

Crypto Currency System for Protecting Social Media by Cryptography

D.A. Agnes Archana , Y.Bhuvaneshwari, S. Suseela

#1 Student of IIIrd Year CSE , Department of Computer Science and Engineering, Periyar Maniammai Institute of Science and Engineering, Vallam. TamilNadu. India. kmuagnesarchana@gmail.com

#2 Student of IIIrd Year CSE , Department of Computer Science and Engineering, Periyar Maniammai Institute of Science and Engineering, Vallam. TamilNadu. India. ybhuvana7@gmail.com

#3 Assistant Professor, Department of Computer Science and Engineering, Periyar Maniammai Institute of Science and Engineering, Vallam. TamilNadu. India. suseelass@gmail.com

Abstract— In the present day, Crypto Currency is a digital currency to exchange like common currencies, digital information, method prepared likely by principles of Cryptography to protect the transactions and Control the creation of new coins. The currency system requires a number of ways to manage supply and enforce different security properties to avoid cheating. Privacy and authentication are the key concern of world recently through social media like transaction, email, chat, conferencing, and telephone calls. Cryptography provides a method for safely encoding a crypto currency system. Crypto currencies that prevent people from tampering with the system and from equivocating to encode, in a mathematical protocol, for creation of new units of the currency. Bit coin only a handful of simple cryptography constructions. In this paper, study cryptography and digital signatures, two primitives that prove to be useful for building crypto currencies. This paper mainly focuses on the current development functioning using that social media influences the crypto currency and block chain.

Keywords— Cryptography, Encryption, Protection and Privacy, Crypto currency, Bitcoin, Blockchain, Social media.

I. INTRODUCTION

Crypto systems, is a Cryptology such as two branches are Cryptography and Cryptanalysis. Cryptography is the plan of cryptosystems, at the same time as cryptanalysis the breaking of cryptosystems The ability and knowledge of building a cryptosystem that is skilled of provide information protection is Cryptography. Information security services that

a mathematical principles in storing and transmitting information in the exacting form can read and development it. Encryption is a critical tools used in cryptography. It is a message can be prepared unreadable for an unintended person who reading by the sender and the recipient. Crypto currencies and Cryptography as shown in Fig 1. A communication isdfbf plaintext using a message as to hide its core is encryption. An encrypted message is ciphertext using back into plaintext is decryption. It is to secure important data on the hard disk or as it passes through that may not be secure itself.

Crypto currencies like Bit coin use a peer-to-peer decentralized method to perform transactions and control of crypto currency through circulated ledger tools, a blockchain, that provides as a public financial transaction database. Bit coin, first released as open-source software in 2009, is the first decentralized crypto currency. [2]

In this paper, we discuss a Crypto Currency System for Protecting and avoid cheating in Social Media by Cryptography. Then the history of cryptography are illustrated in Section 2. In Section 3 we discuss the fundamental concept of cryptography. Section 4 discusses the types of crypto currencies and cryptography algorithms. social media influences the crypto currency and block chain in Section 5. Finally, we have concluded the paper in Section 6.

II. HISTORY OF CRYPTOGRAPHY

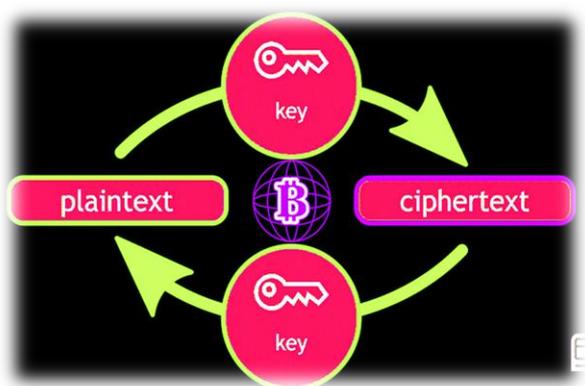


Fig 1. Crypto currencies Cryptography

have fundamental the aim basic on mathematical algorithms are the real securing of digital information. Cryptanalysis is the knowledge of breaking the cipher text and involves cryptography with the purpose to break them. It is the branch of cryptography and co-exist. The cryptography method outcome in the cipher text for transmission or storage.[1] it is

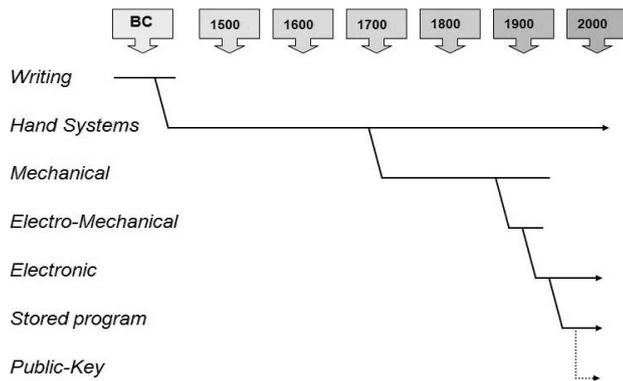


Fig 2. History of cryptography

The cryptography Fig.2. shows history is very essentially goes support a variety of centuries. cryptography was the Caesar cipher encryption process. nowadays, Public still use this method.

Then, encryption methods in instance for World War I, include the One-Time Pad (OTP) that was first developed in 1917, The OTP is permanent forms of encryption. In World War II, once more Encryption made in the 1920s, with the upgrading of automatic cipher systems. encryption these systems were better plans used perfectly like they were approved. For profitable systems, a financial transaction switched from the consumer to the bank. (1980s) of cash equipment or ATM's, trade who found invalid transactions using these machines. cryptography in their plan, businesses happening to take security, and overall from the Internet, cell phones, pay-TV and other networked services ongoing to incorporate. In 1990, the use of the web for a well-known usual for encryption for profitable purposes and the introduction of business transactions more than the Internet. pending 1996 U.S. of cryptography using 40 bits was incomplete. Later in 1998, Nick Szabo created his own cryptocurrency known as "Bit Gold". now 2004, former administrator new laws not in favor of unrestricted use of encryption. it is planned for can examine and development the word cryptography comes from the Greek words are Kryptos (hidden) and Graphein (writing). It is a science of protecting information by encoding it into an unreadable plan, approach of protecting responsive information as it is stored on media or transmitted through set of connections message.

it is about building and analyzing that overcome the manipulate in information security such as information confidentiality, data integrity, and authentication.

These Security services are,

A. Confidentiality - ensuring the privacy of message.
Example: Printing, other forms of disclosure and displaying.

B. Non-repudiation - A method to prove that the sender actually sent this message. if Alice signs the message she cannot reject later that she sent it, for the reason that no one else could make that same name.

C. Integrity checking - Assuring the receiver that the received message has not been changed in any way from the unusual. Alice can make a checksum of the message. Bob can either remove it from the message it and authenticate that the communication has not been misused.

D. Authentication - Alice can indication her communication and Bob can verify that she sent it based on this name. The method of proving one's individuality.

E. Key exchange - The way by which crypto keys are shared between sender and receiver.[3]

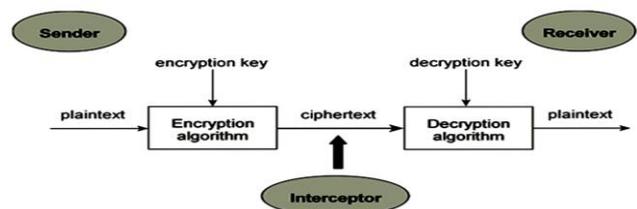
III. FUNDAMENTAL CONCEPT OF CRYPTOGRAPHY

Cryptography be capable of rearrangement and change our information, building it safer on its journey between PCs. It is an performance of cryptography methods and to make available information protection services. a cipher system is also known as a cryptosystem. Only the sender and the receiver will be familiar with the plaintext is the aim of cryptosystem the process. The equipment is supported on the fundamentals of secret codes, improved by new mathematics that protects our information in controlling systems.

1. Computer Security - common name for the group of tools planned to keep information and to prevent hackers
2. Internet Security - procedures to keep information through their communication more than a set of interconnected systems
3. Network Security - procedures to protect information during their communication.

The security requirements of the executive dependable for protection desires a few logical method of essential the requirements, an association in effect, for safety and description of advances to assure those conditions.

1. Security service - The services are planned to respond to protection attacks and to give the service. the protection of the information developmenting systems and it is



moves of a business.

Fig 3. Basic concept of Cryptography

2. Security attack – The security of information any accomplishment that cooperations hold by a business.
3. Security mechanism – It is planned to identify, avoid or improve from a protection attack.[4]

Fig.3. contains Encryption is the method in which information is changed into rather that looks to be chance and empty. Decryption is the development in which the determined information is changed support to its unique structure. Previously the information has been encrypted, it can be stored on lacking confidence media or send out on an insecure network (i.e. Internet) .so that it cannot be read by anyone except the planed receiver. encrypt (encipher) and decrypt (decipher) information is the science of Cryptography..a sender who requests to move a few responsive information to a receiver any gathering intercepting or spying on the message control cannot remove the information. This components are,

- A. Plaintext - It is the information to be kepted for the period of communication. It is a group of all achievable decryption keys is called a key space.
- B. Ciphertext - The ciphertext is not safeguarded. It preserve be intercepted by everyone who has contact to the message channel.It runs on unrestricted channel. It is the twisted description of the plaintext created by the encryption algorithm by means of a particular the encryption key.
- C. An interceptor (an attacker) is an illegal individual who efforts to resolve the plaintext.It can be see the ciphertext and can identify the decryption algorithm. on the other hand, must never know the decryption key.
- D. Encryption Key - It is a importance that is identified to the sender. The sender enters the encryption key into the encryption algorithm with the plaintext to calculate the ciphertext.
- E. Decryption Key - It is a value that is recognized to the receiver. The decryption key is linked to the encryption key, but is not constantly the same to it. The receiver enters the decryption key into the decryption algorithm with the ciphertext to calculate the plaintext.
- F. Encryption Algorithm - It is a mathematical process that produces a cipher text for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a cipher text.
- G. Decryption Algorithm - It is a mathematical method, that makes a exclusive plaintext for any specified ciphertext and decryption key. It is a cryptographic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext. The decryption algorithm basically invalidates the encryption algorithm and is hence strongly connected to it. [5]

IV. TYPES OF CRYPTOCURRENCIES AND CRYPTOGRAPHY ALGORITHMS

Usually currencies are charged supportd on assets like gold, policies of banks and governments.then, regulating agency or assets are in place, the value of the crypto-currency is establishd by the advertise. "blockchains" and "open ledger" are joined to crypto-currencies . Fig.4 shows types of crypto currencies.

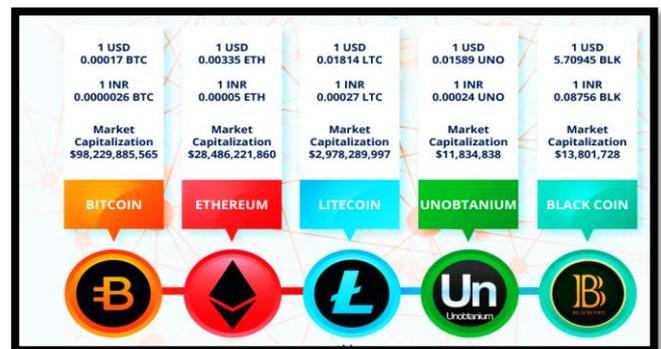


Fig 4. Types of Crypto currencies

A. Bitcoins

It is a well-known brand of digital currency, At a recent trade rate of 3,70,000 INR the value has developed at 750% in just one year.In 2017 It may be 300,000 transactions per day have been made. It first started in 2009 and then crypto-currencies have appeared in the market, some of these are Litecoin, Ripple, Zcash, Ubiq, blackcoin, Ethereum, and Bitconnect. Bitcoin remains to be the most popular type of digital currency global. examples, Bitcoins,using companies like Microsoft and Dell made it b for users to pay for games, apps, and videos by counting money to their accounts. *Fact:* Bit coin is the original cryptocurrency with the most liquidity and brand name recognition with an eight-year track record.

B. Ethereum

crypto-currency, Ethereum is used to transactions with users, that is peer to peer transactions. Ethereum is slowly move slowly to Bitcoin.

C. tecoin

Litecoin operated in a same capacity to its social group like ethereum. It is to conduct smaller transactions like small amount times using Litecoin, making more people to contribute using smaller amounts of money in faster transactions.

D. Unobtanium

A enter element of cryptocurrencies is mining. It is set number of coins that exist in the crypto-currency framework. The rising value of cryptocurrencies, Complex algorithms that get more difficult with the process of mining.

E. Black Coin

A shorter conformation time transactions using Blackcoin much faster. It relies on a system to verify transactions. Then, users stake coins from their slips on the correct to prove the next transaction. [6]

Algorithms

For purposes it will be classified supported on the amount of keys that are in use for encryption and decryption. Fig 5. Contains The three types of algorithms are there,

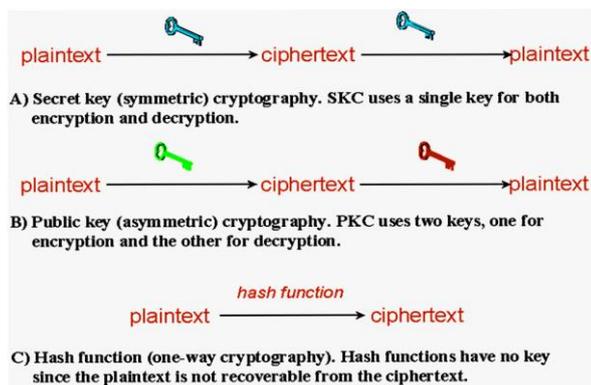


Fig 5. Algorithm of Cryptography

A. Secret Key Cryptography (SKC):

It uses its own key for both encryption and decryption. Mostly used for privacy and confidentiality. It is also called symmetric encryption.

B. Public Key Cryptography (PKC):

It uses one key for encryption and another for decryption. Mainly used for verification, non-repudiation, and key replacement. It is also called asymmetric encryption.

Advantages:

- entity is used in the two of a kind of keys.
- It requires the whole keys are small.

Disadvantages:

- lengthy messages is not possible.
- relationship between an entity and its public key must be established.

C. Hash Functions:

It uses a mathematical change to permanently "encrypt" information, providing a digital fingerprint. Mostly used for communication integrity. [7]

V. SOCIAL MEDIA INFLUENCES THE CRYPTO CURRENCY AND BLOCKCHAIN

Crypto currency is a trending term referring to digital currency that can be cryptography for security measures, purchased, transferred, sold securely by cryptography, which encrypts and keeps the data used to help track cryptocurrency transactions. Unlike currency, which exists is backed by like gold, cryptocurrency is purely digital currency in the internet. Additionally, cryptocurrency, is crypto coin, is not managed by an authorized third party like a bank or government. Public and private keys are used to transfer cryptocurrency.

Social media to impact companies in deep ways. Its cryptocurrency and blockchain tools. A large amount of cryptocurrency can be credited to social media is development and reputation. This relationship between social media, cryptocurrency and blockchain maintains to develop in innovative and stimulating ways. The influence of as cryptocurrency and blockchain technology blossoms. There are level blockchain-based social groups developing up. From the social environments of digital exchange's early stages to majority social media channels, social media and cryptocurrency have a very secure connection definitely.

Social media channels like Facebook, Twitter, Pinterest, Instagram, and others, cryptocurrency is trending. Social media is of way a no brainer, since social is how most public get their information. This is nothing new to dealers.

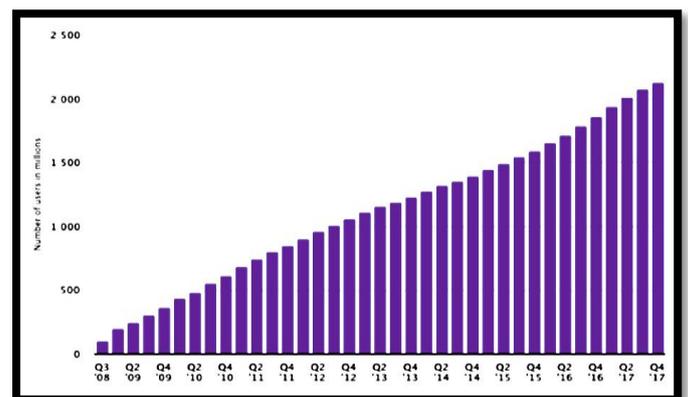


Fig 6. Facebook active users

For example, In Fig 6. shows Facebook is one of the most popular social advertisement choices to contact a great intention viewers. Actually, Facebook is also allowing for cryptocurrency for company development. Cryptocurrency news, and updates to control social media news feeds, the future looks intelligent for crypto-social correlation. It can cause cryptocurrency price changeabilities, for enhanced or

for inferior. Trending news about a big digital prevalence replace hack can cause a considerable go down in digital

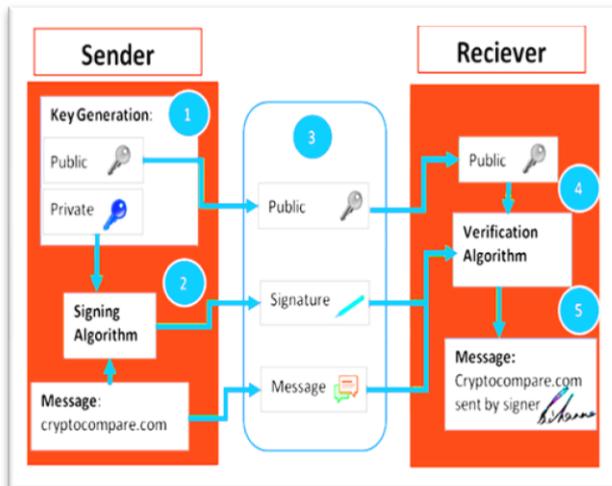


Fig 7. Bitcoin process

currency value. For example, when Hong Kong supported trade Bitfinex was hacked, Bitcoin value drop 20 percent. It gives a big pitfall in the crypto-social bond.[8]

crypto-news you will updated need to twist to social media. For example, Fig 6. Deals with Bit coin can quality of its development to social environment Reddit. It is one of the main social influencer raised areas. From crypto-enthusiasts to crypto-analysts, insight on Reddit. For example, Bit coin and sub reddit has in depth information on the whole thing Bitcoin. It is use a outline of digital signatures to take the process proving that the sender sent the message. i.e. non-repudiation to search the sender can't reject that it was them who sent the message. [9]

VI. CONCLUSION

We have discussed in this paper protecting a crypto currency is a digital or virtual currency that uses cryptography for security. it is hard to counterfeit because of this security feature. Social media hotspots are the first sorting earths for Bitcoin. A block chain, is a increasing list of records, called blocks, which are linked using cryptography. Each block contains a cryptography hash of the before block, a timestamp, and transaction data. The outlook of crypto currency may be all about value slightly particular coin value. Blockchain tools could interrupt the present social media raise. actually the blockchain ideas are great keys to many current

social media points. With possible implementation of blockchain tools in multiple areas, the social influencing crypto currency is being inverted. digital currency and blockchain tools to make its own mark in the social space. Enter blockchain tools. Crypto currency, blockchain can be recognized to social media is development and reputation. It plays a important role finding this information away to the common public. Now there are social media applications planed at using crypto currencies to payment users for spreading information. blockchain tools also transform social media for the better. Facebook is time-consuming, but hit into a useful post every now and then.

REFERENCES

- [1] JustForBeginners, Simply Easy Learning - Introduction of cryptography https://www.tutorialspoint.com/cryptography/modern_cryptography.htm
- [2] Block geeks _The Science Behind Crypto currencies Cryptography <https://blockgeeks.com/guides/cryptocurrencies-cryptography/>
- [3] William H. Saito ,entrepreneur and innovator Cryptography, 2018 https://en.wikipedia.org/wiki/History_of_cryptography <https://saitohome.com/cryptography-101/>
- [4] Prof. D. Chandrasekhar Rao Dr. Amiya Kumar Rath Dr. M. R. Kabat - Protection for cryptography Department of Computer Science and Engineering & Information Technology Veer Surendra Sai University of Technology Burla, Sambalpur, Odisha, http://www.vssut.ac.in/lecture_notes/lecture1428550736.pdf
- [5] Copyright 2015 by Tutorials Point (I) Pvt. Ltd. the science of cryptography and basic concepts https://www.tutorialspoint.com/cryptography/cryptography_tutorial.pdf
- [6] Alisha Rajpal crypto-currencies-types 29th October 2017 [http://www.youthincmag.com/ crypto-currencies-types](http://www.youthincmag.com/crypto-currencies-types)
- [7] Gary C. Kessler, Handbook on Local Area Networks An Overview of Cryptography, 11 August 2018 <https://www.garykessler.net/library/crypto.html>
- [8] Melonie Dodaro, CEO Social Media, Crypto currency and Block chain <https://topdogsocialmedia.com/social-media-cryptocurrency-and-blockchain>
- [9] Antonio Madeira bitcoin cryptography work 29 Jun 2018 <https://www.cryptocompare.com/wallets/guides/how-does-bitcoin-cryptography-work/>