Exploring Bitcoin Cryptocurrency: An Analysis, Applications and its Market Influence

S. Mahaboob Hussain
Vishnu Institute of Technology
Department of CSE
Bhimavaram, Andhra Pradesh

Prathyusha Kanakam
MVGR College of Engineering
Department of CSE
Vizianagaram, Andhra Pradesh

Raghu Varma Edarapalli
MVGR College of Engineering
Department of CSE
Vizianagaram, Andhra Pradesh

ABSTRACT
Being in this digital era, technology continuously updates with new variants in providing security while performing the financial transactions. It is a mandated task for the user for conducting secure transactions in order to defend the intruders to restrict the interference. This paper deals with digital currency- Cryptocurrency, that provides a medium of secure exchange between the peers during financial management. Authors explored the internal scheme of bitcoin and the abstract view of cryptocurrency to know how the bitcoin is providing a shield during financial negotiation between peers with various application in security point of view.

Keywords
Cryptocurrency, Bitcoin, Blockchain, Distributed ledger, Bitcoin wallet

1. INTRODUCTION
To provide strong security measures for e-transactions, a new technology plays its role. Cryptocurrency is an asset in digital format which furnishes an exchangeable medium between peers that participate in the financial transactions. Cryptocurrencies use a decentralized control to immune centralized force electronic money and central banking system. Cryptocurrency is a peer to peer digital exchange system that doesn't require any trusted third party in between them and behaves as decentralized management. Cryptography related to secure sending of currency or messages. So the currency possesses the cryptographic feature to secure the transactions and verifies, validates regularly. See Figure 1.

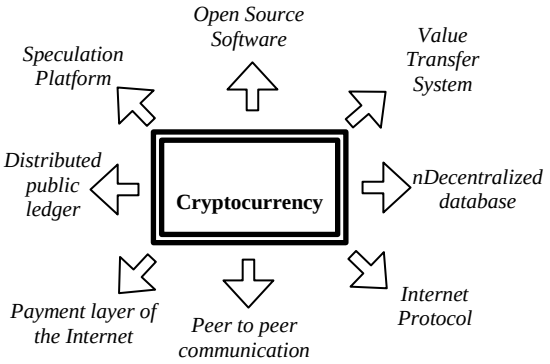

Fig 1: Cryptocurrency centralized control with various parameters and applications

Initially, in 1983 David Chaum originate cryptographic money called e-cash [1][2]. Later he enacted it through DigiCash, which is an early form of cryptographic electronic payments which consists of user software and specific encrypted keys to draw money from banks [3]. It helps to untraceable from others. In 1998, "b-cash", anonymous distributed electronic cash system was introduced by Weidai, immediately was followed by Nick Szabo who created bit gold which uses proof of work [4][5]. It was enhanced as reusable proof of work by Hal Finney.

Satoshi Nakomoto introduced first decentralized cryptocurrency named as bitcoin in 2009. It uses SHA-256 cryptographic function as its proof of work scheme [6][7]. After two years, name coin was created which causes internet censorship more difficult. Thereafter, Litecoin was released, which is the first cryptocurrency uses scrypt as its hash function. Peer coin combines proof of work and proof of stake schemes [8]. IOTA uses tangle instead of blockchain [9].

Before the implementation of the complete picture of cryptocurrency, the electronic payment system requires an additional software for versatile services that includes withdrawing, deposit as well as transferring money between ends. Later they enhanced by incorporating encrypted keys (indulging the cryptographic feature) for e-transactions. Many organizations like DigiCash, Into Space, have to cope up with their individual capabilities in order to render different cryptographic protocols for e-transactions.

2. CRYPTO-CURRENCY
Cryptocurrency is a digital asset that provides a medium of exchange between peers. It employs blockchain technology to avoid the creation of additional monetary units and verifies the fund transferring as well by making use of encryption algorithms. It yields financial inclusion that bears mathematical innovation to serve as a property for making electronic transactions. The cryptocurrency system highly influenced by cryptocurrency units along with their own which is cryptographically satisfied. As it doesn't require any centralized management, all the services should be carried out in a distributed fashion. The ownership of a particular unit should compatible with it. In case of any modification of ownership of the respective unit is encountered, the current owners with that unit are taken into consideration. If same cryptographic unit experienced changes by two different ownership simultaneously, then at most one of them is considered. In the physical systems, while dealing with the money, there are a lot of database entries that the user need to deal with.

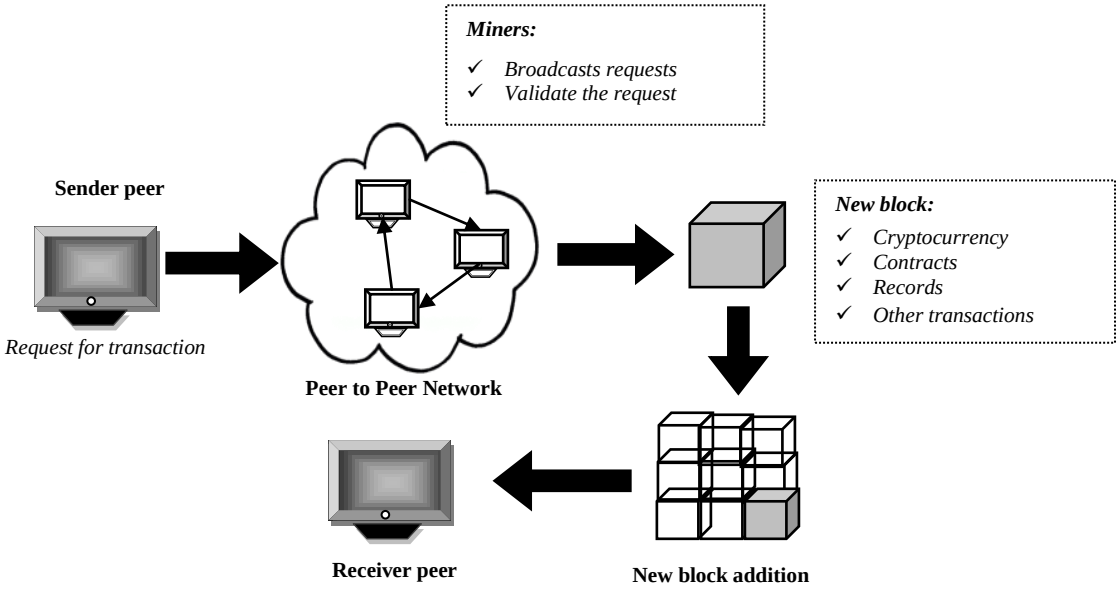

Fig 2: Cryptocurrency peer-to-peer transactions working scheme

When cryptocurrency takes its part in the value communication, it includes the network of peers where each peer has complete information of the transactions and their histories. The working scheme of cryptocurrency fits in five different stages- request, validation, new block creation, incorporating new block, complete as shown in Figure 2.

Sender peer requests for a transaction to the peer network. This request has been sent to peer to peer network where the request broadcasts to all the nodes in the network. Here each node acts as miners where the transaction needs to be validated.

Mining is the crucial part of the cryptocurrency mechanism where the request is validated and confirmed by miners by creating a new block that includes cryptocurrency along with time stamps, contracts, records and other transactions.

Cryptocurrency is the digital commodity used in financial transactions which have the properties like no intrinsic value, no physical form and not determined by the central authority. After the creation of the block, it is incorporated with the previous blockchain to become permanent and unalterable. The completed format will be sent to the receiver.

Table 1 describes the types of crypto-currencies, their attributes - market price, the network on which they operate, algorithm used in their respective scheme. At early stage, bit coin was introduced in 2009 which became a prime model for cryptocurrency. Later in 2011, Litecoin is introduced which operates in its network and uses a separate function- scrypt instead of SHA-256 in proof of work for hashing that requires more memory space and possess slower performance in all types of ideal payments compared to other cryptocurrencies.

Ripple, a privately owned company introduced crypto token in 2012 for validating the transactions and to achieve integrity by making use of its own protocol called consensus [10]. Unlike bitcoin, it operates in a centralized way for computing. Ethereum is the first and foremost distributed computing system which is an open source, programmed with its own language and uses blockchain as its database protocol [11]. Ethereum is energy consumable and relatively slow and the programs smart contracts that written in built-in language are vulnerable to hacking. In 2017, bitcoin cash was implemented that resembles bitcoin by increasing the block size more than 8Mb for enforcing block chain technology.

2.1 Bitcoin

Bitcoin is a cryptocurrency which is in the form of electronic cash. It is a digital currency that depends on the blockchain design that counters all the centralized banking systems.

Its internal design solves the problem of double spending which same single digital token can be spent more than once. To provide security, it uses the mechanism of the distributed ledger where all the transactions are recorded [12].

Table 1. Types of cryptocurrencies with market price and the network

Cryptocurrency	Launched year	Market price	Network	Another name	Algorithm and type of program
Bitcoin	2009	$163 billion	Peer to peer network	NA	Double SHA-256
lite coin	2011	$10 billion	Litecoin Network	alt-coin	scrypt
Ripple (XRP)	2012	$32 billion	Ripple network	Crypto-token called XRP/ Bridge Currency	consensus protocol
Ethereum(ether)	2015	$70 billion	Ethereum network	Native Ether (ETH)	Smart contracts, blockchain
Bitcoin cash	2017	$19 billion	Distributed network	hard fork	proof-of-work

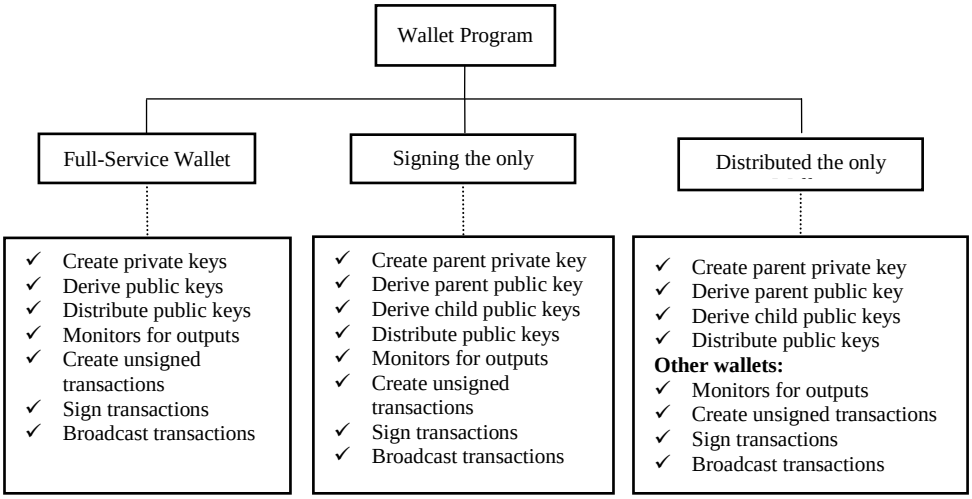

Fig 3: Wallet program functionalities and services

2.2 BitCoin Wallet

As shown in Figure 3, bitcoins are stored in a special program called wallet which consists of two functions- distributing public keys and another for signing the transactions [13]. It is used to generate the address where the address itself called as a public key. For acquiring and broadcasting information purpose, it should be interacted with peer to peer network. Wallet system depends on public key distribution, signing and networked functions. Based on this criterion, wallet programs are of three types- full service, signing only and distributed only. This figure 3 portrays step by step procedure in that respective wallet program. Compared to all the other full-service wallet program is easy to use. But it is prone to attacking the private keys used by the device directly connected to the Internet. In order to overcome the problem, keys are signed by applying hash and also separated by keeping the private keys in a separate wallet. Thus, the signing only wallets provide more security by combining with a networked wallet which interacts with peer to peer network. In the next level, the keys are distributed in order to avoid the reuse of keys.

2.3 Block Chain

The blockchain is the collection of blocks or records which are linked through cryptography and produces the succeeding block by inserting the information resulted from the previous block by applying cryptographic hash on it [14]. Its internal design protects the data from modification by providing a feature of the openly distributed ledger, that stores all the transactions in an efficient and permanent way. Blockchain suites mostly to peer to peer network where each new block of data will be validated and stores the transactions permanently.

Figure 4 depicts the internal structure of blockchain where the previous block is hashed cryptographically that produces a signature which will be inserted to a succeeding block where the hash contains the timestamp and transaction data, which is represented as Merkle tree[1]. In this way, one block of data is linked to another block cryptographically to produce an efficient output block. Thus, it will be more resistant for the modification from the outside world (hacking). Each signature resulted from every block is owned and verified by the miners, acts as peers in the network.

[1] Leaf nodes hold hash of the block and non-leaf node holds cryptographic hash of leaf nodes

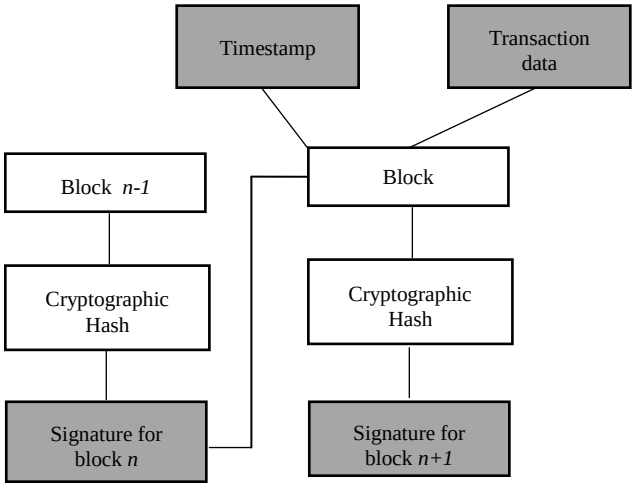

Fig 4: Blockchain secured internal structure

3. APPLICATIONS OF CRYPTOCURRENCY

Cryptocurrency is a digital asset which cannot be altered during its existence and persist as their transactions are recorded in the distributed ledger. Their internal schematic design technology makes them resistant to all types of attacks from the outside world. It gives a counter to all centralized banking systems where the transactions are negotiated between only two peers which are connected through a network. In case of any security issues, applications like semantic forensic are existed to detect the cyber crimes and fraud operations using cognitive predictive task with behavioural patterns on the Web [15].

They have a wide range of applications in various domains.

- *A censorship resistant alternative of wealth*: cryptocurrencies, such as bitcoin , act as a censorship-resistant alternative store of wealth that only the individual with the private keys to the wallet has access to
- *Ethical business practices*: As the blockchain used to record every transaction so that it can lead to strong ethical practices in a business domain.

- *De-corrupting charities*: cryptocurrency can be used to avoid corruption in charitable organizations. Because of its ability to keep companies accountable, blockchain can eliminate many problems occurring with charities, such as fund leaks.
- *Low-cost money transfers*: The most well-known benefit of cryptocurrencies is their ability to send and receive payments at a low cost and at a high speed.
- *Travelling and education*: Due to the explosive growth of the cryptocurrency ecosystem, it is now possible to travel the world and we can pay fees for many universities
- *Fundraising*: Many startups are now using cryptocurrencies in order to fund their ideas, services and products. Instead of using traditional VC funding, or using fund-raising websites
- *Digital publishing engagement*: Digital publishers and advertisers are scrambling to find ways to increase their relevancy with one another.
- *Battling electoral fraud*: By using cryptocurrency, the electoral fraud or any other kind of corruption involving money will no longer be possible

The process of tracing the electoral frauds due to security or authentication issues while performing cryptocurrency transactions will be easy by applying various forensic tools [16]. Some of the application platforms to work with cryptocurrency are mostly open source software(OSS) and consists of a value transfer system with a decentralized database system with an Internet protocol working model. Peer to peer communication is the networking model for all the transactions done in cryptocurrency internal structure.

4. CONCLUSION

To counter all the centralized banking systems, cryptocurrency sets its own path of performing the financial transactions between peer to peer without any third party. Miners verify the transaction produces an unbreakable block of data which does not affect by any kind of modification by the outside world. Out of many cryptocurrencies, bitcoin has the boom in its internal design and the technologies used to construct it. Many other cryptocurrencies are evolving to perform digital secure transactions.

This paper projects a detailed study and analysis of various cryptocurrencies and bitcoin in detail along with its schema. Authors mentioned some of the important applications which play a vital role in understanding the usage of cryptocurrency in business and other industry transactions. Insecurity aspects, authors want to test using cognitive predicting task techniques with behavioural patterns by the intruders on the Web and measure security the level of the bock chain cryptographic hash.

5. REFERENCES

[1] Vincent, Jean-Louis, et al. "Comfort and patient-centred care without excessive sedation: the eCASH concept." Intensive care medicine 42.6 (2016): 962-971.

[2] Chaum, David, Amos Fiat, and Moni Naor. "Untraceable electronic cash." Conference on the Theory and Application of Cryptography. Springer, New York, NY, 1988.

[3] Clark, Tim. "Digicash files chapter 11." CNET News 4 (1998).

[4] Dai, Wei. "b-money, 1998." URL: http://www. weidai. com/bmoney. txt [visited on: 16/08/2018].

[5] Peck, Morgen E. "The cryptoanarchists' answer to cash." IEEE Spectrum 49.6 (2012).

[6] Brito, Jerry, and Andrea Castillo. Bitcoin: A primer for policymakers. Mercatus Center at George Mason University, 2013.

[7] Bonneau, Joseph, et al. "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies." Security and Privacy (SP), 2015 IEEE Symposium on. IEEE, 2015.

[8] Chepurnoy, Alexander, et al. "TwinsCoin: A Cryptocurrency via Proof-of-Work and Proof-of-Stake." IACR Cryptology ePrint Archive 2017 (2017): 232.

[9] Popov, Serguei. "The tangle." cit. on (2016): 131.

[10] Takashima, Ikuya. "Ripple: The Ultimate Guide to the World of Ripple XRP, Ripple Investing, Ripple Coin, Ripple Cryptocurrency, Cryptocurrency." (2018).

[11] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151 (2014): 1-32.

[12] Pilkington, Marc. "11 Blockchain technology: principles and applications." Research handbook on digital transformations (2016): 225.

[13] Liu, Yi, et al. "An efficient method to enhance Bitcoin wallet security." Anti-counterfeiting, Security, and Identification (ASID), 2017 11th IEEE International Conference on. IEEE, 2017.

[14] Nofer, Michael, et al. "Blockchain." Business & Information Systems Engineering 59.3 (2017): 183-187.

[15] Hussain, S. Mahaboob, et al. "Forensics Data Analysis for Behavioral Pattern with Cognitive Predictive Task." International Conference on Next Generation Computing Technologies. Springer, Singapore, 2017.

[16] Prasanthi, B. V., Prathyusha Kanakam, and S. Mahaboob Hussain. "Cyber Forensic Science to Diagnose Digital Crimes-A study." International Journal of Scientific Research in Network Security and communication (IJSRNSC) 50.2 (2017): 107-113.