AN INTRODUCTION TO CRYPTOGRAPHY AND BLOCKCHAIN SYSTEM

[1]P.Kumaraswamy, [2] Dr. R. Vijaya Prakash, [3] A.Harshavardhan [4] Dr. K. Seena Naik

[1] Assistant Professor, Dept. of CSE, S R Engineeing College,Warangal
[2] Professor, Dept. of CSE, S R Engineeing College, Warangal
[3] Assistant Professor, Dept. of CSE, S R Engineeing College,Warangal
[4] Associate Professor, Dept. of CSE, S R Engineeing College,Warangal

E-mail: [1]kumara_swamy_p@srecwarangal.ac.in, [2] vijaya_prakash_r@srecwarangal.ac.in,

[3]harsha_vardan_a@srecwarangal.ac.in, [4] seena_naik@srecwarangal.ac.in

ABSTRACT

Cryptography plays an important role in blockchain system. Currently, blockchain system is using in Banking, Finance, Health, Legal, and several other industries. Almost every leading organization is adopting this technology. However, deep expertise and world-class talent in blockchain is extremely hard to find. The need of the hour is creating this sought after talent pool which will contribute to growth in these sectors. This paper discusses the introduction about the cryptography and block chain system.

Keywords: Cryptography, Symmetric key cryptography, Asymmetric key cryptography, Blockchain, Security, Bitcoin, Ethereum.

INTRODUCTION

Cryptography is the study of mathematical techniques concerned with maintaining information protected either in standalone system or in a computer network from attackers. Many cryptographic schemes were developed to encrypt the data. Such schemes do not allow adversaries to anticipate the information. The one who produces such a cryptic data is a cryptographer. A cryptographer targets on developing and analyzing cryptographic algorithms. Cryptography algorithms [1] are mainly divided into two broad categories. First one is symmetric key cryptography. The second one is asymmetric key cryptography.

SYMMETRIC KEY CRYPTOGRAPHY

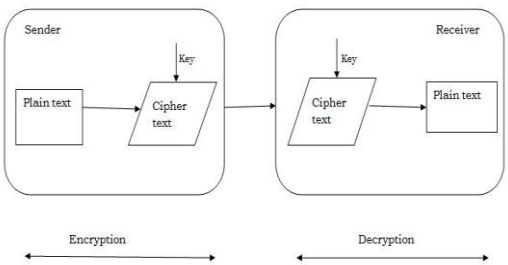

Figure1: Symmetric key cryptosystem

A symmetric key cryptosystem is shown at figure2. In this type of system both sender and receiver should mutually agree on a cryptosystem. Based on their agreement a secret key (key) is used by both the users for encryption and decryption of messages.

If a user wants to send messages to the other, the secret key is used to encrypt and decrypt messages as shown at figure1. Here, the actual message (plain text) is readable by any one. This message is converted into unreadable form (cipher text) with the encryption process on sender side. The resulted cipher text is reformed as plain text by only receiver using decryption process. The drawback of this scheme is discussed here under:

The major drawback observed in symmetric key cryptography was regarding the key distribution. It was necessary to create a secret key by the sender or receiver and send it by a third party (key distribution center). While transmitting the key over the network an attacker stands a chance to capture it. This becomes a disadvantage of the symmetric key cryptography to fail. Therefore, asymmetric key cryptography is explored.

Even though symmetric cryptography has some major problems (which we will discuss in a bit) the biggest advantage of symmetric cryptography is that it requires very little overhead. We just need to share one single key with our recipient to go forward with this method.

Even now, a lot of software use this method in conjunction with asymmetric cryptography to provide fast and efficient encryption/decryption services.

Even though the overhead is significantly lesser, there are a lot of problems with symmetric cryptography[2-3].

Problem 1: The shared key

The fact that the encryption and decryption is done with one single key is a huge problem. First and foremost, the sharing of the key needs to be done in a very secured manner, if anyone gets hold the of key then all our data will be compromised.

Problem 2: It is not scalable

Another huge problem with symmetric cryptography is that it is not scalable at all. Suppose Alice runs an information center and sends data via symmetric key cryptography. It's ok if she is only dealing with 3-4 clients. But the most clients she gets, the more unique public keys she will have to handle and take care of. Eventually, it will become too much to handle. Because of these vulnerabilities of symmetric key cryptography, a solution was needed, and in the 1970's it finally came in the form of Public key cryptography (Asymmetric key cryptography).

ASYMMETRIC KEY CRYPTOGRAPHY

Public-key encryption is a cryptographic system that uses two keys -- a public key known to everyone and a private or secret key known only to the recipient of the message

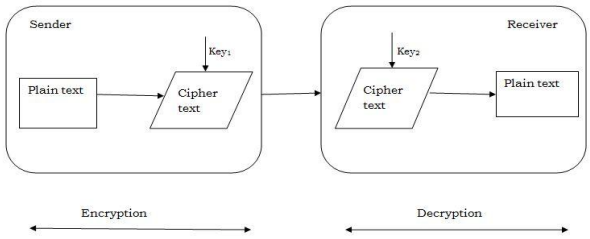

*Figure2: A*symmetric key cryptosystem

An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if we know the public key.

An asymmetric key cryptosystem is shown at figure 2. In this asymmetric key cryptography, two people should mutually accept on a cryptosystem to generate two different keys, namely, public key and private key. The public key of a user (key1) is publicly available. Therefore, it also known as public key cryptography

As illustrated at figure 2, if a sender wants to send a message to the receiver, then the public key of the receiver is used by sender to encrypt the message. When the encrypted message has been received by receiver, he uses his private key (key2) in order to decrypt that message

The asymmetric key cryptography offers the necessary security services such as authentication, confidentiality, integrity, non-repudiation, access control. These security services offer the secure transmission of a message over the network. Moreover, key distribution problem encountered by symmetric key cryptography is avoided by this asymmetric cryptosystem.

This cryptography offers exclusive applications such as digital signature and encryption. The digital signature application is a remarkable feature to send authorized message securely over the network. A genuine public key is required to verify the digital signature of a user. Therefore public key authentication is crucial to perform successful applications using digital signature. Many protocols like SSH, S/MIME, and SSL/TLS uses asymmetric key cryptography for encryption and digital signature functions. Blockchain system uses hashing and digital signature.

HASHING AND DIGITAL SIGNATURE

Hashing is a cryptographic method for transforming large amounts of data into short numbers that are difficult to imitate. It is a key component of blockchain technology and is mainly concerned with the protection and integrity of the data flowing through the blockchain.

This method is mainly used for four processes:

- to verify and validate the account balances of wallets
- to encode wallet addresses
- to encode transactions between wallets
- to make the mining of blocks possible (for mineable cryptocurrencies) by creating the mathematical puzzles that need to be solved to solve a block

A digital signature, similar to our own signature, is used to verify that we are who we say we are. When it comes to cryptocurrencies, digital signatures are mathematical functions that are matched to a specific wallet.

Thus, they function as proof that a specific wallet is actually the wallet it claims to be – essentially, it's a digital identification of a wallet [6-10]. By attaching a digital signature to a transaction, no one can dispute that that transaction came from the wallet it purports to have come from, and that wallet can't be impersonated by another wallet.

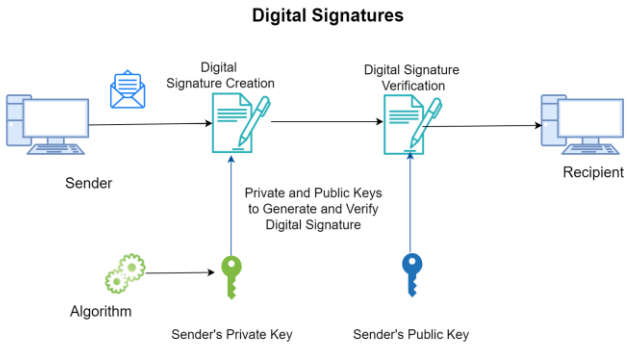

Figure3: Digital signature

Digital signatures use cryptography for wallet identification and secretly match the public and private key of a wallet. Our public key is basically our bank account number, while our private key is the pincode. It doesn't matter if people know our bank account, because the only thing they can do with it is deposit money to our account. However, if they know our pincode too, we can have a real problem.

In blockchain, the private key is used for the encryption of transactions, while the public key is used for the decryption. This is possible because the sending party is the one responsible for a transaction. The sending party encrypts the transaction with their private key, but this can be decrypted with the recipient's public key because they only need to verify that it was indeed we who sent the message. If the sending party's public key doesn't work to decrypt the transaction, then the transaction isn't from that wallet.

INTRODUCTION TO BLOCKCHAIN SYSTEM

Blockchain is a technology that can allow individuals and companies to make instantaneous transactions on a network without any middlemen. Transactions made on blockchain are completely secure. The function of blockchain technology is kept as a record of what happened. Cryptographic encryption algorithms ensure that no record of a transaction on blockchain can be altered after the fact.

A blockchain without internet is nothing [5]. The initiation of electronic transactions is preferable , but physical money holds equal significance in case of internet failure. Different network speeds in varied locations is a key factor that affects blockchain. A remote place with slow internet may find it difficult to adopt this tech. Internet Service Providers (ISPs) have the power to control the transmission rate of packets from one layer to another. We can say that the number and speed of packets transmitted and received can be varied thereby making blockchain perform poorly. Here comes another issue that is of net-neutrality, which if it ends, will promote discrimination towards different blockchain applications.

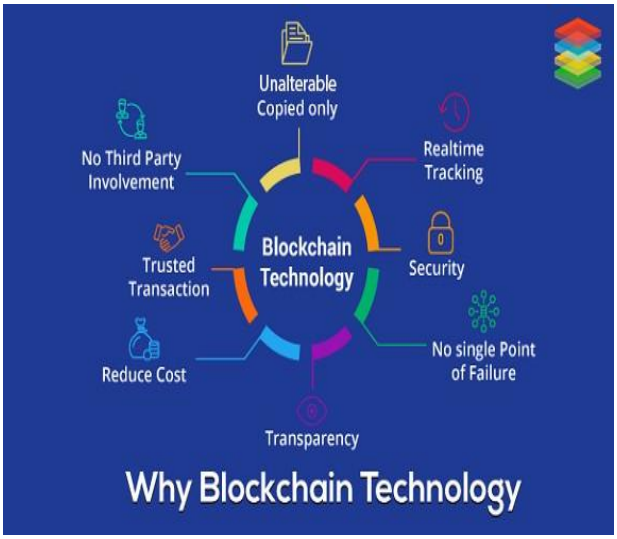

Figure 4: why blockchain technology

Blockchain fetches within itself the idea of privacy with the help of cryptography. It is able to provide privacy to its users effectively because it provides a highly encrypted network. But this leads to another problem. Privacy does help in anonymous transmission of information but in case of any discrepancy there is nothing that can be done. No one knows from where the information is coming and where it is going. If someone steals my Bitcoins, cyber police is completely helpless because of the huge amount of encryption and decentralization. On the other hand, although anonymous, all information is shared in a public ledger. Everything that is recorded by the blocks can be viewed by anyone and everyone.

The following are some important features of blockchain system

1. Blockchain will keep score of all type of data exchanges. This is called a ledger system, and the data exchanges are called 'transactions.' After verification, every transaction gets to add up to the ledger as a block.
2. It uses a different kind of distributed network to ensure that every transaction is on the point between P2P nodes.
3. After a block gets added and verified, no one can alter its information.

BLOCKCHAIN WORKING PROCESS

Blockchain ensures security in this network by using the concept of 'Key.' If we use a set of encrypted keys we will get a unique identification that no one can break. We will get a private and public key, using this combination we will get a unique identity [4].

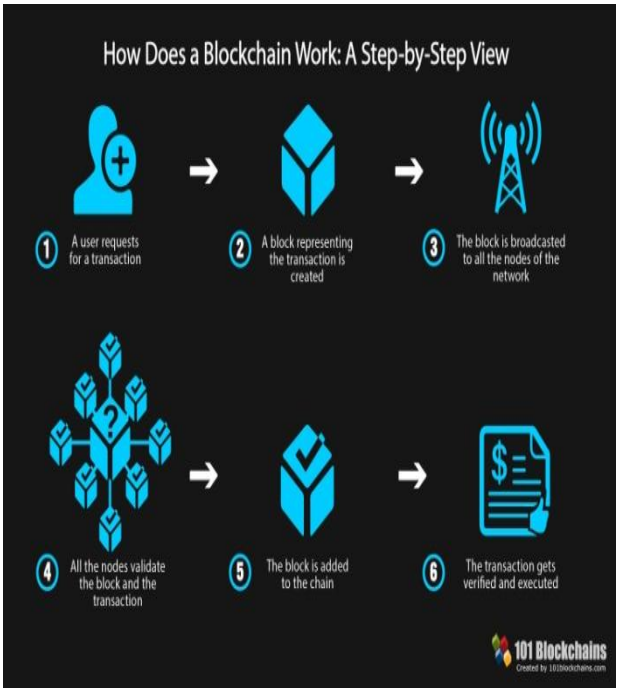

Figure 5: blockchain technology step by step view

Others will use our public key to find us on the network. With the help of our private key, we will be able to sign any action or authorize transactions associated with our public key.

If we think about cryptocurrencies, then the public key will get used as our wallet address, and we will use the private key to withdraw, send or buy digital money. That's why it's essential for us to keep this key safe.

If someone gets their hands on our private key, then he/she could access all our digital assets and misuse it.

So, every time we send something over the network, we will authorize it. It might be something like "Todd is sending Jamie 2 BTC", this will include the public key of Jamie to locate him and Todd's public and private key to encrypt the transaction.
After the transaction, the system nodes will verify it, and it will get added to the ledger with the help of a unique id and time frame.

In short, every transaction will have the same features, a public key, digital signature, unique ID and the timestamp.

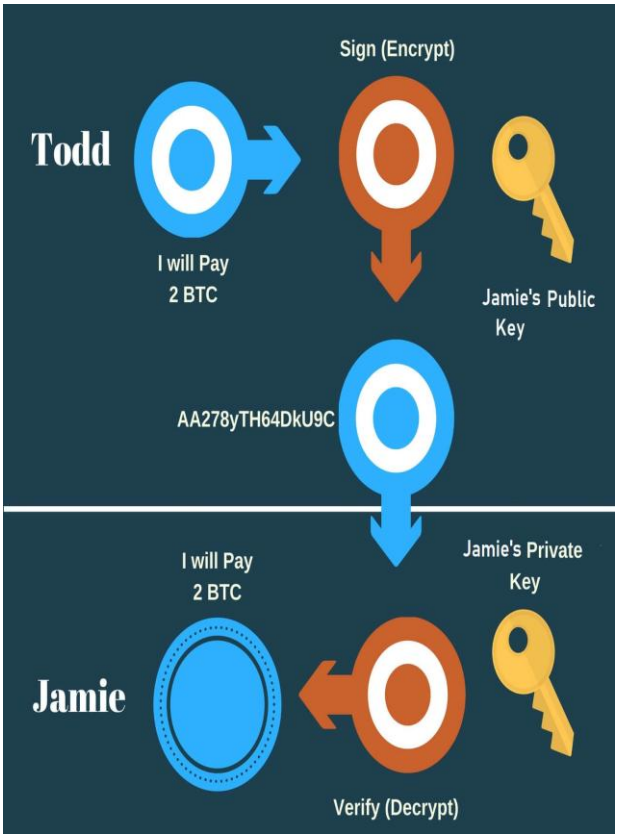

Figure 6: blockchain technology working process

The public keys don't have any recognizable sequence, we won't be putting our name there. It will consist of random letters and numbers. That's why no one can trace it back to us or vice versa.
We will also get to generate as much as keywords as we want and come up with new key pairs along the process.
No system is 'unhackable' on the internet. But lockchain makes sure that it's one of the most secured ones so far. Many industrial farms verified this statement including the Northwest Passage Ventures. It doesn't work like traditional means like banks, so to hack it we have to hack all the computer using it. The process is utterly tricky, and that's why it's considered extremely secured.

To compute all the resources, hackers have to face many challenges, because of the vast number of computers.
Just like any other technology, blockchain has a long way to go. However, if we compare Blockchain versus Centralized platforms, blockchain will surely win.

CONCLUSION

Blockchain technology can be integrated into multiple areas. The primary use of blockchain today is as a distributed ledger for cryptocurrencies, most notably bitcoin. Businesses have been thus far reluctant to place blockchain at the core of the business structure. The public key cryptography is mixed in this technology to make the system very secure.

REFERENCES

1. Schneier, Bruce. Applied cryptography. Ed 2nd., JohnWiley & Sons, New York, 1996.
2. https://blockgeeks.com/guides/cryptocurrencies-cryptography/
3. https://www.blockchain-council.org/blockchain/how-does-blockchain-use-public-key-cryptography/
4. https://101blockchains.com/ultimate-blockchain-technology-guide/
5. https://blog.unocoin.com/what-factors-are-influencing-blockchain-technology-300de42a9e05
6. Srinivas Aluvala, K.RajaSekhar, Deepika Vodnala," Analysis of Security Threats and Issues in MANETs, International Journal on Advanced Computer Theory and Engineering, JUN, 2015,vol.4, issue 5, ISSN: 2319-2526
7. Dr. R.Vijaya Praksah and T.Dhanalaxmi " A Survey on Secure and Privacy-Preserving Information Brokerage System Against Intruders" International Journal of Computer Applications and Engineering Technology, Volume 4,issue 1, JAN, 2015, ISSN: 2277-7962.
8. Rajesh Mothe and P.Kumaraswamy "Secure Message Authentication In Pervasive Computing" International Journal For Technological Research In Engineering, Volume 3, Issue 4, December-2015, ISSN : 2347 – 4718
9. Y.Chanti, Dr.Seena Naik, M.Rajesh, Y.Nagender and B.swathi " A modified Elliptic Curve Cryptography Technique for Securing Wireless Sensor Networks", International Journal of Engineering & Technology, Volume 7,issue 8, December, 2018,ISSN: 2227-524X
10. P.Kumaraswamy, Dr.C.V..Guru Rao and Dr.V.Janaki" Functioning of secure key authentication scheme in Public key cryptography", International Journal of Pure and Applied Mathematics, Volume 118,issue 14, March,2018,ISSN: 1314-3395.