International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

The Evolving Payment System-Bitcoin

Kusuma Goli, Alekya Sattu, Pranava Yada
G.Narayanamma Institute of Technology and Sciences

ABSTRACT

In this paper,we present about BITCOIN .It was created in 2009, was the first decentralised cryptocurrency.We have gathered the information from the surveys and from various organizations on how they have used the concept of Cryptocurrency in different aspects.A cryptocurrency is a digital or virtual currency designed to work as a medium of exchange. It uses cryptography to secure and verify transactions as well as to control the creation of new units of a particular cryptocurrency. Essentially, cryptocurrencies are limited entries in a database that no one can change unless specific conditions are fulfilled.Based on the information gathered,There have been many attempts at creating a digital currency during the 90s tech boom, with systems like Flooz, Beenz and DigiCash emerging on the market but inevitably failing. There were many different reasons for their failures, such as fraud, financial problems and even frictions between companies' employees and their bosses.Notably, all of those systems utilized a Trusted Third Party approach, meaning that the companies behind them verified and facilitated the transactions. Due to the failures of these companies, the creation of a digital cash system was seen as a lost cause for a long while.Then, in early 2009, an anonymous programmer or a group of programmers under an alias Satoshi Nakamoto introduced Bitcoin. Satoshi described it as a 'peer-to-peer electronic cash system.' It is completely decentralized, meaning there are no servers involved and no central controlling authority. We shall discuss the the different characteristics of Bitcoin ,How to manufacture and use them,Pros and Cons of Bitcoin,How Bitcoin mining is done,Companies which accept it,whether it is legal or illegal and how actually the transaction works .We shall also highlight on how to sell and buy Bitcoins and how Block Technology works.

KEYWORDS

Bitcoin; Decentralised; Cryptocurrency; Mining; Divisibility; Authenticity; Portable; Counterfeit; Encrypted; Security; Pitfalls; Enforcement; Revolutionizing; Peer to peer; Electronic; legality; Blockchain; Hashing; Layman; Transactions;

INTRODUCTION

One of the most important problems that any payment network has to solve is double-spending. It is a fraudulent technique of spending the same amount twice. The traditional solution was a trusted third party - a central server - that kept records of the balances and transactions. However, this method always entailed an authority basically in control of your funds and with all your personal details on hand.Although people refer to bitcoin as a decentralised digital currency, We prefer to think of it as an electronic asset to sidestep questions around which government backs it and who sets the interest rate, which are often a mental block in understanding bitcoin.As an electronic asset, you can buy bitcoins, own them, and send them to someone else.

WHAT IS A BITCOIN?

BITCOIN is a type of digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.It is a form of digital currency, created and held electronically. No one controls it. Bitcoins aren't printed, like dollars or euros – they're produced by people, and increasingly businesses, running computers all around the world, using software that solves mathematical problems.It's the first example of a growing category of money known as cryptocurrency.

A software developer called Satoshi Nakamoto proposed bitcoin, which was an electronic payment system based on mathematical proof. The idea was to produce a currency independent of any central authority,

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

transferable electronically, more or less instantly, with very low transaction fees.Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the network. Bitcoin is open-source; its design is public, nobody owns or controls Bitcoin and everyone can take part. Through many of its unique properties, Bitcoin allows exciting uses that could not be covered by any previous payment system.

CHARACTERISTICS OF BITCOIN

1.SCARCE:

Money's scarcity should fall into a narrow band of objects that are widely available, however can not be easily created or found. Objects such as sea shells, which were once used as money, are too rare to be widely used except in specific locations, and objects such as sand are too abundant to have any significant value in small quantities.

The supply of bitcoin is tightly controlled and highly predictable. WIth some margin of error[11] the supply of bitcoin can be forecast out 100 years. The 21 million units should be sufficient for large amounts of trade – accounting for its divisibility.

2.DURABLE:

To function as an acceptable store of value, a proper form of money should not degrade over time. Things that were previously used as money such as cattle and grain do not last for more than several years, and would not be considered durable.

Bitcoin is completely digital, so it will not degrade with use. Additionally, bitcoin wallets can be easily duplicated to prevent file corruption.Lost coins are not reprintable so extra care must be taken.

3.PORTABLE:

Proper money should be able to be used in day-to-day transactions, and as such it needs to be highly portable in order to carry on one's person.

Bitcoin scales exceptionally well for larger quantities since it is completely digital. Anything from $0.01 to $1B can fit on a flash drive. Additionally, bitcoins can be transferred almost instantly to a recipient anywhere in the world that is connected to the internet.

4.AUTHENCITY VERIFICATION:

Money needs to be readily identified and verified. This reduces the risk to people accepting it for payment, and reduces the transaction time if it's easy to verify the authenticity.

Bitcoin cannot be visually identified since it does not exist in physical space. Software can be used to identify it in the block chain, however at its current stage this requires a fair amount of technical knowledge. Additionally, physical instantiations such as paper wallets and casascius coins are difficult to verify the true quantity of bitcoins stored.

5.STORAGE:

In order to operate as a store of value, it is necessary to be able to store in large quantities. Objects such as art and chemical compounds are difficult to store and require significant effort to maintain value.Similar to the portability characteristic, there are no scaling concerns storing bitcoin. There may be concerns as the blockchain gets larger over the years, however this should scale appropriately with advances in hardware.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

Additionally, backup methods such as cloud storage of encrypted files and using Shamir's Secret Sharing key add redundancy and reduce risk of loss due to error.

6.DIFFICULT TO COUNTERFEIT:

In order to be a reliable store of value, the object itself must be hard to counterfeit. Recipients should be confident that they are receiving authentic items, or else they will be reluctant to use it for trade in the future.

It is cryptographically impossible to counterfeit a bitcoin. The closest analogue would be attempting a double spend attack, where the recipient believes they received coins that were not actually transferred to their account.

7.IT'S FAST:

You can send money anywhere and it will arrive minutes later, as soon as the bitcoin network processes the payment.

8.WIDESPREAD USE:

Lastly, money should be able to be traded for a wide variety of products and services. The reliability of being able to spend money when you need to, and not having to be concerned with whether a merchant will accept it adds significant value.

Bitcoin is only accepted by a small fraction of web sites, and an even smaller fraction of brick and mortar stores.

HOW BITCOINS ARE CREATED?

New bitcoins are generated by a competitive and decentralized process called "mining". This process involves that individuals are rewarded by the network for their services. Bitcoin miners are processing transactions and securing the network using specialized hardware and are collecting new bitcoins in exchange.

The Bitcoin protocol is designed in such a way that new bitcoins are created at a fixed rate. This makes Bitcoin mining a very competitive business. When more miners join the network, it becomes increasingly difficult to make a profit and miners must seek efficiency to cut their operating costs. No central authority or developer has any power to control or manipulate the system to increase their profits. Every Bitcoin node in the world will reject anything that does not comply with the rules it expects the system to follow.

Bitcoins are created at a decreasing and predictable rate. The number of new bitcoins created each year is automatically halved over time until bitcoin issuance halts completely with a total of 21 million bitcoins in existence. At this point, Bitcoin miners will probably be supported exclusively by numerous small transaction fees.

Bitcoin is the first implementation of a concept called "cryptocurrency", which was first described in 1998 by Wei Dai on the cypherpunks mailing list, suggesting the idea of a new form of money that uses cryptography to control its creation and transactions, rather than a central authority. The first Bitcoin specification and proof of concept was published in 2009 in a cryptography mailing list by Satoshi Nakamoto. Satoshi left the project in late 2010 without revealing much about himself. The community has since grown exponentially with many developers working on Bitcoin.

Satoshi's anonymity often raised unjustified concerns, many of which are linked to misunderstanding of the open-source nature of Bitcoin. The Bitcoin protocol and software are published openly and any developer around the world can review the code or make their own modified version of the Bitcoin software. Just like current developers, Satoshi's influence was limited to the changes he made being adopted by others and therefore he did not control Bitcoin. As such, the identity of Bitcoin's inventor is probably as relevant today as the identity of the person who invented paper.

Bitcoin is often compared with gold, and one of the chief factors of similarity it the way they're both obtained. Similarly to gold, new Bitcoins are created via the process called "mining." In fact, Bitcoin mining has a two-fold purpose: it allows for the creation of new coins and facilitates the processing of transactions in the network. Another parallel with the precious metal is that there's a limited amount of Bitcoins that can ever be

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

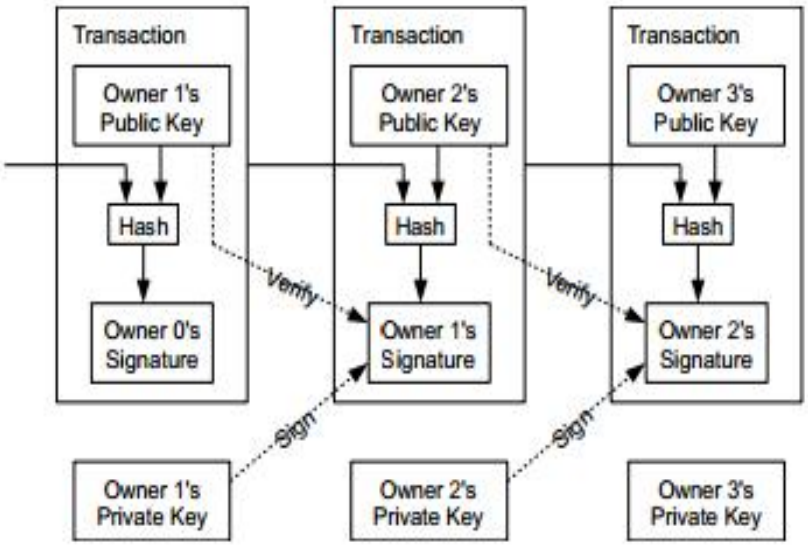
mined: no more than 21 mln coins. As of 2017, nearly 17 mln Bitcoins have already been mined. Mining can be quite a competitive task as new Bitcoins are created at a predictable and fixed rate. Those rates have been defined by Satoshi Nakamoto, the creator of Bitcoin, in the white paper published in 2008. The more miners join the network, the more difficult it becomes to make a profit for each of them. Because of that, miners have to remain highly competitive to keep receiving Bitcoins as a reward for validating the transactions.

HOW BITCOIN TRANSACTION WORKS?

A Bitcoin transaction[1] is a signed piece of data that is broadcast to the network and, if valid, ends up in a block in the blockchain.The purpose of a Bitcoin transaction is to *transfer ownership* of an amount of Bitcoin to a Bitcoin address.Bitcoin transactions are sent from and to electronic bitcoin wallets, and are digitally signed for security. Everyone on the network knows about a transaction, and the history of a transaction can be traced back to the point where the bitcoins were produced.

The important components of a Bitcoin Transaction are :

1. Transaction ID
2. Descriptors and MetaData
3. Inputs
4. Outputs



Bitcoin Transaction Inputs and Outputs

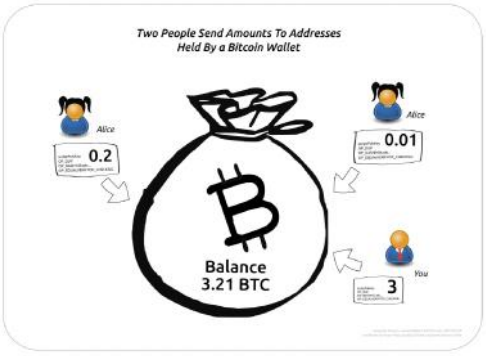
Firstly, four axiomatic truths about transactions:

- Any Bitcoin amount that we send is always sent to an address.
- Any Bitcoin amount we receive is locked to the receiving address – which is (usually) associated with our wallet.
- Any time we spend Bitcoin, the amount we spend will always come from funds previously received and currently present in our wallet.
- Addresses receive Bitcoin, but they do not send Bitcoin – Bitcoin is sent from a wallet.

The amounts that go into our wallet are not jumbled like the coins in a physical wallet. The received amounts don't mix but remain separate and distinct as the exact amounts received by the wallet.

You create a brand new wallet and, in time, it receives three amounts of 0.01, 0.2 and 3 BTC as follows: you send 3 BTC to an address associated with the wallet and two payments are made to another address by Alice.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018



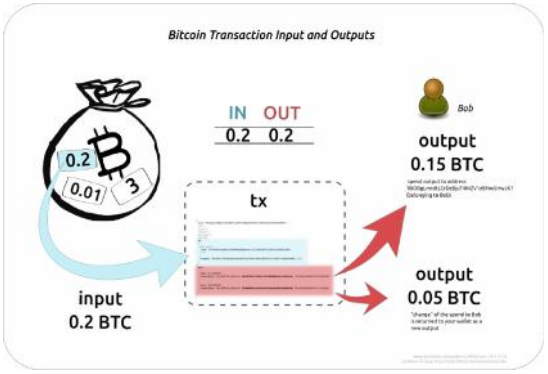
The wallet reports a balance of 3.21 BTC, yet if you were to virtually peek inside the wallet, you would see – not 321,000,000 satoshi (321 mil satoshi) – but three distinct amounts still grouped together by their originating transactions: 0.01, 0.2 and 3 BTC.

The received bitcoin amounts don't mix but remain separated as the exact amounts sent to the wallet. The three amounts in the example above are called the outputs of their originating transactions.

Bitcoin wallets always keep outputs separate and distinct.

Let's consider an example by following the money in a scenario where you send 0.15 BTC to Bob.The spend transaction your wallet creates will send 0.15 BTC to Bob's address – where it will reside in *his* wallet as an output – waiting eventually to be spent.

Instead, the wallet selects a spend candidate from amongst the three existing "outputs" contained in the wallet. So, it chooses (for various reasons that are not important now) the 0.2 BTC output. The wallet will unlock the 0.2 BTC output and use the whole amount of 0.2 BTC as an input to your new 0.15 BTC transaction. The 0.2 BTC output is "spent" in the process.



International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

PROOF-OF-WORK

Bitcoin the platform is built on the concept of "proof of work" data that is expensive and time-intensive to produce but can be easily verified.Nakamoto says that proof-of-work[3] is used to implement a peer-to-peer distributed timestamp network (mentioned above). The process scans for a value that when hashed, results in a certain numerical expression. The timestamp network must reconcile this value with a block's hash. CPU power is needed to satisfy the proof-of-work, and the block cannot be changed without redoing the work. Later blocks are chained after it, and to change the block would require redoing all the blocks after it.

The language may be technical but the concept is simple. Proof-of-work is what safeguards the blockchain. Nakamoto says that a hash created by a timestamp server is assigned a unique number that is then used to identify the hash in the blockchain. Inherent in this unique number is a math puzzle that a computer must solve before a transaction can happen. Once a correct answer is given, it serves as proof that the specified work has been done.

When someone sends an electronic coin, they must take a hash's unique number and solve an inherent math puzzle. The answer is then passed to the recipient to check if the solution is correct — an important validation step. If the answer is correct, the payment/transaction takes place and adds to the length of the blockchain. If not, the proposed transaction is rejected.

Proof-of-work provides one vote per CPU, not by IP address. Otherwise an attacker may allocate several IPs in an attempt to hack the network. Secondly, the longest chain of blocks[5]serves as proof that the CPUs invested the greater amount of work in that longer chain. This process secures the blockchain by requiring would-be-attackers to redo the work of the block and all blocks after it (i.e., solve all those math puzzles) and then try to surpass the work of all the honest computers in the network. Nakamoto says that it'd be an extremely difficult task for an attacker to do just that, and that the probability of success diminishes exponentially the more blocks are added to a chain.

So how does proof-of-work protect the blockchain? In layman's terms, honest CPUs in the network solve each hash's math problem. As these computational puzzles are solved, these blocks are bundled into a chronologically-ordered chain. Thus the term blockchain. This validates to the entire system that all the required "math homework" has been completed. An attacker would have to redo all the completed puzzles and then surpass the work of honest CPUs in order to create a longer chain — a feat that would be extremely unlikely if not impossible. This sequence makes Bitcoin transactions irreversible. Nakamoto points out that honest nodes[10] in the network need to collectively possess more CPU power than an attacker.

PROS AND CONS OF BITCOIN:

PROS:

Freedom in Payment

- With Bitcoin it is very possible to be able to send and get money anywhere in the world at any given time.
- You don't have to worry about crossing borders, rescheduling for bank holidays, or any other limitations one might think will occur when transferring money.
- You are in control of your money with Bitcoin. There is no central authority figure in the Bitcoin network.

Control and Security

- Allowing users to be in control of their transactions help keep Bitcoin safe for the network.
- Merchants cannot charge extra fees on anything without being noticed. They must talk with the consumer before adding any charges.
- Payments in Bitcoin can be made and finalized without one's personal information being tied to the transactions.
- Due to the fact that personal information is kept hidden from prying eyes, Bitcoin protects against identity theft.
- Bitcoin can be backed up and encrypted to ensure the safety of your money.

Information is Transparent

- With the blockchain, all finalized transactions are available for everyone to see, however personal information is hidden.
- Your public address is what is visible; however, your personal information is not tied to this.
- Anyone at anytime can verify transactions in the Bitcoin blockchain[9].
- Bitcoin protocol cannot be manipulated by any person, organization, or government. This is due to Bitcoin being cryptographically secure.

Very Low Fees

- Currently there are either no fees, or very low fees within Bitcoin payments.
- With transactions, users might include fees in order to process the transactions faster. The higher the fee, the more priority it gets within the network and the quicker it gets processed.
- Digital Currency exchanges help merchant process transactions by converting bitcoins into fiat currency. These services generally have lower fees than credit cards and PayPal.

Fewer Risks for Merchants

- Due to the fact that Bitcoin transactions cannot be reversed, do not carry with them personal information, and are secure, merchants are protected from potential losses that might occur from fraud.
- With Bitcoin, merchants are able to do business where crime rates and fraud rates may be high. This is because it is very hard to cheat or con anyone in Bitcoin due to the public ledger, otherwise known as the blockchain.

CONS:

Lack of Awareness & Understanding

- Fact is many people are still unaware of digital currencies and Bitcoin.
- People need to be educated about Bitcoin to be able to apply it to their lives.
- Companies like Tigerdirect and Overstock accepting Bitcoin as payment is great. However, if they do not have a knowledgeable staff that understands digital currencies, how will they help customers understand and use Bitcoin for transactions?
- The workers need to be educated on bitcoins so that they can help the customers. This will definitely take some time and effort. Otherwise, what is the benefit of such large companies accepting Bitcoin if its staff doesn't even know what digital currencies are?

Risk and Volatility

- Bitcoin has volatility mainly due to the fact that there is a limited amount of coins and the demand for them increases by each passing day.
- However, it is expected that the volatility will decrease as more time goes on.
- As more businesses, medias, and trading centers begin to accept Bitcoin, its' price will eventually settle down.
- Currently, Bitcoin's price bounces everyday mainly due to current events that are related to digital currencies.

Still Developing

- Bitcoin is still at its infancy stage with incomplete features that are in development.
- To make the digital currency more secure and accessible, new features, tools, and services are currently being developed.
- Bitcoin has some growth to do before it comes to its full and final potential.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

- This is because Bitcoin is just starting out, and it needs to work out its problems just like how any currency in its beginning stage would need to.

BITCOIN MINING

Bitcoin mining[2] is the process of adding records of a new transaction to the Blockchain - the public ledger of all transactions that have ever taken place in the Bitcoin network.New transactions are added in batches called “blocks” roughly every 10 minutes, hence the name Blockchain. The ledger is needed for the nodes of the Bitcoin network to always be able to confirm valid transactions.In order to become a Bitcoin miner, a person first needs a computer and mining software - like the GUIMiner. This program uses the computer’s resources to perform complex mathematical calculations.When any one miner succeeds in solving their math problem, they get to create a new block and receive a certain number of Bitcoins as a reward, known as “the block reward.”Every 210,000 blocks, or, roughly, every four years, the block reward is halved. It started at 50 Bitcoin per block in 2009, and in 2014 it was halved to 25 Bitcoins per block.However, mining on personal computers has only been feasible in the early years of Bitcoin. By now, the network is so competitive, that using specialized hardware is the only way to make a profit.

The first ASICs - or Application-Specific Integrated Circuits - were introduced in 2013, designed specifically for the purpose of mining from the start.

Despite the existence of such specialized equipment, the situation didn’t become easier for miners, as new, more efficient ASICs are released all the time. And the problem of paying for electricity bills is only exacerbated by the new, power-hungry hardware.

Nowadays there are many prominent companies which design and produce mining hardware. Among them, are Bitfury, Bitmain. You may also find used equipment on eBay or Amazon.

So, to recap, miners use their hardware to verify valid transactions, pack them into blocks, solve mathematical problems during the process which is called “hashing,” and, after getting a correct solution, add new blocks to the Blockchain.

What is ‘hashing’?

rk published in 2008 which outlines what Bitcoin is and how it works. There are many projects now with the wBitcoin uses a cryptographic hash function SHA-256 for encryption. This algorithm allows you to take data of any size and turn it into a string of a specific, predefined size. The resulting string is called a “hash,” and the process of applying the hash function to random inputs is called “hashing.”

It’s impossible to predict what the hash of any one input will be until you actually calculate it. The goal of the miners is to keep feeding the hash function with different inputs until they get a specific hash value which is below a certain threshold, which is called the “difficulty” of network.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

The difficulty is automatically adjusted every 2016 blocks - or, roughly, every 14 days - in accordance with the growing or shrinking combined computational power of the network.

If the network became more powerful over the last 2016 blocks, then the difficulty value is decreased to make it harder to find a valid hash and vice versa.

Considering the immense computational power that the Bitcoin network currently employs, it takes trillions of computer-generated guesses from all over the world until the right hash value is found by someone. And if you are the first to do it - congrats! You have just mined a block and got a reward of 12,5 Bitcoins.

Pitfalls to avoid in mining

As with any other activity, mining has some pitfalls to avoid. Let's take a closer look at some mistakes usually made by newbie miners:

You shouldn't start mining without preparations. Given that it is a highly competitive sphere, profitable mining requires thorough planning and preparation. Many examples can be found of people, who had bought too much hardware equipment without calculating all the costs of running it and the likely profit rates. After finding out that they can't maintain profitable operations with their equipment, these unfortunate miners usually have to re-sell it at a large discount.

You also shouldn't follow the hype and mine whatever coin that is the most trendy at the moment. From time to time, one coin or another will get overhyped, and a lot of new miners will start pouring in, driving the difficulty of its network up. As a result, mining becomes very hard for everyone, and almost no one manages to make a profit. This scenario has taken place recently with Ethereum, for example.

What you should do, is take good care of your PC. Mining places a huge load on the computer's processors, which have to run at full capacity all the time. If done without proper care, it might cause hardware malfunctions.

WHO ACCEPTS BITCOINS?

Bitcoins are taking over the crypto-currency marketplace. They're the largest and most well-known digital currency. Many large companies are accepting bitcoins as a legitimate source of funds. They allow their online products to be bought with bitcoins. With the extreme facilitation of transfer and earning of bitcoins, it would be a mistake not to accept these new-found online coins as cash.

Subway,Microsoft,Reddit,OkCupid,heapAir.com,Expedia.com,Gyft,Wikipedia,Apple,Dell,Ebay,Amazon etc to name a few.

IS IT LEGAL/ILLEGAL?

Every single fiat currency in the world is created, released and controlled by a single entity – in most cases a central bank. By law, ordinary citizens are only allowed to buy, sell or keep the currency. If someone tries to create any amount of money, they will inevitably find themselves behind bars. When Bitcoin was introduced, it created a completely new and unique paradigm. The world's first digital, decentralized currency that isn't

controlled by anyone at all. Moreover, the very concept of Bitcoin implies that anyone with enough computing power can create coins by simply being an active part of the community. As it's becoming more and more mainstream, law enforcement agencies, tax authorities and legal regulators all over the world are trying to wrap their heads around the concept of crypto currency and where exactly does it fit in existing regulations and legal frameworks. The legality of Bitcoin depends on who you are, where you are in the world, and what you're doing with it. Here's our guide on legal issues concerning Bitcoin, where we mostly focus on the US but cover other major countries as well.

It's understandable to have questions about the legality of using Bitcoin. The platform introduced a brand new paradigm away from the traditional regulators and regulations that govern fiat currency. Unlike illegal, counterfeit money, which is a blatant example of a "currency" that misrepresents itself as legal tender, Bitcoin is entirely different. Nevertheless, it operates in a seemingly gray area when it comes to regulation. However, many of these concerns boil down to misunderstandings or a lack of concrete rules that govern Bitcoin, rather than overt violations of the law.The question surrounding the relationship between Bitcoin and the law really depends on how the digital currency is being used. Ever since the now-defunct Silk Road gained notoriety, regulators have been concerned about Bitcoin's semi-anonymity and decentralized nature. In the U.S., as well as in other countries, authorities fear that the platform could be used for money laundering and the purchase of illicit goods without being traced. Not helping Bitcoin's reputation with authorities was its prevalence as a payment service for the Silk Road, a digital marketplace where users could purchase illegal goods. Whether or not people use Bitcoin as a way to participate in expressly illegal activities doesn't make the digital currency itself illegal. The illegality of the activity is the issue, whether it's paid for in bitcoin, cash or gold. However, even when bitcoin is used for legitimate purposes, rules are a little more complex.

According to the U.S. Treasury Department's Financial Crimes Enforcement Network[7], as of 2013, using bitcoin to purchase well-natured goods and services is not illegal. However, those who mine bitcoins and trade them for traditional currency or operate exchanges on which bitcoins are bought and sold are labeled "money transmitters" and could be subject to special laws that govern that type of activity. To date, those laws have rarely, if ever, been enforced to crackdown against bitcoin use.

When it comes to taxation, the IRS[4] views bitcoin and other virtual currencies as property for federal tax purposes, similar to stocks and bonds, and federal tax law dictates that purchasers and/or sellers must treat it as such. In other places around the world, the legality of Bitcoin is viewed differently[6], but for the most part it remains relatively safe to use as long as it is not tied to illicit purchases or activities. Many countries have issued statements indicating that bitcoin and other digital currencies are not regulated and do not exist as officially sanctioned currencies: a status that could put users at risk but would not have them violating any laws. Bitcoin is outright illegal in some countries, such as Iceland. Depending on where and how you utilize bitcoin, it is important to remain up-to-date on the latest regulations concerning the digital currency. As laws change across borders, governing bodies and, increasingly, as the platform gains popularity, questions about bitcoin legality will continue to be raised.

HOW THEY ARE SECURED

With traditional payments, users attain privacy when banks limit information available to the parties involved as well as the third party. With the peer-to-peer network, privacy can still be achieved even though transactions are announced. This is accomplished by keeping public keys anonymous. The network may be able to see payment amounts being sent and received, but transactions are not linked to identities. Additionally, Nakamoto proposes that a new private key should be used for each transaction to avoid payments being linked to a common owner.

To maintain privacy, Nakamoto says it's important for public keys to keep a user's identity anonymous. While everyone may be able to see transactions, no identifiable information is distributed.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

HOW WE CALCULATE BITCOINS

It's highly unlikely for an attacker to create an alternate chain faster than an honest chain. Nodes won't accept an invalid transaction or blocks containing them. Moreover, an attacker is limited in what he can attempt to do: He can only try to change one of his own transactions to retrieve coins he recently spent.

The probability that an attacker succeeds drops exponentially the more valid blocks are added to the chain. Nakamoto says that an attacker would have to get lucky early on to have a remote chance. Moreover, a receiver creates a new public key and gives it to a sender shortly before signing. This makes it difficult for an attacker to execute a fraudulent transaction through a parallel chain.There's a higher probability that an honest node will find a block faster than an attacker. It'd be extremely difficult for an attacker to solve several proof-of-work puzzles in a row faster than the rest of the honest nodes. Every 10 minutes, there are new puzzles being solved by nodes in the network.

BITCOIN WALLET

A Bitcoin wallet is a software program where Bitcoins are stored. To be technically accurate, Bitcoins are not stored anywhere; there is a private key (secret number) for every Bitcoin address that is saved in the Bitcoin wallet of the person who owns the balance. Bitcoin wallets facilitate sending and receiving Bitcoins and gives ownership of the Bitcoin balance to the user. The Bitcoin wallet comes in many forms; desktop, mobile, web and hardware are the four main types of wallets

WHERE ARE ACTUALLY BITCOINS USED?

- Computers
- Pizzas and coffee
- Airline Tickets
- Hotel Rooms Booking

HOW THEY ARE SECURED

With traditional payments, users attain privacy when banks limit information available to the parties involved as well as the third party. With the peer-to-peer network, privacy can still be achieved even though transactions are announced. This is accomplished by keeping public keys anonymous. The network may be able to see payment amounts being sent and received, but transactions are not linked to identities. Additionally, Nakamoto proposes that a new private key should be used for each transaction to avoid payments being linked to a common owner.

To maintain privacy, Nakamoto[8] says it's important for public keys to keep a user's identity anonymous. While everyone may be able to see transactions, no identifiable information is distributed.

CONCLUSION

Bitcoin is revolutionizing the $1.8 trillion global payments industry and people around the world are rethinking the meaning of their money. Moreover, the underlying technology and network that process Bitcoin transactions, known as blockchain, is transforming industries as varied as banking, farming, logistics, healthcare, elections and manufacturing, to name a few.All this is made possible by Satoshi Nakamoto's groundbreaking woord "bitcoin" in them. The real Bitcoin is the one that is most inline with the original vision of Bitcoin, as presented in the whitepaper.

The peer-to-peer system for electronic payments relies on a distributed network of honest nodes to validate transactions. Validation replaces the need to trust expensive third parties such as banks. The electronic coins are made from digital signatures, and proof-of-work that form the blockchain prevent double-spending. The system stays secure so long as honest nodes control more CPU power than an attacker. Moreover, the nodes

accept longer blocks as valid and work on extending them. This protocol rejects invalid blocks, and potential fraud, in the process. Rules and incentives can be enforced using a voting system.

REFERENCES

[1]https://bitcoin.org/bitcoin.pdf
[2]https://bitcoinmagazine.com/guides/what-bitcoin-mining/
[3]https://en.bitcoin.it/wiki/Proof_of_work [4]https://bitcoinmagazine.com/articles/bitcoin-transactions-and-american-taxation-an-interview-with-daniel-winters-cpa-1479747337/
[5]https://en.bitcoin.it/wiki/Block
[6]https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory
[7]https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf
[8]A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.
[9]http://blockchain.info/
[10]https://en.bitcoin.it/wiki/Full_node
[11]http://www.thegenesisblock.com/at-this-rate-the-last-new-btc-will-be-issued-55-years-ahead-of-schedule/