Blockchain:

Enhance the Authentication and Verification of the Identity of a User to Prevent Data Breaches and Security Intrusions

1st Haydar Teymourlouei
Department of Technology & Security
Bowie State University
Bowie, USA
hteymourlouei@bowiestate.edu

2nd Lethia Jackson
Department of Technology & Security
Bowie State University
Bowie, USA
ljackson@bowiestate.edu

Abstract—Blockchain has attracted many of attention across the world. Instead of storing information in centralized servers, blockchain utilize a network of independent computers that replicate each record of data it creates. Users can use blockchain and still experience hacker hijacking a user’s session and accessing user’s virtual wallet. The biggest hindrance for migrating several online services is the ability to secure the data and verify the identity of the users of that service. In this paper, we propose the methods which it will provide authentication and verification of the Identity of a user to prevent data breaches and security intrusions. The user will need to use of multi-step authentication where a randomly generated key is sent to the user's email, cellular device for validation if that user wants to add to the blockchain. At present, online authentication depends on a password or on the occasional use of dual-factor authentication.

Keywords—Blockchain, Authentication, Data Breaches, Security, Bitcoin

I. BACKGROUND

The world of the blockchain design established on October 2008 and it associated with a person named Satoshi Nakamoto. Nakamoto published a paper by using an obscure Internet mailing list detailing a design for a public database distributed and synchronized every ten minutes across thousands of computers. It is accessible to anyone and yet hackable by no one. Its purpose was to provide a decentralized, bulletproof record of exchange for a new digital currency which Nakamoto termed it as Bitcoin.

The importance of Blockchain Technology is to secure sensitive records and to authenticate the identity of the user. The technology has Keyless Security Infrastructure which it stores data hashes on blockchains. Correspondingly, it runs a hashing algorithm for their verification. It has a Public Key Infrastructure, which it is an encryption approach. It is most helpless man-in-the-middle and DDoS attacks, therefore, it deleted out of the equation. Any attempt of data manipulation can be spotted without effort since the existing hash is available on other nodes linked to the system, permitting banks to go beyond asymmetric encryption and caching in public keys. The blockchain is the technology that is used in the common cryptocurrency bitcoin. It is innovative in numerous ways. It can be a solution to several challenges associated with digital transactions, for instance, double spending and currency reproduction. The cost of online transactions can be decreased by using blockchain and at the same time increasing authenticity and security [12]. Fig 1 shows how the blockchain approach to land rights could also be used to map and secure genetic resources that will be critical to building a global bio-economy.

Fig. 1. Blockchain Process [9]

II. INTRODUCTION

The blockchain technology offers a solution for a diversity of security concerns that exist in our everyday activities of life. Furthermore, the blockchain can offer a solution by decentralizing the ownership of credentials and offering a collectively accessible protocol for verifying records of an
individual in an immutable chain of data. The data could be stored in a shared ledger rather than based on individual storage. Shared ledger can be downloaded by each separate user of the blockchain and it is a record of every transaction ever made. If someone wants to become a part of the blockchain network, they must have a wallet. Initially, a user must register with an email address and a user-created password. An email is sent to the user to authenticate the user. This allows the users access to their wallet. When users want to login again, they have to use their wallet ID and the password. Authentication and verification are significant parts of preventing user identity against data breaches and security intrusions. Using civic app, control flow of personal data and manage identity and credentials are the methods to prevent data breaches from the users. In order to prevent security intrusions, it is necessary to use firewall and techniques. Also, there are recommendations which it will support the methodology for better preventions.

Blockchain is simply a series of blocks that records data in hash functions with timestamp and the link to the former block. The said blocks are stored anonymously with other stakeholders within a network. It eliminates centralized points of vulnerability which cybercriminals can exploit. Blockchain technology can play as an essential role in make safe internal communications, which are disposed to data leaks and cyberespionage. Since end-to-end encryption fails to cover the metadata. It can lead to leakage of sensitive information. In a blockchain-based system, the metadata used for communications is scattered in the distributed ledger and cannot be collected at one central point.

Blockchain technologies can be roughly divided into three types as follow:

- Public blockchain which it allows user to check the transaction, verify it and can also participate in the process of getting compromise. Like Bitcoin and Ethereum are both Public Blockchain

- Consortium blockchains means the node that had authority can be chosen in advance. It always has partnerships like business to business, the data in blockchain can be open or private.

- Private blockchain, node will be restricted, though not every node can participate this blockchain, it has strict authority management on data access.

The following are blockchain structure. First, there is blockchain structure in the block. It contains main data, hash of previous block, hash of current block, timestamp and other information. Another structure is the main data. This is depending on what service is this blockchain applicable, for example: transaction records, bank clearing records, contract records or IOT data record. There is hash on blockchain structure. It converts an input of numbers and letters into an encrypted output of a fixed length. A hash is created using an algorithm and is essential to blockchain management in cryptocurrency. Blockchain used Merkle tree function to generate a final hash value, which is also Merkle tree root. This final hash value will be used to record in block header, by using Merkle tree function, data transmission and computing resources can be drastically reduced. Also, there is timestamp. It is time of block generated.

Smart contracts” are decentralized agreements built in computer code and stored on a blockchain. Supporters of smart contracts visualize a future where commerce takes place completely using smart contracts, avoiding the high costs of contract drafting, judicial intrusion, opportunistic behavior, and the inherent uncertainties of written language. The appeal of “smart contracts,” agreements built in computer code. Also, it stored on a blockchain. It is comparable to that of Bitcoin in many ways and other early blockchain applications, harnessing the same critical features as decentralized consensus, prompt exchange, and complex computational states. On Fig 2 indicate that smart contracts can check whether conditions are satisfied and then instantaneously provide the bargained-for goods or money. A smart contract is immutable and unmodifiable once created, since its logic is seeded into a blockchain spread across multiple points. It prevents influential parties from unscrupulously breaching the contract or extracting a beneficial modification that weaken weaker counterparties [14].

![Fig. 2. Smart Contracts](image)

Nowadays, many blockchain applications concentrates on modernizing the internal information device of organizations. A variety of blockchain companies are offering products that it makes recordkeeping low-cost and more correct, for instance in healthcare data tracking, property registration, supply chain management, and protecting intellectual property, amongst others. Nevertheless, extreme blockchain’s advocates visualize that the technology will transform not only how firms organize internally, but also how they interact externally. If blockchain code can instantaneously affect an exchange of goods based on the satisfaction of specified conditions, why would businesses rely on expensive, unpredictable agreements written in human language?

Cryptocurrency is simply a form of digital money that is designed to be secure and, in many cases, anonymous. It connected with the internet that uses cryptography, the process of converting legible information into an almost uncrackable code, to track purchases and transfers. It has evolved in the digital era with elements of mathematical theory and computer science to become a method to secure communications, information and money online. They do not work as currencies, they are grossly inefficient. They are not meaningfully distributed in terms of trust. Cryptocurrencies are tradeable cryptographic tokens, with Bitcoin as the most famous
example. Bitcoin, developed by a pseudonymous creator, Satoshi Nakamoto, consists of a distributed public ledger system showing all balances associated with public keys. To spend Bitcoin, someone with the corresponding private key signs a message indicating the balances should be transferred to a set of destinations and then broadcasts this message through a peer-to-peer network. Fig 3 is an example of Bitcoin which it shows the balance of the account. The network will then validate the transaction as valid in the public ledger and commits it to another block in the ledger containing at most 1MB of data. To prevent the block from being tampered, the Bitcoin system uses “proof of work”1 to protect its hash chain. Each block contains a pointer to the previous block creating the “blockchain”, and every miner attempts to create a new valid block.

Fig. 3. Bitcoin [6]

### III. HOW BLOCKCHAIN WORKS?

How does digital currency reliably pass back and forth on a decentralized network full of strangers that do not have a reason to trust one another? By generating a permanent ledger of transactions that cannot be changed by any single network member [17]. The main working processes of blockchain are as follows:

- The sending node records new data and broadcasting to network.
- The receiving node checked the message from those data which it received, if the message was correct then it will be stored to a block.
- All receiving node in the network execute proof of work or proof of stake algorithm to the block.
- The block will be stored into the chain after executing consensus algorithm, every node in the network admit this block and will continuously extend the chain base on this block.

Blockchain technology comes in particularly handy when it comes to monitoring supply chains. By removing paper-based trails, businesses should be able to pinpoint inefficiencies within their supply chains quickly, as well as locate items in real time. Further, blockchain would allow businesses, and customers, to view how products performed from a quality-control perspective as they traveled from their place of origin to the retailer. The following are real world use of blockchain technology.

**Payment processing and money transfers** arguably the most logical use for blockchain is to expedite the transfer of funds from one party to another. As noted, with banks removed from the equation, and validation of transactions ongoing 24 hours a day, seven days a week, most transactions processed over a blockchain can be settled within a matter of seconds.

Retail loyalty rewards programs Blockchain could further revolutionize the retail experience by becoming the go-to for loyalty rewards. By creating a token-based system that rewards consumers, and storing these tokens within a blockchain, it would incentivize consumers to return to a certain store or chain to do their shopping. It would also eliminate the fraud and waste commonly associated with paper- and card-based loyalty rewards programs.

Copyright and royalty protection in a world with growing internet access, copyright and ownership laws on music and other content has grown hazy. With blockchain, those copyright laws would be beefed up considerably for digital content downloads, ensuring the artist or creator of the content being purchased gets their fair share.

The blockchain would also provide real-time and transparent royalty distribution data to musicians and content creators.

A. Who Use Blockchain?

A blockchain transaction begins with one party agreeing to send data to another. These data could be anything. But because the point of a blockchain is to create a permanent, verifiable record of exchange, the data usually represent some asset. The common examples units of a cryptocurrency or other financial instrument are contracts, deeds or records of ownership like medical information or other identity data. The following are companies leveraging Blockchain for identification and authentication. Walmart, Maersk, British airways, UPS and FedEx are examples of the companies that they are using blockchain technology [16].

Also, Blockchain has Internet-of-Things (IoT). Internet of Things (IoT) platforms are the key for the development of scalable IoT applications and services that connect real and virtual worlds between objects, systems, and people. However, as the IoT platform market represents a truly new market segment that it was almost non-existent a few years ago. The platforms are complex and changing quickly. IoT platforms perform simple functions for example, providing useful information, and others can provide services through collaborations with IoT devices. With an Internet of Things (IoT) paradigm, applications can deliver useful services and convenience by interacting with services connected to IoT platforms. IoT platforms perform simple functions such as providing useful information, and others can provide services through collaborations with IoT devices. This situation needs the security generic service interface and results in a range of IoT architectures through not only the configuration settings of IoT devices and resources but also varied environments of collaboration for each device.
IV. RECOMMENDATIONS

These are recommendations of preventing data breach and security intrusions. By using the following recommendations, it will enhance the authentication and verification of the identity of a user.

A. Prevent Data Breaches

It is significant to enhance the authentication and verification of the identity of a user to prevent data breaches. The blockchain protects an identity by encrypting it and securing it from spammers and marketing schemes.

B. Using Civic App

This method will help to secure private sign-up and login. It also prevents data breaches from the users. New account creation can be simplified by providing verified identity data with the Civic app. While this service is more likely to work like Facebook login process. In general, Civic App secure: private sign-up and secure private login offers both privacy of data transactions and greater trust in user identity [5].

C. Control Flow of Personal Data

To control flow of personal data is important process to protect all data. It decreases the capabilities of data breaches. By using passports, birth or Wedding certificates, it easier to get more details of the user and they are the tools identify someone identity.

In 2014, the first digital passport launched on GitHub. It could help owners identify themselves online and off. Individuals must take a picture of them self, stamp it with a public and private key, both of which are encoded to prove it is legitimate. The passport stored on the ledger, given a Bitcoin address with a public IP and confirmed by blockchain users.

A few things are more significant than documents showing persons are born, married, died which open their rights to all sorts of privileges, yet mismanagement is rife. The blockchain could make record-keeping more reliable by encrypting birth and death certification and empowering citizens to access this crucial information.

D. Manage Identity and Credentials

It is necessary to manage identity and credentials through a simple digital wallet experience. Personal identification includes driver’s license, computer password, identity cards, keys and social security ID. Blockchain ID is a digital form of ID that’s engineered to replace all these forms of physical identification. In the future, fintech scientists say people will be able to use the one digital ID for signing up at any registrar. It is open source, secured by the blockchain, and protected by a ledger of transparent account.

E. Prevent Security Intrusions

Security technologies are very essential to balance the needs for access and protection of information. By using security intrusion detection, it will help to prevent any possible security intrusions. Also, techniques that are better at detecting insider security threats are desired.

F. Using Firewall

Firewalls are network security components that handle incoming and outgoing network traffic based on a set of rules. They have been a first line of defense in network security for decade. They establish a barrier between secured and controlled internal networks that it can be righthand and untrusted outside networks like the Internet. A firewall can be hardware or software.

G. Techniques

The following are techniques to prevent security intrusions based on authentication and verification of the identity of a user.

- Use a two-factor authentication and verification method.
• Use minimum password length of 15 characters
• Require the use of alphanumeric passwords and symbols
• Prevent the use of personal information as password such as phone numbers and dates of birth

More people worldwide face identity challenges. It is mandatory to focus on how to enhance the authentication and verification of the identity of a user to prevent data breaches and security intrusions. Microsoft is one of the companies that it is looking to change the situation. It is creating digital IDs within its Authenticator app currently used by millions of people. This would give users a way to control their digital identities. Furthermore, this would allow individuals in impoverished regions to get access to financial services or start their own business. Microsoft’s attempts to create a decentralized digital ID are in the early stages. Blockchain technology can be applied to identity applications in different areas example blockchain identity on use cases [13]: Digital Identities, passports, birth certificates, wedding certificates and IDs.

H. Public and Private Key Security

To access to a blockchain needs both a public and a private key. Keys are cryptic strings of characters of sufficient length to make “the odds of guessing” them truly astronomical. Since it is basically impossible to access data within a blockchain short of the right combination of public and private keys, this represents the strength of blockchain technology especially in security area. Without the right keys, there is no hacker will be able to access data. Keys must be available to users in 30 seconds to prevent security intrusions. Hackers are more likely to find the correct keys to access identities of the users.

I. Fingerprint

There are three Software creates a “fingerprint” for the new block by hashing the data inside it, together with two other pieces of information: the fingerprint of the preceding block and a random number called a nonce. The validated block is added to the blockchain with a digital fingerprint that also mathematically encodes the validated fingerprints of every block preceding it. These nested fingerprints make the blockchain increasingly secure with every new block that gets added because altering a single bit of information anywhere in the blockchain would drastically change not only the fingerprint of that block but every subsequent one in the chain as well.

V. METHODOLOGY

The HTTP communication uses several TCP connections. In this case, the server requires a method to identify every user’s connections. The most common method which is used the authentication process. Also, the server sends a token to the client browser. The attack has the agreement of the session token by stealing or estimating a valid session token to obtain unauthorized access to the web server. This compromising of session token can take place in different ways. Usually, the method having already been used to steal session ID by installing malicious code on the client website. After that event, the cookie will be able to purloin. The most effective way to prevent session hijacking is to permit the protection from the client side. It suggested taking preventive measures for the session hijacking on the client side.

The blockchain application creators approach the user authentication and qualification, validation particular their application. It is significant for a technical professional to view, blockchain through the scope of the cybersecurity and not by software or network infrastructure. As a fact, blockchain technology will take over the world forever and it is imperative for the technology industry. As it is known that blockchain is a paradigm shift. It is metamorphosing the technology industry and the economic infrastructure of the country in the future.

Fig. 6 above shows how authentication flow and can be secured. The blockchain authentication flow is a significant part of the process which consist of two factors: username and password. The implementation of the two factors will act as a barrier between the user login and the user access. A valid user can log in to their blockchain account with the username and password. As soon as the user logs in, the data will go to the cloud database to verify the information entered. Subsequently, the user will get a validation key to verify his/her identity. The cloud database houses the accounts for each user who has authorization to use the blockchain. To continue the process, the user will need to confirm their request to log in by entering the validation key. The validation key is a random number generated by an algorithm. The central database matches the recovery key against the random number to prove validation. The random key will continue to be used since it provides an extra layer of protection and searches to match the user’s recovery key. The random key is only used once since it eliminates a hacker’s possibility of reusing the same random key to get access to the blockchain. The random key generates a different number known as a credential each time the user tries to gain access. The key is given to the user after he/she has entered in the required credential. In the cloud, the database requests the transaction. In addition, the network
nodes confirm the user transaction by verifying the information on the network. If hackers want to hijack the session and gain access to the data, the random key will not be labeled as a valid user. As soon as the validation is done, the transaction is combined to create a new block which contains the date for the ledger. A cryptocurrency step will take place to verify the transfer of funds. The transaction is completed after the new block is added to the existing blockchain which serves as permanent protection.

A. Database

A blockchain is a database because it is a digital ledger that keeps information in data structures called blocks. In the same way, a database stores information in data structures which it called tables. Nevertheless, a blockchain is a database and database are not a blockchain. This is because they are not identical. They are both store information and differ in design. Correspondingly, there is a difference in purpose between the two. It is perhaps what is not clear to those who want to understand why blockchains are needed and the reason databases are better suited for storing certain data.

A blockchain utilizes a distributed network of nodes that is decentralized. The meaning of decentralization is all nodes on the network store a copy of the blockchain. The nodes either save an entire copy (full nodes) of the blockchain or execute mining operations or they can do both. It is not necessary to have an administrator to authorize a block of transactions. It will need to have miners that perform this verification by solving cryptographic puzzles based on a problems level proportional to the total network hashing power available. Once the block has been built on to the blockchain, the information is immutable and obvious to all. Blockchain transactions are non-recursive, meaning they cannot be replicated once validated in a block. A blockchain is high “fault tolerant” since if one or more nodes are down, there will always be other nodes obtainable that will run the blockchain.

To ensure that no one can change the data from the start point to the end point, I would like to initiate a simple and secure Blockchain Database API.

Blockchain is a database that allows the transfer of value within computer networks. This technology is expected to disrupt several markets by ensuring trustworthy transactions without the necessity of a third party. The proliferation of this technology is, however, threatened by technical issues that remain to be resolved [11]. A blockchain is made up of a series of blocks which contain data and each block contains a cryptographic representation of the previous block, which means that it becomes very hard to change the contents of any block without then needing to change every subsequent one; hence where the blockchain essentially gets its immutable properties. Since blockchains use cryptography, the SHA256 cryptographic hashing technique will be used to create hashes of our blocks. A block source file will be created in which the function prototypes will be declared. Blockchain technology was made popular when it was devised for the Bitcoin digital currency, as the ledger is both immutable and public. This means that, as one user transfers Bitcoin to another user, a transaction for the transfer is written into a block on the blockchain by nodes on the Bitcoin network. A node is another computer which is running the Bitcoin software and, since the network is peer-to-peer, it could be anyone around the world; this process is called ‘mining’ as the owner of the node is rewarded with Bitcoin each time they successfully create a valid block on the blockchain.

VI. Conclusion

In conclusion, blockchain is the technology behind bitcoin. While blockchain technology is very effective at facilitating and maintaining records, there are the needs of improving the authentication and verification of the identity of a user to prevent data breaches and security intrusions. By using Civic App, control flow of personal data, manage identity and credentials are the methods to prevent data breaches. To prevent security intrusion, it needs to use firewall and techniques. It recommended to use fingerprint and secure public and private key to keep identity of user protected. Blockchains designed for communities with a higher level of trust between users. These chains rely on a central authority that grants specific users access to the system, so they can serve as transaction validators.

REFERENCES


