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

Bit Coin

Vasireddy Rishitha, Seethamraju Saikeerthi, Y.Ananya Reddi
G. Narayanamma Institute of Technology and Science (for women)

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'll 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 rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.*

Keywords:

Bit coin, peer-to-peer, bit coin wallet ,block chain

INTRODUCTION

Bitcoin is a new currency that was created in 2009 by an unknown person using the alias Satoshi Nakamoto. Transactions are made with no middle men – meaning, no banks. Bitcoin is an information technology breakthrough that facilitates both a secure, decentralized payment system and a tool for the storage, verification and auditing of information, including digital representations of value. A bitcoin is also the intangible unit of account that facilitates the decentralized computer network of Bitcoin users. Bitcoin is not a company or a company product.

Bitcoin is important because it represents a new means of forming consensus reliably and promptly across time and geography. As currently designed, Bitcoin is an open and transparent system that allows all users to easily come to an agreement on the authenticity of transactions andinformation stored on the network, all without the need to involve a trusted third party and without the concern of censorship of information or value transmitted across the network. Adaptations of the Bitcoin technology allow for different controls and access, but the basic premise of reliable and prompt network agreement regarding information (including value) is at the heart of this technology.

Unlike traditional computer networks and payment systems, Bitcoin is not administered by any centralized authority or controlled by any rights holder. Instead, it was introduced to the world as an open source project. It may be utilized by any person, without fee, by downloading Bitcoin software and accessing the peer-to-peer network. These users collectively provide the infrastructure and computing power that processes and verifies transactions and information posted through that network and recorded on its decentralized ledger. A group of computer scientists and programmers volunteer their time toward upgrading and improving the Bitcoin software code, primarily through an open repository on the GitHub website.

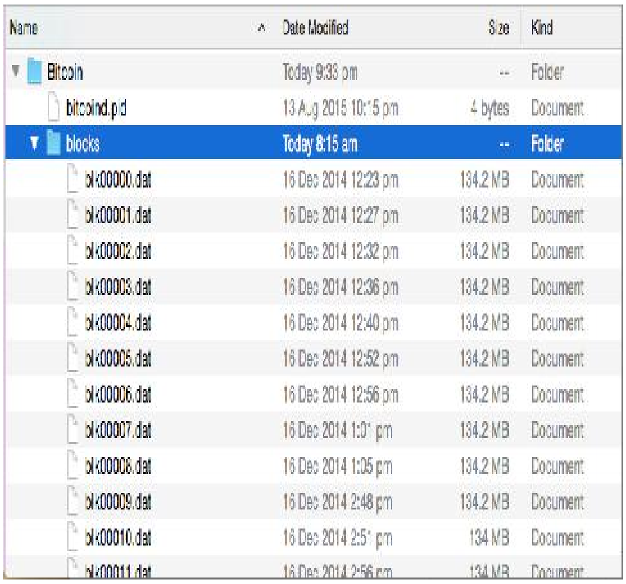
A significant economy has grown, and continues to grow, around Bitcoin, both as a payment network and as a potential information technology tool. There has also been substantial investment in bitcoins as a digital asset. The economy is driven on the one hand by direct participants and venture capitalists seeking to disrupt existing systems and on the other hand by financial institutions seeking to appropriate the innovation to improve those same existing systems. Understanding the diversity of the economy begins with understanding Bitcoin itself.

How does it work?

A network of computers validates and keeps track of bitcoin payments, and ensures that they are recorded by being added to an ever-growing list of all the bitcoin payments that have been made.

Keeping track of payments: The Bitcoin Blockchain

There is a file (well, split into several files) called “The Bitcoin Blockchain”, sitting on thousands of computers across the world, including my laptop at home. When you read the word “blockchain”, think “database” or even “list” and you have the right kind of idea.



Name	Date Modified	Size	Kind
Bitcoin	Today 9:33 pm	--	Folder
bitcoind.pid	13 Aug 2015 10:15 pm	4 bytes	Document
blocks	Today 8:15 am	--	Folder
blk00000.dat	16 Dec 2014 12:23 pm	134.2 MB	Document
blk00001.dat	16 Dec 2014 12:27 pm	134.2 MB	Document
blk00002.dat	16 Dec 2014 12:32 pm	134.2 MB	Document
blk00003.dat	16 Dec 2014 12:36 pm	134.2 MB	Document
blk00004.dat	16 Dec 2014 12:40 pm	134.2 MB	Document
blk00005.dat	16 Dec 2014 12:52 pm	134.2 MB	Document
blk00006.dat	16 Dec 2014 12:56 pm	134.2 MB	Document
blk00007.dat	16 Dec 2014 1:01 pm	134.2 MB	Document
blk00008.dat	16 Dec 2014 1:05 pm	134.2 MB	Document
blk00009.dat	16 Dec 2014 2:48 pm	134.2 MB	Document
blk00010.dat	16 Dec 2014 2:51 pm	134 MB	Document
blk00011.dat	16 Dec 2014 2:56 pm	134 MB	Document

Fig:A screenshot of The Bitcoin Block chain files on computer. Here you can see the Bitcoin Blockchain split into files, each 134MB big, and the total is about 50GB at time of writing.

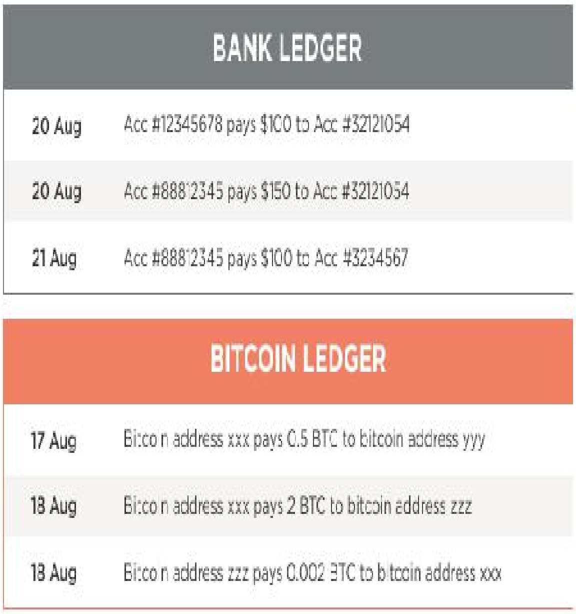
This file contains data about all the bitcoin transactions, that is payments of bitcoins from one account to another, that have ever happened. This is often called a ledger, similar to a bank’s ledger which keeps a record of payments between bank accounts.

The bitcoin network

The computers which store this file also run software that connects them over the internet to the other computers running the same software. This forms a network of computers that can talk to each other, relaying information about

1. new payments (at time of writing there is about one new bitcoin payment per second, but this comes in fits and starts)

2. updates to The Bitcoin Blockchain (every 10 mins or so, a new “page” or block of valid transactions is confirmed and is distributed to all of the computers on the network)



BANK LEDGER	
20 Aug	Acc #12345678 pays $100 to Acc #32121054
20 Aug	Acc #88812345 pays $150 to Acc #32121054
21 Aug	Acc #88812345 pays $100 to Acc #3234567

BITCOIN LEDGER	
17 Aug	Bitcoin address xxx pays 0.5 BTC to bitcoin address yyy
18 Aug	Bitcoin address xxx pays 2 BTC to bitcoin address zzz
18 Aug	Bitcoin address zzz pays 0.002 BTC to bitcoin address xxx

fig:Simplified bank ledger vs bitcoin ledger: they are similar.

When you make a bitcoin payment, a payment instruction is sent to the network. The computers on the network validate the instruction and relay it to the other computers. After some time has passed, the payment gets included in one of the block updates, and is added to The Bitcoin Blockchain file on all the computers across the network.

Peer-to-peer

The distribution of data works on a peer-to-peer basis, rather than client-server. Peer-to-peer is like a gossip network where everyone tells a few other people the news (about new transactions and new blocks), and eventually the message gets to everyone in the network. This is as opposed to client-server is more like a conventional organisation where a boss tells subordinates the news, and the boss is a central point of reference, and potential failure.

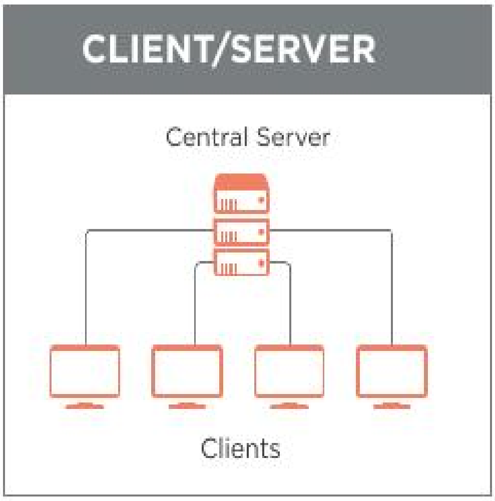


Fig: Client-server data distribution Model

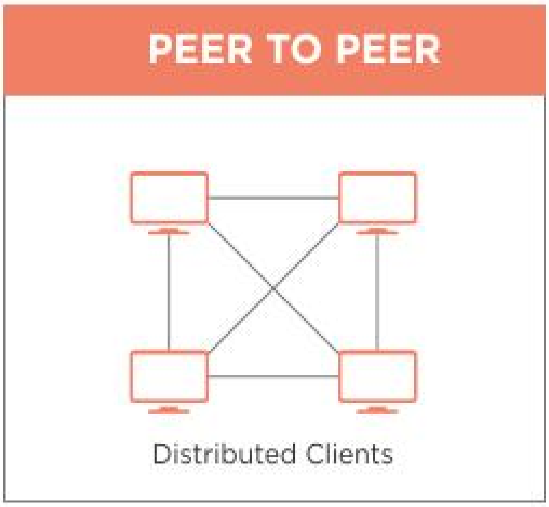


Fig:Peer-to-Peer data distribution Model

One benefit of peer-to-peer (p2p) over client-server is that with p2p, the network doesn't rely on one central point of control which can fail.

Transactions

The definition of a Bitcoin is a "chain of digital signatures" that can be passed from one person to another using an electronic signature (hash).

An analogy to this is signing for a package that you have received and then writing a forwarding address on the package before sending it onwards. Passing the Bitcoin from one person to another is like playing a game of pass the parcel, except each time the parcel is passed, the history of the parcels locations is written on it. This history creates the Bitcoin "Blockchain" which is essentially a ledger/log of the Bitcoin(s) transaction history.

Unlike parcels in the real world, digital parcels can be sent to more than one recipient at the same time (imagine sending the same email to multiple people). This is problematic as it could lead to people "double spending" their digital currency.

Bitcoin overcomes this problem as time stamps are used to ensure that whenever a Bitcoin is passed on, a duplicate copy of that coin cannot be double spent (fraud). Each transaction is time stamped and processed by the Bitcoin system in order of their respective time stamp. Therefore, if a coin is sent to two recipients, the coins will have different time stamps and hence the second coin sent will be automatically rejected by the system.

The Bitcoin system processes every transaction and "publicly announces" whenever a transaction takes place. This ensures that the system, along with its users, moderate the chain of transactions (blockchain) to ensure fraudulent activity does not take place. Using this method of moderating transactions ensures that a 3rd party is not needed and the Bitcoin system is truly decentralised.

Further to this, the participants of the system (computers/nodes) must agree on a single transaction timeline. If participants use different time lines, the double spending problem will reoccur and/or multiple block chains will be created (Mayhem!).

To avoid this, the majority of computers (nodes) in the network agree upon a singular timeline and process transactions relative to this time.

Timestamp Server

The timestamp server is a simple piece of software that is used to digitally timestamp data. The server takes a small section of the transaction data (a hash) and timestamps it. This time stamped hash is then made publicly available for everyone to see. The existence of this time stamped hash therefore proves that the transaction exists and is therefore valid.

As previously described in the “Transactions” section, the electronic signature of the previous transaction (hash) is also included in the newly created hash. This therefore creates a chain of transactions (Blockchain) as each new time stamped hash includes the previous hashes. The size of the Blockchain will therefore get larger as the transaction history increases.

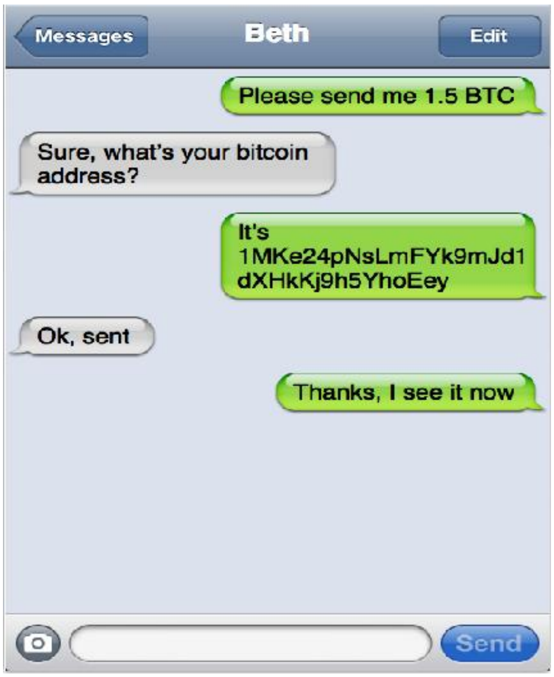
This demonstrates why more processing power is needed to “mine” the block chain as its length increases. When Bitcoin was first introduced, a small desktop computer could efficiently “mine” Bitcoins (process transactions), however a desktop computer can no longer do this and specialised computers are needed to process the transactions due to the length of the Blockchain.

How are bitcoins stored?

Bitcoin ownership is tracked on The Bitcoin Blockchain, and bitcoins are associated with “bitcoin addresses”. Bitcoins themselves are not stored; but rather the keys or passwords needed to make payments are stored, in “wallets” which are apps that manage the addresses, keys, balances, and payments.

Bitcoin accounts: addresses

In banking you have accounts which keep pots of money separate; in bitcoin you have addresses. A bitcoin address is similar to a bank account number, with a few differences.Here’s an example of a bitcoin address: Just like with bank accounts, if you want to receive a bitcoin payment, you need to tell someone your bitcoin address, so they know where to send bitcoins to. A typical conversation, which could be in person, or online, (Whatsapp/Skype etc) looks like:



Please send me 1.5 BTC

Sure, what’s your bitcoin address?

It's 1MKe24pNsLmFYk9mJd1dXHkKj9h5YhoEey

Ok, sent

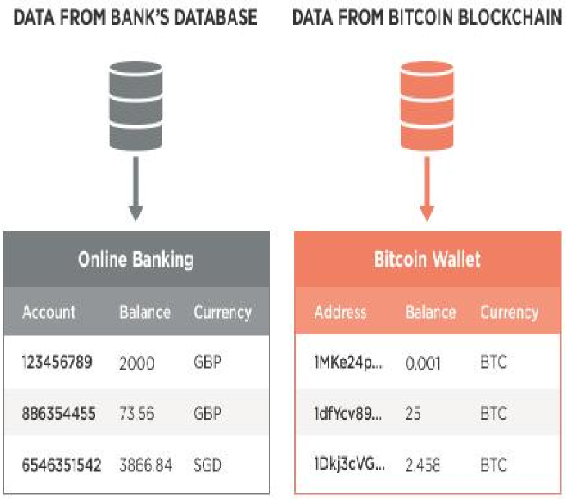
Thanks, I see it now

Fig:(BTC and XBT mean the same thing and are industry standard abbreviations for bitcoins, like GBP for Pound Sterling)

Bitcoin wallets

With my bank, under one single username/password, I control a number of accounts (e.g. incoming salary, monthly savings, tax, etc), each of which have a balance or amount of currency. Similarly, Bitcoin wallets are apps that display all of your bitcoin addresses, display balances and make it easy to send and receive payments.

For a wallet to provide accurate information, it needs to be online or connected to a Bitcoin Blockchain file, which it uses as its source of information. The wallet will read the Bitcoin Blockchain file and calculate the balances in each address. Bitcoin wallets let you create bitcoin addresses to receive incoming transactions and make outgoing payments, plus have other features that make them user friendly.



Online Banking

Account	Balance	Currency
123456789	2000	GBP
886354455	73.56	GBP
6546351542	3866.84	SGD

Bitcoin Wallet

Address	Balance	Currency
1MKe24p...	0.001	ETC
1dfYcv89...	25	ETC
1Dkj3cVG...	2.458	ETC

Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.

As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

[6] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[7] W. Feller, "An introduction to probability theory and its applications," 1957.