|| Volume 2 || Issue 5 || November 2017 || ISSN (Online) 2456-0774

INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH AND ENGINEERING TRENDS

# Review on Digital Crypto Currencies

**Sachin Wayase[1], Rohan Shedge[2]**

*Computer Engineering, Parikrama Polytechnic, Kashti, Maharashtra, India[1]*
*D.Y. Patil College of Engineering, Akurdi, Pune, Maharashtra, India[2]*
*sachinwayse@gmail.com[1], rohan_it2005@gmail.com[2]*

*Abstract*— **A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they will generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and re-join the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.**

## I INTRODUCTION

A cryptocurrency is a digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets. Crypto currencies are a type of digital currencies, alternative currencies and virtual currencies. Crypto currencies use decentralized control as opposed to centralized electronic money and central banking systems. The decentralized control of each crypto currency works through a block chain, which is a public transaction database, functioning as a distributed ledger.

Decentralized cryptocurrency is produced by the entire cryptocurrency system collectively, at a rate, which is defined when, the system is created and which is publicly known. In centralized banking and economic systems such as the Federal Reserve System, corporate boards or governments control the supply of currency by printing units of fiat money or demanding additions to digital banking ledgers. In case of decentralized cryptocurrency, companies or governments cannot produce new units, and have not so far provided backing for other firms, banks or corporate entities which hold asset value measured in it. The underlying technical system upon which decentralized cryptocurrencies are based was created by the group or individual known as Satoshi Nakamoto. In the past, the word “centralized” was a given for all institutions that managed finances. To be centralized means that there is a trusted intermediary to handle whatever asset may be in a trade. In a bank, for example, a customer gives their money over to the bank to hold for them. This one institution is now in complete control of the customer’s money.

In many cases, this is much safer than a person finding some way to manage. Banks have many securities and a team to watch over their customers’ money. The bank can also offer a variety of services, such as loans, because the bank has a large amount of money and has created a trust relationship with the customer. Centralized cryptocurrency exchanges are no different. A user can store their money on the exchange. The currency is now in the hands of the exchange, but the trust of the middleman makes it easy for a customer to recover a lost password or 2FA because that customer has given the exchange full access to their account. This can also take the pressure off of the customer of being 100% in control of their money. There are many stories of investors losing hundreds of thousands of dollars because they lost the private keys to their hardware wallet. If their money were in a centralized exchange, they wouldn’t have to worry about that; recovering would be as easy as showing a passport or verifying identification.

### History of Crypto Currencies

After seeing all the centralized attempts fail, Satoshi tried to build digital cash system without a central entity. Like a Peer-to-Peer network for file sharing. This decision became the birth of crypto currency. They are the missing piece Satoshi found to realize digital cash. The reason why is a bit technical and complex, but if you get it, you‘ll know more about crypto currencies than most people do. So, let‘s try to make it as easy as possible. To realize digital cash you need a payment network with accounts, balances, and transaction. That‘s easy to understand. One major problem every payment network has to solve is to prevent the so-called double spending: to prevent that one entity spends the same amount twice. Usually, a central server who keeps record about the balances does this. In a decentralized network, you don‘t have this server. So you need every single entity of the network to do this job. Every peer in the network needs to have a list with all transactions to check if future transactions are valid or an attempt to double spend. However, how can these entities keep a consensus about this record. If the peers of the network disagree about only one single, minor balance, everything is broken. They need an absolute consensus. Usually, you take, again, a central authority to declare the correct state of balances. Nobody did know until Satoshi emerged out of nowhere. In fact, nobody believed it was even possible. Satoshi proved it was. His major innovation was to achieve consensus without a central authority. Crypto currencies are a part of this solution – the part that made the solution thrilling, fascinating and helped it to roll over the world. The crypto currency is a digital currency in which no any other security is required rather than the cyber security. If we get success to achieve the cyber security the no need of the any fraud exchange can happen.

**Block chain**

When crypto currency was the only block chain, there was not much of a distinction between the terms and they were used interchangeably. As the technology matured and a variety of block chains bloomed, the uses quickly diverged from the pure money aspect. Instead, technologists experimented with ideas like decentralized name registry. Other uses utilized the peer-to-peer aspect to deliver messages in a discrete way. In the end, many of these projects failed to find a good use of the technology. The projects left standing helped demonstrate what was possible with beyond buzzwords. In recent years, corporations and enterprises have been experimenting with block chain technology, but the token as a valued asset presents a problem for most organizations and consortiums using it. If they do not like the crypto currency aspect, than what do corporations get out of block chain. For any institution, the anti-fragile distributed nature is beneficial, along with promises for a more hack-proof environment. Regulators will enjoy the auditability that cryptographic receipts provide–named "triple entry accounting". That is great and all, but one of the main benefits of block chain is as a trust protocol to coordinate possibly untrusting entities

**Time stamping**

Using Bitcoin's block chain to timestamp data has evolved far past single-file uploads that have users pay a Crypto Currencies network fee. Full-featured APIs and platforms as if Open timestamps are free, open source protocols, which allow a wide range of applications to be built on top of them. Also read: Crypto Currency's Block chain Time stamping Standards Face Off Open timestamps has been offering a robust, yet free protocol that allows anyone to build Block chain time stamping into his or her service since 2012. At least four companies are currently using this protocol. Stampers, Block Notary, Eternity Wall, and Verisartall use it at the core of their businesses today. Crypto Currency .com spoke with Open timestamps creator Peter Todd about what is new with this tool, how it works, and his plans for it. Time stamping is not difficult crypto, so I think most "block chain" companies will have that kind of talent on hand; We have to have put a lot of effort into making sure the Open timestamps protocol is simple and easy to understand and implement, even if you are not a crypto expert

**Mining**

Crypto Currency mining is the process by which transactions are verified and added to the public ledger, known as the block chain, and the means through which new bitcoin are released. Anyone with access to the internet and suitable hardware can participate in mining. The mining process involves compiling recent transactions into blocks and trying to solve a computationally difficult puzzle. The participant who first solves the puzzle gets to place the next block on the block chain and claim the rewards. The rewards, which incentivize mining, are both the transaction fees associated with the transactions compiled in the block as well as newly released

**Crypto Currency**

Mining crypto coins is an arms race that rewards early adopters. You might have heard of Crypto Currency, the first decentralized crypto currency that was released in early 2009. Similar digital currencies have crept into the worldwide market since then, including a spin-off from Bitcoin called Bitcoin Cash. You can get in on the cryptocurrency rush if you take the time to learn the basicsn properly.

**Wallets**

A crypto currency wallet stores the public and private keys , which can be used to receive or spend the crypto currency. A wallet can contain multiple public and private key pairs. As of January 2018, there are over thirteen hundred crypto currencies; the first and best known is bit coin. The crypto currency itself is not in the wallet. In case of bit coin and crypto currencies derived from it, the crypto currency is decent rally stored and maintained in a publicly available ledger. Every piece of crypto currency has a private key. With the private key, it is possible to write in the public ledger, effectively spending the associated crypto currency.

**Economics**

Crypto currencies are used primarily outside existing banking and governmental institutions and are exchanged over the Internet. While these alternative, decentralized modes of exchange are in the early stages of development, they have the unique potential to challenge existing systems of currency and payments.

**Legality**

The legal status of crypto currencies varies substantially from country to country and is still undefined or changing in many of them. While some countries have explicitly allowed their use and trade, others have banned or restricted it. Likewise, various government agencies, departments, and courts have classified bitcoins differently. China Central Bank banned the handling of bitcoins by financial institutions in China during an extremely fast adoption period in early 2014.In Russia, though cryptocurrencies are legal, it is illegal to actually purchase goods with any currency other than the Russian ruble.

## II ADVANTAGES AND DISCUSSION

Over the last couple of years, the term crypto currency has been rapidly gaining ground and understanding of its use and value in the public eye. At first it seemed unfamiliar and somewhat scary like the credit card looked to users in its early days. You might be more familiar with terms like Bit coin, and Ether. These are all crypto currencies using the Block chain to keep this currency and technology safe. Currently, there are many types of crypto currency. A simple Google search of the popular trend shows you the start of the growth and where it is taking us.

**How will crypto currency help you?**

**Fraud**: Individuals crypto currencies are digital and cannot be counterfeited or reversed arbitrarily by the sender, as with credit card charge-backs.

**Immediate Settlement:** Purchasing real property typically involves some third parties (Lawyers, Notary), delays, and payment of fees. In many ways, the bit coin/crypto currency block chain is like a "large property rights database," says Gallippi. Bitcoin contracts can be designed and enforced to eliminate or add third party approvals, reference external facts, or be completed at a future date or time for a fraction of the expense and time required to complete traditional asset transfers.

**Lower Fees:** There are not usually transaction fees for cryptocurrency exchanges because the network compensates the miners (Side note: This is the case for now). Even though there is no bitcoin/cryptocurrency transaction fee, many expect that most users will engage a third-party service, such as Coinbase, creating and maintaining their bitcoin wallets. These services act like Paypal does for cash or credit card users, providing the online exchange system for bitcoin, and as such, they are likely to charge fees. It's interesting to note that Paypal does not accept or transfer bitcoins.

**Identity Theft:** When you give your credit card to a merchant, you give him or her access to your full credit line, even if the transaction is for a small amount. Credit cards operate on a "pull" basis, where the store initiates the payment and pulls the designated amount from your account. Cryptocurrency uses a "push" mechanism that allows the cryptocurrency holder to send exactly what he or she wants to the merchant or recipient with no further information.

**Access to Everyone:** There are approximately 2.2 billion individuals with access to the Internet or mobile phones who do not currently have access to traditional exchange; these people are primed for the Cryptocurrency market. Kenya's M-PESA system, a mobile phone-based money transfer, and microfinancing service recently announced a bitcoin device, with one in three Kenyans now owning a bitcoin wallet. (Let me repeat that again. 1/3)

**Decentralization:** A global network of computers uses block chain technology to jointly manage the database that records Bitcoin transactions. That is, Bitcoin is managed by its network, and not any one central authority. Decentralization means the network operates on a user-to-user (or peer-to-peer) basis. The forms of mass collaboration this makes possible are just beginning to be investigated.

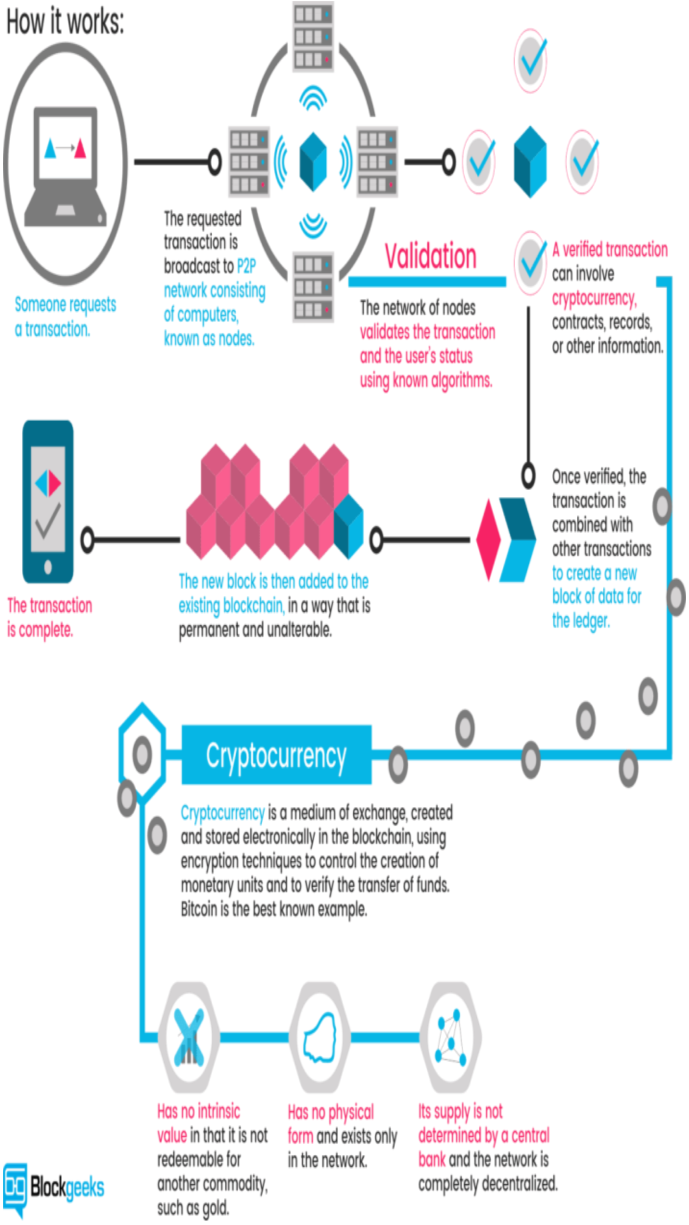
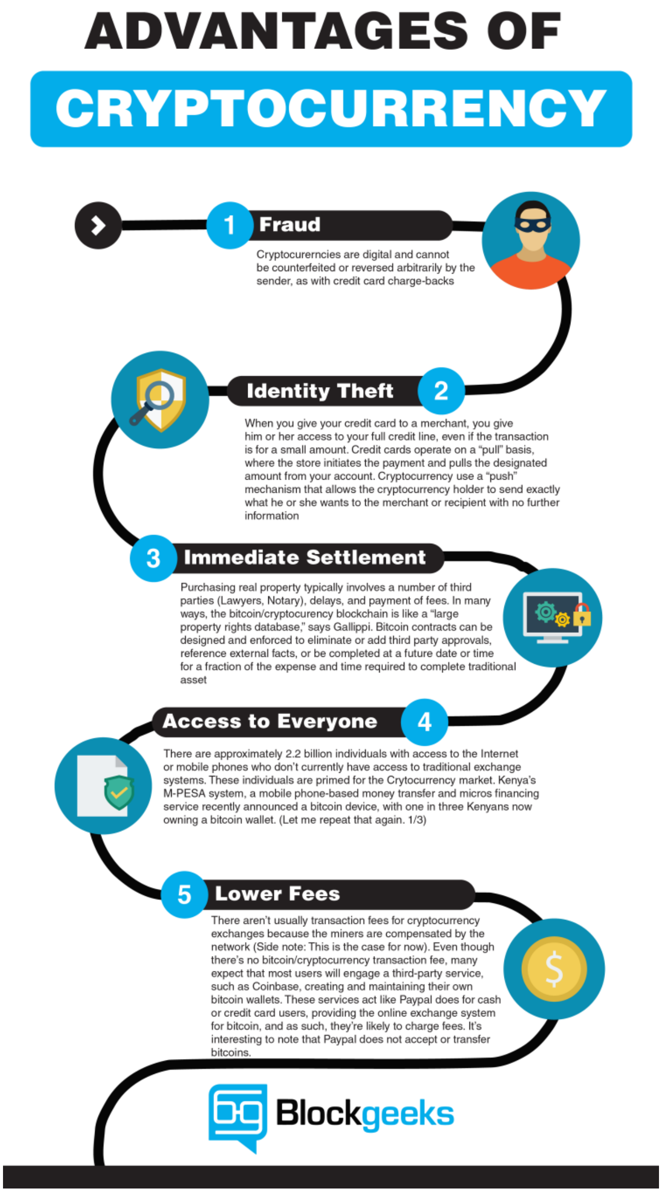

How it works:
Someone requests a transaction.
The requested transaction is broadcast to P2P network consisting of computers, known as nodes.
Validation
The network of nodes validates the transaction and the user's status using known algorithms.
A verified transaction can involve cryptocurrency, contracts, records, or other information.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
The transaction is complete.
Cryptocurrency
Cryptocurrency is a medium of exchange, created and stored electronically in the blockchain, using encryption techniques to control the creation of monetary units and to verify the transfer of funds. Bitcoin is the best known example.
Has no intrinsic value in that it is not redeemable for another commodity, such as gold.
Has no physical form and exists only in the network.
Its supply is not determined by a central bank and the network is completely decentralized.
Blockgeeks

*Figure1: Working of Crypto Currency Mining.*



ADVANTAGES OF CRYPTOCURRENCY

1 Fraud

Cryptocurerncies are digital and cannot be counterfeited or reversed arbitrarily by the sender, as with credit card charge-backs

2 Identity Theft

When you give your credit card to a merchant, you give him or her access to your full credit line, even if the transaction is for a small amount. Credit cards operate on a “pull” basis, where the store initiates the payment and pulls the designated amount from your account. Cryptocurrency use a “push” mechanism that allows the cryptocurrency holder to send exactly what he or she wants to the merchant or recipient with no further information

3 Immediate Settlement

Purchasing real property typically involves a number of third parties (Lawyers, Notary), delays, and payment of fees. In many ways, the bitcoin/cryptocurency blockchain is like a “large property rights database,” says Gallippi. Bitcoin contracts can be designed and enforced to eliminate or add third party approvals, reference external facts, or be completed at a future date or time for a fraction of the expense and time required to complete traditional asset

4 Access to Everyone

There are approximately 2.2 billion individuals with access to the Internet or mobile phones who don’t currently have access to traditional exchange systems. These individuals are primed for the Crytocurrency market. Kenya’s M-PESA system, a mobile phone-based money transfer and micros financing service recently announced a bitcoin device, with one in three Kenyans now owning a bitcoin wallet. (Let me repeat that again. 1/3)

5 Lower Fees

There aren’t usually transaction fees for cryptocurrency exchanges because the miners are compensated by the network (Side note: This is the case for now). Even though there’s no bitcoin/cryptocurrency transaction fee, many expect that most users will engage a third-party service, such as Coinbase, creating and maintaining their own bitcoin wallets. These services act like Paypal does for cash or credit card users, providing the online exchange system for bitcoin, and as such, they’re likely to charge fees. It’s interesting to note that Paypal does not accept or transfer bitcoins.

Blockgeeks

*Figure 2: Advantages of Cryptocurranies.*

## III CONCLUSION

Cryptocurrencies such as BitCoin still have numerous significant obstacles to overcome before they could totally replace current currency systems. The most immediate is the simple opposition from existing financial institutions, which wield great power and have incentives to discourage the proliferation of cryptocurrencies. Other large corporations, even when amenable to the idea of cryptocurrencies, do not currently consider them stable enough to keep as assets for long periods.

In addition to battling the current economic system, crypto currencies have some internal challenges to overcome. Attempting to convert the entire world financial system to the Bit Coin model, for example, could cause such a massive growth in block chain size that the distributed ledger model would become impractical [. It is also still unclear whether block chain technology could be successfully adapted to use cases which require very high speeds with high volumes (on the order of seconds instead of hours), and would be poorly suited for any application which required some degree of reversibility [4]. Finally, because of the substantial energy costs and diminished rewards over time associated with the "mining" process, users may eventually be forced to bear increasingly high and unreasonable transaction costs.

## REFERANCES

[1] https://blockgeeks.com/guides/what-is-cryptocurrency/

[2] https://cointelegraph.com/explained/centralized-cryptocurrency-exchanges-explained

[3] https://www.economist.com/sites/default/files/the_future_of_cryptocurrency.pdf

[4] https://www.telegraph.co.uk/technology/0/cryptocurrency/.