

Bitcoin & The Blockchain

Sammy Diamantstein

A dark blue diagonal gradient bar that starts from the bottom left corner and extends towards the top right corner, covering the lower half of the slide.

Agenda

- The origin Story
- Blockchain VS Bitcoin
- What Problems do Bitcoin and Blockchain solve
 - Fraud
 - Centralization of Authority
- What is the Blockchain: High Level
- What makes up the Block chain
 - Transaction, Timestamping, Proof of Concept, a Network,
- Blockchain space saving and Privacy
- Incentive structure and Bitcoin Splitting
- Financial applications
- Non-financial applications
- Critiques and Faults
- Why it Here To Stay

Origin Story:

The foundations for the modern Blockchain were outlined in Satoshi Nakamoto's white paper

Bitcoin: A Peer-to-Peer Electronic Cash System

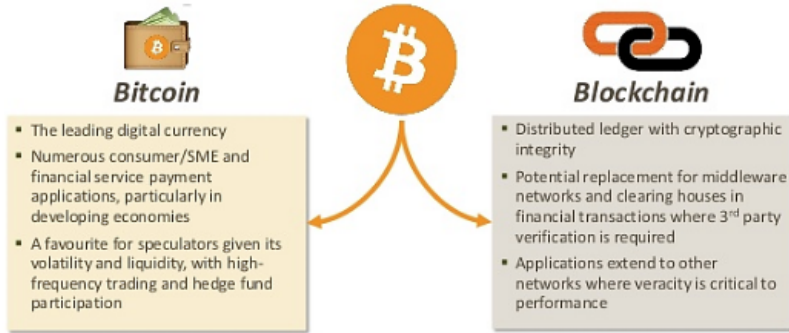
Satoshi Nakamoto
satoshiin@gmx.com
www.bitcoin.org

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.

- Satoshi Nakamoto, a pseudonym for either a man, woman, or a collective, released a white paper in November 2008
- While the word blockchain is never explicitly used in the paper, Nakamoto refers to the use of the bitcoin, which itself will be explained, in a manner that describes what we today call the Blockchain.
- The first work on a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and W. Scott Stornetta. The however lacked the distributed nature of blockchain as described by Nakamoto.

Bitcoin at its most fundamental level is a breakthrough in computer science – one that builds on 20 years of research into cryptographic currency, and 40 years of research in cryptography, by thousands of researchers around the world.

Blockchain VS Bitcoin



Bitcoin:
"A digital coin as a chain of digital signatures" (Nakamoto)

- Basis of a digital currency
- Electronically created and held
- Commodity: 21 million can ever be "mined"
- Bitcoins are mined
- Divisible Units

Blockchain:

- Append only sequential data structure
- Hash pointer linked list of blocks
- Each block is a record of a transaction
- Used to build a ledger or record of transactions
- Copies of the blockchain are kept by everyone
- "Miners" append to it

While the proposed bitcoin payment system was exciting and innovative, it was the mechanics of how it worked that was truly revolutionary. Shortly after the white paper's release, it became evident that the main technical innovation was not the digital currency itself but the technology that lay behind it, known today as blockchain.

"Blockchain is to bitcoin, what the internet is to email

..A big electronic system, on top of which you can build applications. Currency is just one"

Analogy is close to correct, but that bitcoin is the asset used to reward miners who use computing power to validate transactions un the blockchain, and won't do so without reward.

- Blockchain needs a financial reward system, and bitcoin mediates it.



What Problems does the Blockchain solve?

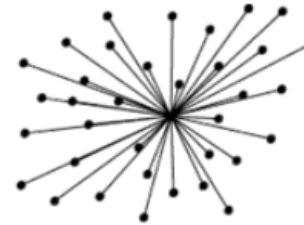
1. Removal of 3rd parties: Decentralization
 - Increase reliability
 - Decreased cost of transacting
 - Decreased time to transact
2. Fraud:
 - Cryptographic proof instead of trust: Fraud
 - Double Spending

Decentralization

"What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."-Nakamoto

Transactions between parties that require the trust provided by 3rd parties cost:

- i. Time
- ii. Money
- iii. Control



centralised



decentralised

1. By Increasing the time and cost in transactions, a limiting of the traction size and frequency occurs, making it unreasonable to perform certain transactions. Decentralizing power away from third party powers, like the greek central bank who seized private funds, ensures that trust in institutions is replaced with certainty in cryptography.
 - How is this decentralization achieved? We will soon see.

Fraud Protection

1. Reversible Transactions

- A fraction of traditional financial transactions are fraudulent.
- Computationally impossible to revert transaction

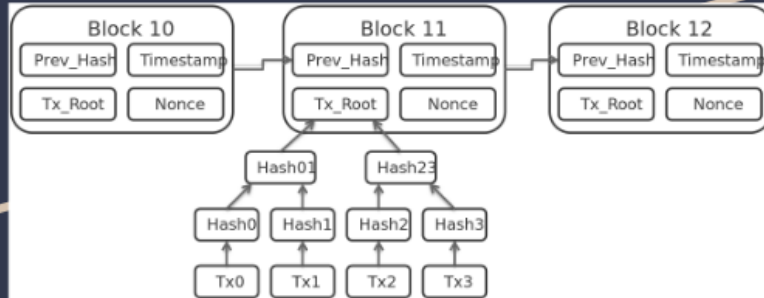
2. Byzantine Generals Problem

3. Double Spending

- The risk that a person could concurrently send a single unit of currency to two different sources.

1. Using *Cryptography* involves the use of codes and protocols to establish secure communications. Transaction reversal Fraud is prevented due to computational challenge of changing many nodes in the blockchain
2. Bitcoin is the first practical solution to a longstanding problem in computer science called the Byzantine Generals Problem. To quote from the original paper defining the B.G.P.: “[Imagine] a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement.”
3. The risk that a person could concurrently send a single unit of currency to two different sources. The bitcoin/ blockchain

What is the Blockchain?



A blockchain is a **ledger of facts**, replicated across several computers assembled in a peer-to-peer network.

- Facts can be anything from monetary transactions to content signature.
- All communication inside the network takes advantage of cryptography to securely identify the sender and the receiver.
- When a node wants to add a fact to the ledger, a consensus forms in the network to determine where this fact should appear in the ledger; this consensus is called a **block**.

Timestamp: The time when the block was found

Reference to Parent (Prev_Hash): This is a hash of the previous block header which ties each block to its parent, and therefore by induction to all previous blocks. This chain of references is the eponymic concept for the blockchain.

Merkle Root (Tx_Root): The Merkle Root is a [reduced representation](#) of the set of transactions that is confirmed with this block. The transactions themselves are provided independently forming the **body of the block**. There must be at least one transaction: The [Coinbase](#). The Coinbase is a special transaction that may create new bitcoins and collects the transactions fees. Other transactions are optional.

Nonce: An arbitrarily picked number to conveniently add entropy to a block header without rebuilding the Merkle tree.



Blockchain Features

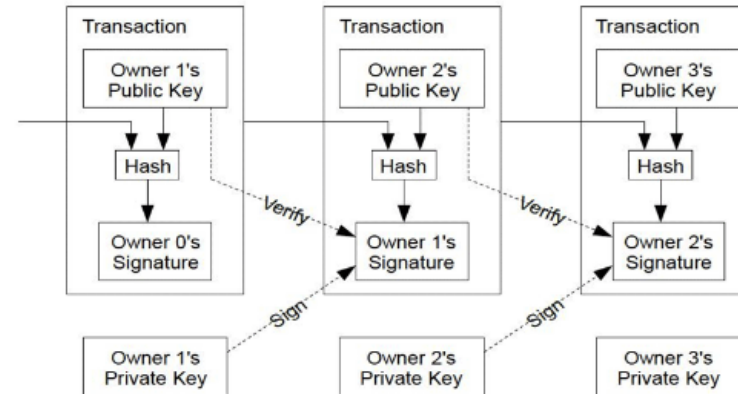
1. Transactions
2. Timestamp Server
3. Proof-of-Work
4. Network
5. Incentive System
6. Ledger Size
7. Payment Verification
8. Combining and Splitting Value
9. Privacy
10. Safety

...

We will examine the Blockchain and Bitcoin through Nakamoto's paper sections

Transaction

“electronic coin as a chain of digital signatures”
- Nakamoto



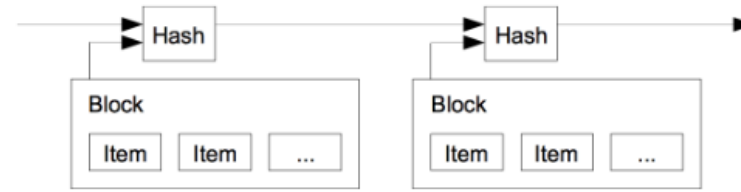
A coin owner transfers coins by digitally signing(via ECDSA) a hash digest of the previous transactions and the public key of the next owner. This signature is appended to the end of the coin

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.

What your wallet holds are addresses. These addresses can occur in the Bitcoin block chain, which can - at its simplest - be seen as a big database of balances for each Bitcoin address. Your wallet also holds a private key for each address, which can be seen as the password needed to spend the balance that is accredited to the corresponding address.

When you spend some bitcoins, you send them from one of your addresses to another address. Only the person that owns the private key corresponding to the address, can spend the bitcoins on its balance. **The problem of the double spend now comes into play: What prevents owner 0 from sending his coin to owner 1 and owner 2 at the same time?**

TimeStamp



Each block contains a Unix time timestamp. In addition to serving as a source of variation for the block hash, they also make it more difficult for an adversary to manipulate the block chain.

Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it

Solves the double spend problem:

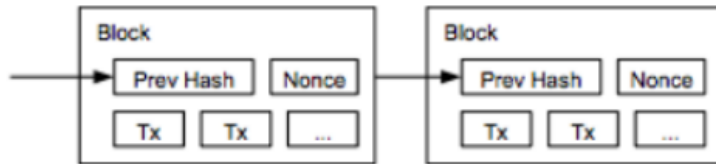
Bitcoin overcomes this problem as time stamps are used to ensure that whenever a Bitcoin is passed on, a duplicate copy of that coin cannot be double spent (fraud). Each transaction is time stamped and processed by the Bitcoin system in order of their respective time stamp. Therefore, if a coin is sent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

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.



Proof-of-Work

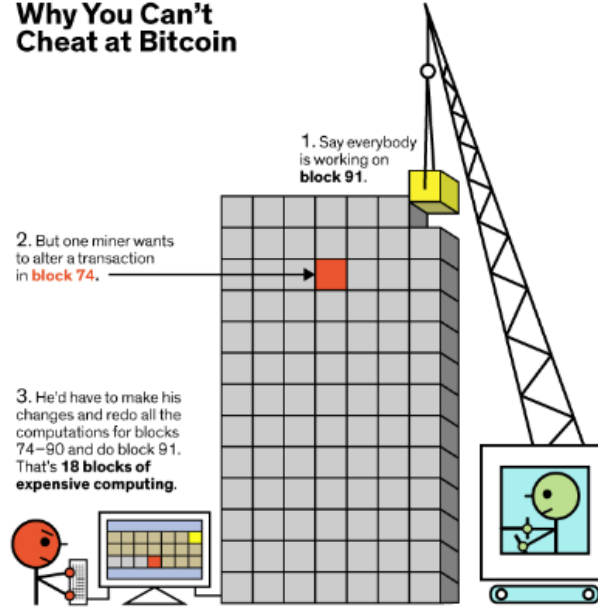
HashCash Algorithm used by trial and error to discover a "nonce" number that when included in the block yields a hash with a sufficient number of leading zero bits.



Click to add text

Why You Can't Cheat at Bitcoin

1. Say everybody is working on **block 91**.
2. But one miner wants to alter a transaction in **block 74**.
3. He'd have to make his changes and redo all the computations for blocks 74–90 and do block 91. That's **18 blocks of expensive computing**.
4. What's worse, he'd have to do it all **before** everybody else in the Bitcoin network finished **just the one block (number 91)** that they're working on.



A bitcoin miner runs a computer program that collects unconfirmed transactions from coin dealers in the network. With other data these can form a block and earn a payment to the miner, but a block is accepted by the network only when the miner discovers by trial and error a "nonce" number that when included in the block yields a hash with a sufficient number of leading zero bits to meet the network's difficulty target. Blocks accepted from miners from the bitcoin Blockchain that is a growing ledger of every bitcoin transaction since the coin's first creation.

The first party, as determined by the timestamp to provide the proof-of-work receives the bitcoins.

Network

The steps to run the network are as follows:

- 1) New transactions are broadcast to all nodes.
- 2) Each node collects new transactions into a block.
- 3) Each node works on finding a difficult proof-of-work for its block.
- 4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
- 5) Nodes accept the block only if all transactions in it are valid and not already spent.
- 6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Rules of the network

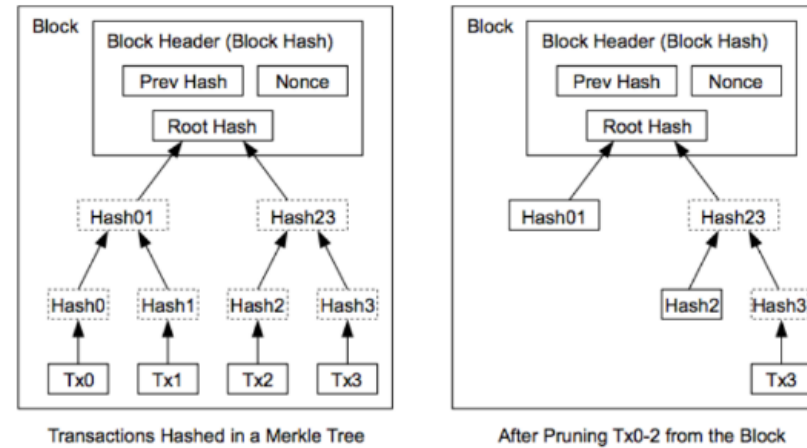
-Nodes always consider the longest chain to be the correct one and will keep working on extending it.

-If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer

-New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

Reclaiming Disk Space Pt.1

Why isn't the size of the blockchain a serious problem for bitcoin?



Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.

Reclaiming Disk Space Pt.2: Simplified Payment Verification

The issue of needing to store the complete blockchain ledger on each node by using

1) Full nodes:

stores the complete blockchain ledger locally. Here, the size of the blockchain is a problem because the full node will have to store all the transactions that ever happened on the blockchain.

2) Lightweight or partial nodes:

They don't store the complete ledger. Instead they use a simplified payment verification (SPV) mode which only requires them to download a part of the blockchain. They will connect to full node clients and use bloom filters to ensure that they only receive transactions which are necessary and relevant to their operation.

Most full nodes serve lightweight clients by allowing them to refer their transactions to the network and by notifying them when a transaction affects their wallet.

Incentive System

Why would Miners expend computing power to create proof of concepts?

People add transaction records to Bitcoin's public ledger of past transactions or "Mine" because when a node provides a valid proof of concept, they are rewarded with 12.5 bitcoins. The number of bitcoins rewarded is halved each 210,000 blocks mined.

- The incentive system is built to limit the number of existing bitcoins, making more of a like commodity than a currency

Combining and Splitting Value

Can Bitcoin be bought/sold in fractions?

“Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.”

Multiple inputs for a transaction. If I buy 1 bitcoin, it can be composed of .2 from person a, .5 from person b, .3 from person c.

Privacy

Pseudo Anonymity produced by public key cryptography

By using a public key in all blockchain transactions, a list of identities are made available for anyone to see, although the person behind the key is not revealed.

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.

Traditional Privacy Model























New Privacy Model



Here we see that we decouple the concept of the identity and the transaction, allowing the transactions to be publicly viewable with the exact identity of the party being revealed. Prior to this model, identity was held private through efforts of the third party, who in the case of buy and selling stocks, facilitate the trades, declare the trade on the ticker tape, but keeps the information hidden.]

Non- Financial Applications

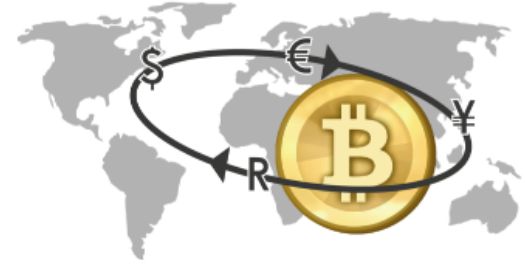
Non-Financial Use Cases					
Digital Content/Documents, Storage & Delivery		Authentication & Authorization		Digital Identity	Marketplace
					
BitProof, Blockcai, Ascribe, ArtPlus, Chainy.Link, Stampery, Blocktech (Alexandria), Bisantyum, Blockparti, The Rudimental, BlockCDN		The Real McCoy, Degree of Trust, Everpass, BlockVerify,		Sho Card, Uniquld, Onename, Trustatom	Providing premium rights & brand based coins: MyPowers
Smart Contracts		Real Estate		Diamonds	Gold & Silver
					
Otonomos, Mirror, Symbiont, New system Technologies		Factom		Everledger	BitShares, Real Asset Co., DigitalTangible (Serica), Bit Reserve
Blockchain in IoT		App Development		Network Infrastructure & APIs	
					
Filament, Chimera-inc.io, ken Code – ePlug		Proof of ownership for modules in app development: Assembly		Ethereum, Eris, Codius, NXT, Namecoin, Colored Coins, Hello Block, Counterparty, Mastercoin, Corona, Chromaway, BlockCypher	
				Other	
				 <u>Prediction platform:</u> Augur  <u>Election Voting:</u> Follow My Vote  <u>Patient Records management:</u> BitHealth	
Financial Use Cases					
Currency Exchange & Remittance		P2P Transfers		Ride Sharing	Data Storage
					
Coinbase (Wallet), BitPesa, Billion, Ripple, Stellar, Kraken, Fundrs.org, MeXBT, CryptoSigma		BTC Jam, Codius, BitBond, BitnPlay (Donation), DeBuNe (SME's B2B transactions)		La'zooz	Storj.io, Peernova
				Trading Platforms	Gaming
					
				equityBits, Spritzle, Secure Assets, Coins-e, DXMarkets, MUNA, Kraken, BitShares	PlayCoin, Play(on DACx platform), Deckbound

Authorship and ownership , Commodities ,Data management, Digital identity, identification authentication,E-voting, Network infrastructure, Reputation

verification & ranking, Government & organizational governance

Financial Applications: Bitcoin & Blockchain

1) International Remittance



2) Creation of a modern economic system

3) Micropayments



1) One immediately obvious and enormous area for Bitcoin-based innovation is international remittance. Every day, hundreds of millions of low-income people go to work in hard jobs in foreign countries to make money to send back to their families in their home countries – over \$400 billion in total annually, according to the World Bank. Every day, banks and payment companies extract mind-boggling fees, up to 10 percent and sometimes even higher, to send this money. |

2) Moreover, Bitcoin generally can be a powerful force to bring a much larger number of people around the world into the modern economic system. Only about 20 countries around the world have what we would consider to be fully modern banking and payment systems; the other roughly 175 have a long way to go.

3) A third fascinating use case for Bitcoin is micropayments, or ultrasmall payments. Micropayments have never been feasible, despite 20 years of attempts, because it is not cost effective to run small payments (think \$1 and below, down to pennies or fractions of a penny) through the existing credit/debit and banking systems. The fee structure of those systems makes that nonviable.