IJFEAT

INTERNATIONAL JOURNAL FOR ENGINEERING APPLICATIONS AND TECHNOLOGY

TITLE: BLOCKCHAIN TECHNOLOGY AND CRYPTOCURRENCY

Ashanka nutpelliwar[1], Bhagyashri tete[2], Chitrakshi Gatkine[3], Shivani Range[4]

[1]*Student, department of IT, Jawarharlal Darda Institute Of Engineering &Technology,Maharashtra, India,* ***nutpelliwarashanka@gmail.com***

[2]*Student, department of IT, Jawarharlal Darda Institute Of Engineering &Technology,Maharashtra, India,* ***bhagyashri_tete@yahoo.com***

[3]*Student, department of IT, Jawarharlal Darda Institute Of Engineering &Technology,Maharashtra, India,* ***chitrakshi19gatkine@gmail.com***

[4]*Student, department of IT, Jawarharlal Darda Institute Of Engineering &Technology,Maharashtra, India,* ***rangeshivani0@gmail.com***

Abstract

A blockchain can be referred to as a collection of records or open record that gets shared amongst participating parties. Every transaction that gets incorporated is first verified by all the participants of that transaction. Once the data gets recorded by the blockchain, can never be rewritten or changed. Thus the blockchain can be termed as a record book of all the transactions held. Cryptocurrencies, the decentralized bitcoin or say ethereum which can be termed as peer to peer computerized cash also uses the blockchain technology. Security is about the protection of assets. Data security refers to protective digital privacy measures that are applied to stop unauthorized access to computers, personal databases and websites. Cryptography protects users by providing functionality for the encryption of knowledge and authentication of other users. Compression is that the process of reducing the amount of bits or bytes needed to represent a given set of knowledge . It allows saving more data. Cryptography may be a popular ways of sending vital information during a secret way. The scenario of present day of data security system includes confidentiality, authenticity, integrity, non repudiation No key is used in this algorithm. A fixed-length hash value is computed as per the plain text that creates it impossible for the contents of the plain text to be recovered. Hash functions are also used by many operating systems to encrypt passwords.. The security of communication may be a crucial issue on World Wide..

Index Terms: ***Blockchain, Bitcoin Encryption and decryption, Compression, hash function, Cryptography***

---------- *** ----------

1. INTRODUCTION

Bitcoin, the world"s commonest and accepted cryptocurrency, has been increasing in popularity. It has an equivalent basic structure because it did when created in 2008, but repeat instances of the planet market changing has created a replacement demand for cryptocurrencies much greater than its initial showing. By employing a cryptocurrency, users are ready to exchange value digitally without third party oversight. The word cryptography has come from a Greek word, which suggests secret writing. In the present day context it refers to the tools and is received techniques wont to make messages secure for communication between the participants and make messages resistant to attacks by hackers. For private communication through public network, cryptography plays a really crucial role. The role of cryptography are often illustrated with the assistance an easy model of cryptography as shown in Fig. The message to be sent through an unreliable medium is understood as plaintext, which is encrypted before sending over the medium. The encrypted message is

understood as cipher text, which at the opposite end of the medium and decrypted to urge back the first plaintext message. In this lesson. Cryptography algorithms based on

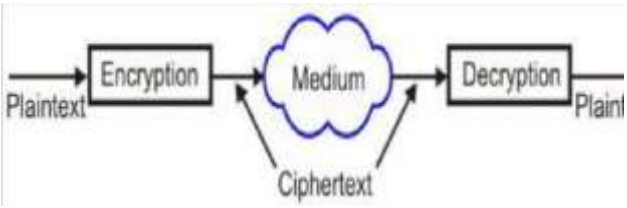

Fig-1: A simple cryptography model

symmetric key cryptography are addressed and public key cryptography are addressed.

2: SYMMETRIC KEY CRYPTOGRAPHY

Symmetric encryption may be a sort of encryption where just one key (a secret key) is employed to both encrypt and decrypt electronic information. The entities communicating via symmetric encryption must exchange the key in order that it are often utilized in the decryption process. This encryption method differs from asymmetric encryption where a pair of keys, one public and one private, is used to encrypt and decrypt messages. Symmetric key ciphers are valuable because:

• It's relatively inexpensive to supply a robust key for these ciphers.

• The keys tend to be much smaller for the extent of protection they afford.

The algorithms are relatively inexpensive to process

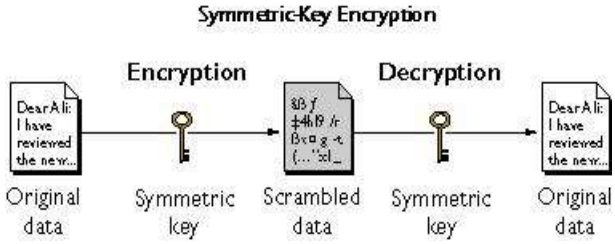

Fig-2: Symmentric Key Encryption

By using symmetric encryption algorithms, data is converted to a form that can't be understood by anyone who doesn't possess the key to decrypt it. Once the intended recipient who possesses the key has the message, the algorithm reverses its action in order that the message is returned to its original and understandable form. The secret key that the sender and recipient either use might be a selected password/code or it are often random string of letters or numbers that are generated by a secure random number generator (RNG). For banking-grade encryption, the symmetric keys must be created using an RNG that is certified according to industry standards, such as FIPS 140-2.

3: ASYMMENTRIC KEY CRYPTOGRAPHY

Asymmetric key cryptography algorithm is additionally called Public key cryptography algorithm. This algorithm uses a pair of keys for encryption and decryption. Public key encrypts the data and corresponding private key or secret key for decryption. It is computationally infeasible to deduce the private key from the public key; anyone who has a public key can encrypt the data but cannot decrypt it. Only the person who has the corresponding private key can decrypt the data. The need for the sender and receiver to share secret key via some secure channel is eliminate; all communication involved only public key, and no private key's ever transmitted or shared. RSA implements a Public key cryptosystem, also as digital signatures. This algorithm is based on the mathematical fact that is easy to find and multiply large prime numbers together, but it is extremely difficult to factor their product. The private and public keys in RSA are supported very large prime numbers. It is the selection and generation of the public and private key. This algorithm involves the use of two keys: (i) A public key which may be known b anybody and can be used to encrypt message. (ii) A private key, known only by the recipient and used to decrypt message. SRNN algorithm is analogous with RSA with some modification and included more security. This algorithm we've extremely sizable amount that has two prime factors. In addition of this algorithm we have used to two short range natural numbers in pair of keys. This modification increases the security of the cryptosystems.

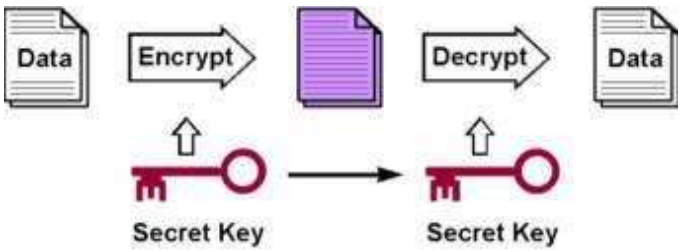

Fig-3: Public-key cryptography

Public-key cryptography, or asymmetric cryptography, could also be a cryptographic system that uses pairs of keys: public keys, which may be disseminated widely, and private keys, which are known only to the owner. The generation of such keys depends on cryptographic algorithms supported mathematical problems to supply one-way functions. Effective security only requires keeping the private key private; the overall public key are often openly distributed without compromising security.In such a system, a person can encrypt

a message using the receiver's public key, but that encrypted message can only be decrypted with the receiver's private key.

4. BENEFITS

Bitcoin has strength intentionally to form it a viable currency that has elevated it in status over the years, more notably the fixed limit of bitcoin which will exist. Bitcoin are going to be mined with diminishing returns every four years until the utmost number of bitcoins are reached: a complete of 21 million (King, 2013). This aspect of Bitcoin is vital for its value. Due to the limited amount of bitcoins, it will never become inflated from an overabundance of bitcoins. Also, bitcoin and other cryptocurrencies are generally thought to be being protected against inflation originating from national government changes or restrictions (Margo, 2016). This creates a "safe haven" for investors to place their wealth into, because it generally doesn't lose value supported inflation. Bitcoin is quickly showing its strength as a refuge against inflating national currencies. However, as is the case with most commodities, the price can fluctuate wildly based on many other external factors. The combination of demand for a secure haven option and its price volatility helped Bitcoin to become the simplest performing currency of 2015 using the US Dollar Index (Desjardins, 2016). This means that Bitcoin was the highest valued currency in the entire world at the end of last year. This is no small feat in a global economy with powerhouses like China and the United States running the landscape. A strength of our analysis is that we take under consideration the prices of operating a cryptocurrency that prohibits double-spending. This allows us to quantitatively assess how efficient Bitcoin as a medium of exchange can be relative to existing means of payment. Calibrating our model to Bitcoin data, we find that from a social welfare perspective using Bitcoin is close to 500 times more costly than using traditional currency in a low inflation environment. This is, however, a result of the inefficient design of Bitcoin as a cryptocurrency. Bitcoin uses both currency growth and transaction fees to get rewards for mining. In its current form, the cryptocurrency reward structure is too generous so that too many resources are being used to rule out double-spending and making it a secure form of payment. We show that the optimal way of providing rewards for mining is exclusively via currency creation at a really low rate instead of by using transaction fees. The optimal design of Bitcoin would generate a welfare cost of only about 0.08% of consumption which is equivalent to a cash system with moderate inflation. • No Third-Party Seizure: No central authority can manipulate or seize the currency since every currency transfer happens peer-to-peer a bit like cash . In particular, bitcoins are yours and only yours, and therefore the central authority cant take your cryptocurrency, because it doesn't print it, own it, and control it correspondingly. • Anonymity and transparency: Unless Bitcoin users publicize their wallet addresses publicly, it is extremely hard to trace transactions back to them. However, even if the wallet addresses was publicized, a new wallet address can be easily generated. This greatly increases privacy in comparison to traditional currency systems, where third parties potentially have access to non-public financial data. Moreover, this high anonymity is achieved without sacrificing the system transparency as all the bitcoin transactions are documented in a public ledger. • No taxes and lower transaction fees: Due to its decentralized nature and user anonymity, there is no viable way to implement a Bitcoin taxation system. In the past, Bitcoin provided instant transactions at nearly no cost. Even now, Bitcoin has lower transaction costs than a credit card, Paypal, and bank transfers. However, the lower transaction fee is only beneficial in situations where the user performs a large value international transaction. This is because the average transaction fee becomes higher for very small value transfers or purchases such as paying for regular household commodities. • Theft resistance: Stealing of bitcoins isn't possible until the adversary have the private keys (usually kept offline) that are related to the user wallet. In particular, Bitcoin provides security intentionally, as an example, unlike with credit cards you don't expose your secret (private key) whenever you create a transaction. Moreover, bitcoins are free from Charge-backs, i.e., once bitcoins are sent, the transaction can't be reversed. Since the ownership address of the sent bitcoins will be changed to the new owner, and it is impossible to revert. This ensures that there's no risk involved when receiving bitcoins.

5. CHALLENGES

High energy consumption: Bitcoins blockchain uses PoW model to realize distributed consensus within the network. Although, the utilization of PoW makes the mining process more immune to various security threats like Sybil and double spending, it consumes a ridiculous amount of energy and computing resources. In particular, processing a bitcoin transaction consumes quite 5000 times the maximum amount energy as employing a Visa MasterCard, hence innovative technologies that reduce this energy consumption are required to ensure a sustainable future for Bitcoin. Furthermore, due to the continuous increase in network load and energy consumption, the time required for transaction processing is increasing. • Wallets can be lost: Since there is no trusted third party if a uses lost the private key associated with her wallet due to a hard drive crash or a virus corrupts data or lost the device carrying the key, all the bitcoins in the wallet has been considered lost for forever. There is nothing that can be done to recover the bitcoins, and these will be forever orphaned in the system. This can bankrupt a wealthy Bitcoin investor within seconds. • (Facilitate) Criminal activity: The

considerable amount of anonymity provided by the Bitcoin system helps the would-be cyber criminals to perform various illicit activities such as ransomware,tax evasion, underground market, and money laundering.

6. CONCLUSION

The future of blockchain technology will still drive cryptocurrency wallet application development. This technology adds security, transparency, and convenience to several financial transactions. Plus, its applications continue to expand. Bitcoin may be a cryptocurrency which will be used for any online retailer through Cryptopay, a Bitcoin open-end credit . Plus, many online retailers accept Bitcoin for payment.

As the number of digital wallet apps continues to rise, users will continue to utilize these apps to cut out intermediate financial arbiters and quickly receive and send digital currency with ease. This fact alone is groundbreaking, particularly for users that don't utilize banks, and for several international transactions that would be difficult without the utilization of a digital wallet. There is little question that blockchain technology is an innovative tool which will make it much easier to navigate the planet of cryptocurrency.

REFERENCES

[1]. Peter D. DeVries Professor of MIS University of Houston – Downtown One Main Street, FAMIS Department, B428, Houston, TX 77002 United States of America, An Analysis of Cryptocurrency, Bitcoin, and the Future

[2]. K. Sheela1 , E. George Dharma Prakash Raj, InKeSi-Increased Key Size Method in SRNN Public Key Cryptography Algorithm

[3] Jonathan Chiu† Bank of Canada Thorsten V. Koeppl‡ Queen's University, The Economics of Cryptocurrencies – Bitcoin and Beyond

[4] Mauro Conti, Senior Member, IEEE, Sandeep Kumar E, Member, IEEE, Chhagan Lal, Member, IEEE, Sushmita Ruj, Senior Member, IEEE, A Survey on Security and Privacy Issues of Bitcoin