singly linked list of blocks. Each block consists of details of the transactions. And transaction could be an asset, contract or any value that can represented in the block in the form of an asset. Blockchain based privacy preserving medical data sharing digital record (medichain) is a private blockchain using hyper-ledger fabric. Only those who have permission to access the medical data can request and use the service. Here in medichain, the asset can be the medical data which must protected enough. Medical data sharing digital record (medichain) uses secure hash algorithm and efficient elliptic curve cryptographically (ECDSA) assigned digital signature (DS) for data provenance and mining of blocks with tamper proof medical records. Usage of private blockchain makes

the data invisible from public and access granted for valid users only. This enhances security, anonymity and privacy for medical based records. From the survey on various dig-ital transaction technologies and different blockchain systems implies the medshare [12] can be used to eliminate issues regarding medical data sharing. Modification in the existing system with advancement in various phases of the system will help us to build privacy preserving data sharing digital ledger for medical field.

## VI. Conclusion

In this review paper, comparative study on various hashing mechanism and consensus algorithms is used to determine which one is more good and faster to the proposed model and this related study resulted like SHA-256 is comparatively efficient and faster than other techniques. With the help of SHA-256 and elliptic curve digital signature algorithm with GPU accelerated signature server used to maximize comput-ing power. This will reduce routing attacks related to the blockchain. Where routing attacks are the only possible attacks to the existing system and in all other ways the proposed system is a tamper proof one. Blockchain as a service can be treated as a catalyst for security aspects in various inter networking domains and the digital economy. Open source BaaS, it is publically accessible. It is a remarkable incorrupt-ible methodology to weave the entire world in the network of trust, accountability and transparency. A combination of blockchain based system using private blockchain using hy-perledger fabric for private based needs for example medical data record sharing system, server will decrease the chance of failures with maximum sustainable results.

## References


[1] N. Abdullah, A. Hakansson and E. Moradian (2017). Blockchain based approach to enhance big data authentication in distributed en-vironment. Ubiquitous and Future Networks (ICUFN), 2017 Ninth International Conference on, 887–892. IEEE.

[2] S. Antao, J.-C. Bajard and L. Sousa (2010). Elliptic curve point multiplication on gpus. Application-specific Systems Architectures and Processors (ASAP), 2010 21st IEEE International Conference on, 192– 199. IEEE.

[3] M. Apostolaki, A. Zohar and L. Vanbever (2017). Hijacking bitcoin: Routing attacks on cryptocurrencies. Security and Privacy (SP), 2017 IEEE Symposium on, 375–392. IEEE.

[4] J. Benet (2014). Ipfs-content addressed, versioned, p2p file system. arXiv preprint arXiv:1407.3561.

[5] B. Bogdan (2018). Blockchain und der schutz unserer privatsphare¨. MedRevolution, 93–108. Springer.

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

[7] P. Forte, D. Romano and G. Schmid (2016). Beyond bitcoin-part ii: Blockchain-based systems without mining. IACR Cryptology ePrint Archive, 2016, 747.

[8] S. Nakamoto (2008). Bitcoin: A peer-to-peer electronic cash system.

[9] W. Pan, F. Zheng, Y. Zhao, W.-T. Zhu and J. Jing (2017). An efficient elliptic curve cryptography signature server with gpu acceleration. IEEE Transactions on Information Forensics and Security, 12(1), 111–122.

[10] P. K. Sharma, S. Singh, Y.-S. Jeong and J. H. Park (2017). Dist-blocknet: A distributed blockchains-based secure sdn architecture for iot networks. IEEE Communications Magazine, 55(9), 78–85.

[11] S. Singh and N. Singh (2016). Blockchain: Future of financial and cyber security. Contemporary Computing and Informatics (IC3I), 2016 2nd International Conference on, 463–467. IEEE.

[12] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du and M. Guizani (2017). Medshare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access, 5, 14757–14767.

[13] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A. B. Tran and S. Chen (2016). The blockchain as a software connector. Software Architecture (WICSA), 2016 13th Working IEEE/IFIP Conference on, 182–191. IEEE.