
Welcome

Theory Of Blockchain

On The Basics of Bitcoin

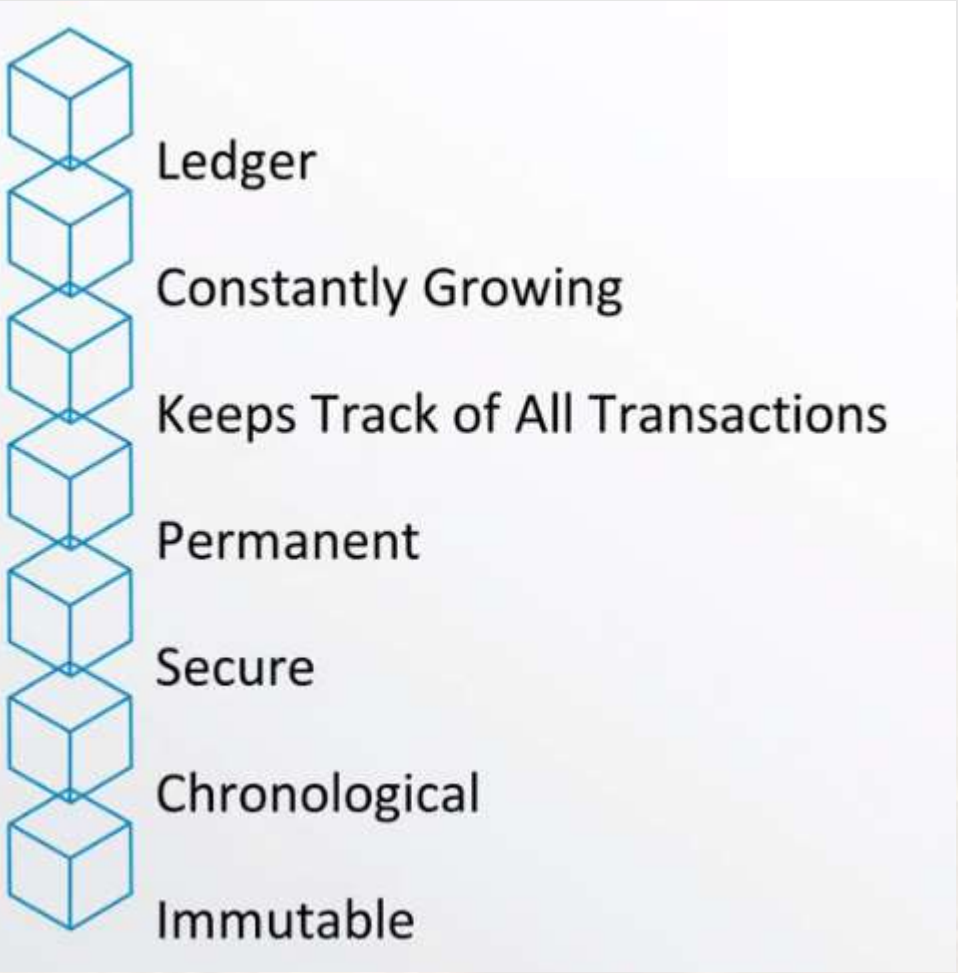
What we learn today?

- What is Blockchain?
- What is Bitcoin?
- Key concepts in Bitcoin.
- The value of Blockchain.
- Common Misconceptions.
- Getting Started with Bitcoin.

What is Blockchain?

> A Blockchain is a constantly growing ledger that keeps a permanent record of all the transactions that have taken place, in a secure, chronological and immutable way.

What is Blockchain? [Cont.]



Lets break down the definition of blockchain into its fundamental aspects.

What is Bitcoin ?

Bitcoin is a cryptocurrency. It is a decentralized digital currency without a central bank or single administrator that can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries.

What is cryptocurrency?

A cryptocurrency is a digital asset designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets. Example include bitcoin and litecoin.

Defining Cryptocurrency

> Cryptocurrency is a type of digital asset which can be used to exchange value between parties.

It uses encryption to secure how it's transferred and to control the creation of new units of that currency.

- Bitcoin
- Litecoin
- Z-Cash
- Monero
- Dash (Digital Cash)

Bitcoin Mining

Bitcoin mining is the backbone of the Bitcoin network. Miners provide security and confirm Bitcoin transactions. Without Bitcoin miners, the network would be attacked and dysfunctional. Bitcoin mining is done by specialized computers. The role of miners is to secure the network and to process every Bitcoin transaction.

Bitcoin Miners

A mining pool is a group of miners who combine their computing power and split the mined bitcoin between participants. A disproportionately large number of blocks are mined by pools rather than by individual miners

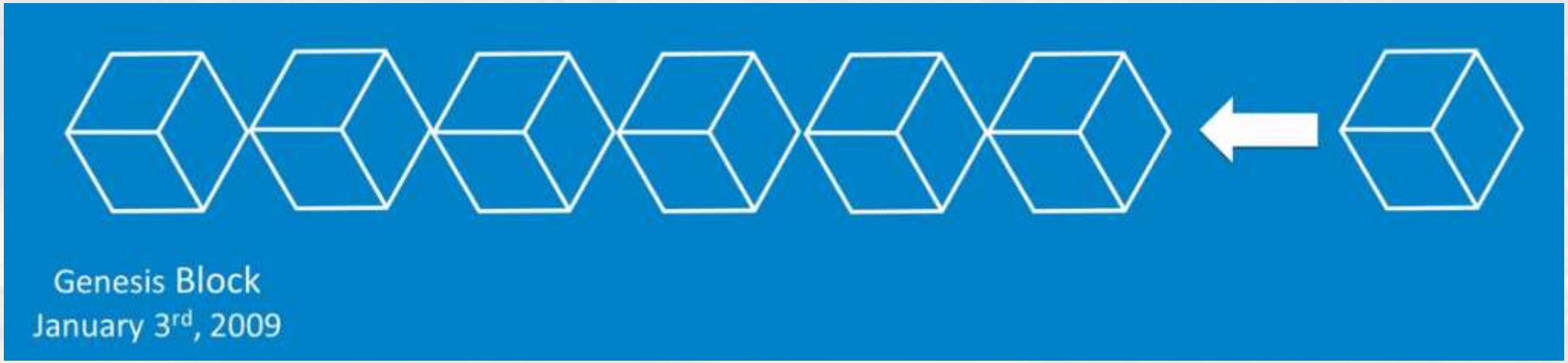
Role Of Bitcoin Miners

> The role of a miner is to build the blockchain of records that form the Bitcoin ledger.

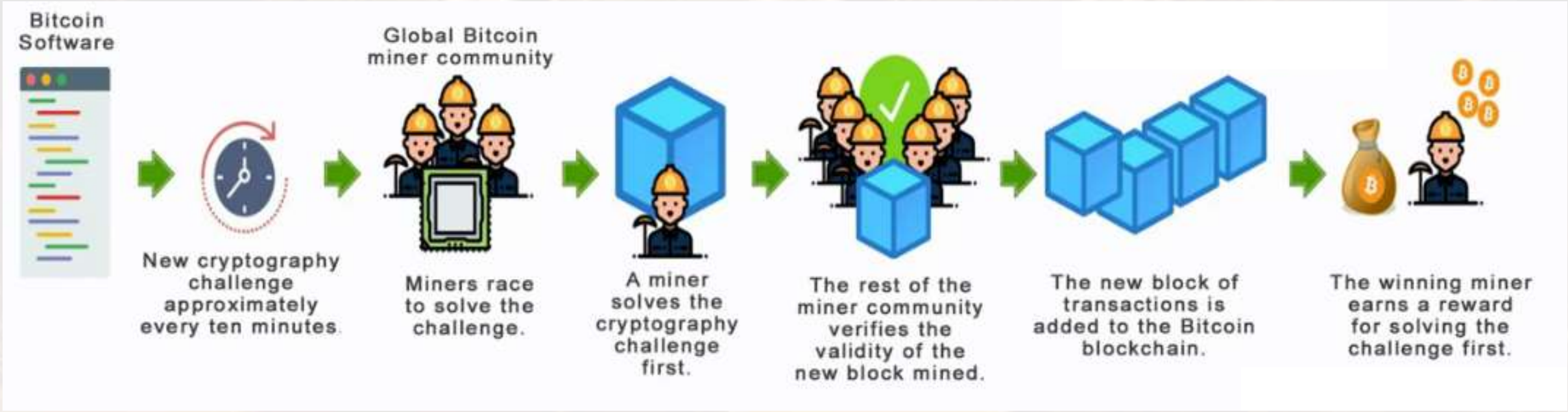
- Miners
- Process and Confirm Transactions
- Powerful Bitcoin Mining Computers
- Solve Cryptography Math Problems
- Rewarded in Bitcoin

How bitcoin blockchain is build ?

The block is sent out to the bitcoin network, which are made up of people running high-powered computers. These computers compete to validate the transactions by trying to solve complex mathematical puzzles. This validated block is then added onto previous blocks creating a chain of blocks called a bitcoin blockchain



:Four Components of Bitcoin:



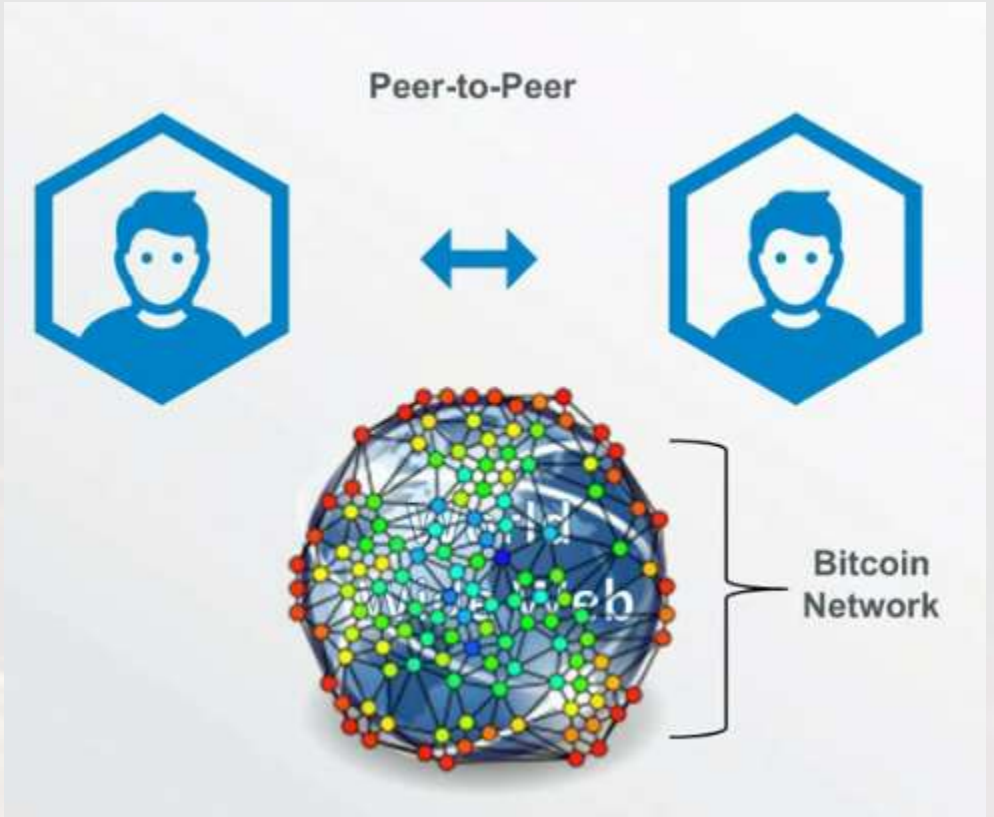
:Sending Money Over Internet:

Sending Money Over Web

A 3rd party such as a bank, credit card or other institution

- Controls the transfer
- Keeps record of transaction
- Centralized

:Bitcoin Transfer of Value:



Birth of Bitcoin

> 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.

- Satoshi Nakamoto
"Bitcoin: A Peer-to-Peer Electronic Cash System"

Bitcoin: A Peer-to-Peer Electronic Cash System

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

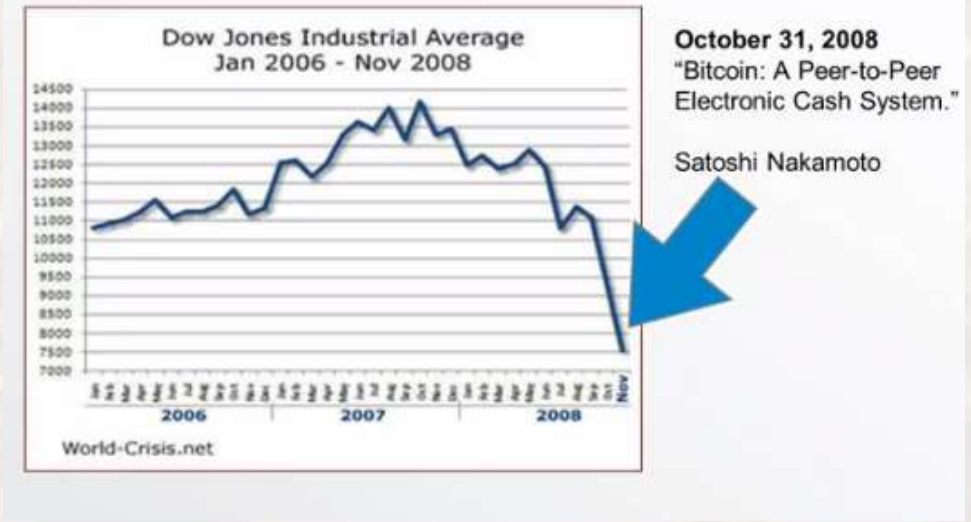
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required 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.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

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. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

1



October 31, 2008
"Bitcoin: A Peer-to-Peer Electronic Cash System."

Satoshi Nakamoto

1976 Mutual Distributed Ledgers (MDL)

"New Directions in Cryptography"

Ecash – 1983

Hashcash Proof-of-Work – 1997

b-money -1997

Bitgold - 1998

Key Features That Blockchain Add to Internet

Value

Enables a unique asset to be transferred over the Internet without a middle centralized agent.

Trust

Creates a permanent, secure and unalterable record of who owns what. Using advanced Hash Cryptography, "Information integrity" is preserved.

Reliability

Decentralized network structure ensures that there is no single point of failure which could bring the entire system down.

Smart Contract

A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible.

:Father Of Smart Contracts:

Nick Szabo on Smart Contracts (1994)

> A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries.
>
> Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs.

:Decentralized Autonomous Organization:
or
:Decentralized Autonomous Cooperation:

Uber

Top Five Uses of Blockchain in Business

- Supply Chain Management: Example - Walmart
- Real Estate: Example - Australian banks ANZ and Westpac
- Insurance: Example - Maersk [World Largest Shipping Company]
- Certificate of Authenticity: Example - Det Norske Veritas [DNV]
- Humanitarian Aid: Example – United Nations World Food Program

Walmart

- In partnership with IBM
- Tracking pork products across China
- Reduced the time it takes to track food from days to minutes
- 1% reduction in food borne disease in USA = $700B Savings
- 48MM people in USA become ill from food borne diseases

Australian banks: ANZ and Westpac

- In partnership with IBM
- Digitized commercial property lease guarantees
- Increased transparency
- Reduced risk, error and fraud

Maersk

- In partnership with Microsoft
- Shipping Insurance
- Successful 20 week proof of concept
- Make auditing aspects of a shipping supply chain easier
- Improve the tamper-resistance
- Sharing of data in realtime

Det Norske Veritas

In partnership with Deloitte

Instant verification of Certificates of Authenticity

90,000 certificates

Improve the tamper-resistance

Reduce fraud and counterfeiting

United Nations

United Nations World Food Programme

Uses Ethereum to Aid Syrian Refugees

10,000 Syrian refugees living in the Azraq camp in Jordan

Increased transparency

Reduction in fraud

Lower intermediary costs

UNITED NATIONS

Limitations Of Blockchain Technology

Early Stage

Lack of Awareness

Limited Available Technical Talent

It Is Immutable

No Reversals or Modifications

Key Management

Scalability

Time to Process

:Some Common Misconceptions:

Bitcoin is Anonymous

Bitcoin is Used to Launder Money

Blockchain is a Better Database

Blockchain is Bitcoin

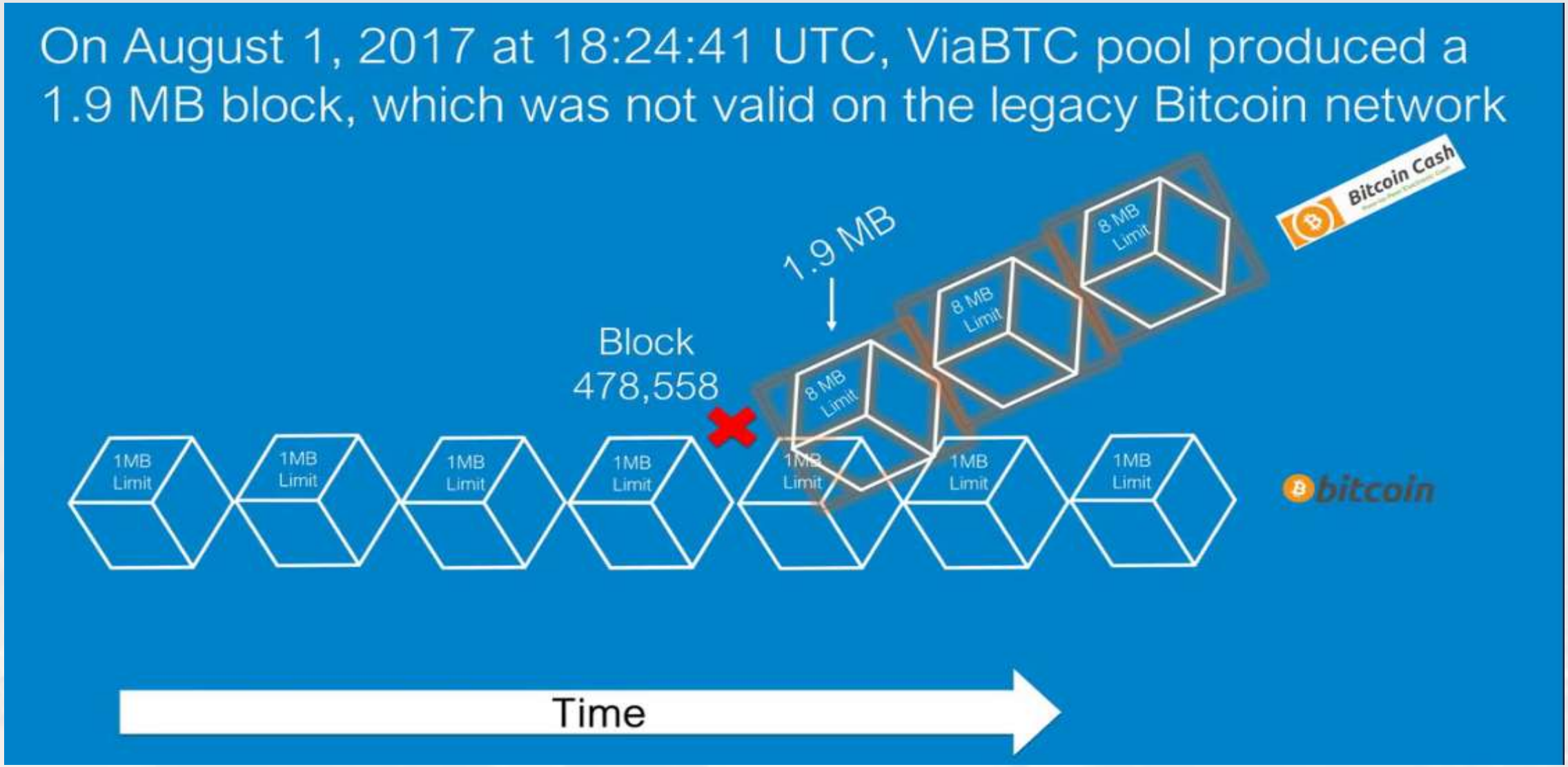
You Need to Buy a Full bitcoin

What is Bitcoin Cash?

A new cryptocurrency developed from a “Hard Fork” in the Bitcoin Blockchain.

Increases block size to 8MB from the 1MB limit prior to the fork.

Bitcoin Cash – How?



What is a fork?

A Fork takes place when a blockchain splits into two different paths forward.

Types: Hard and Soft

Hard Fork – Introduces a change that forces everyone to upgrade.

Soft Fork – Introduces change that is backwards compatible. Doesn't need upgrade.

Interesting Facts About Forks

Forks on Bitcoin happen on a regular basis

Two or more miners solve a block at same time – for a while there are extra chains

Eventually one of the chains wins over the other

Orphan block

Back to the Mempool

Hard Fork: Bitcoin Cash

Soft Fork: SegWit

UASF: User Activated Soft Fork

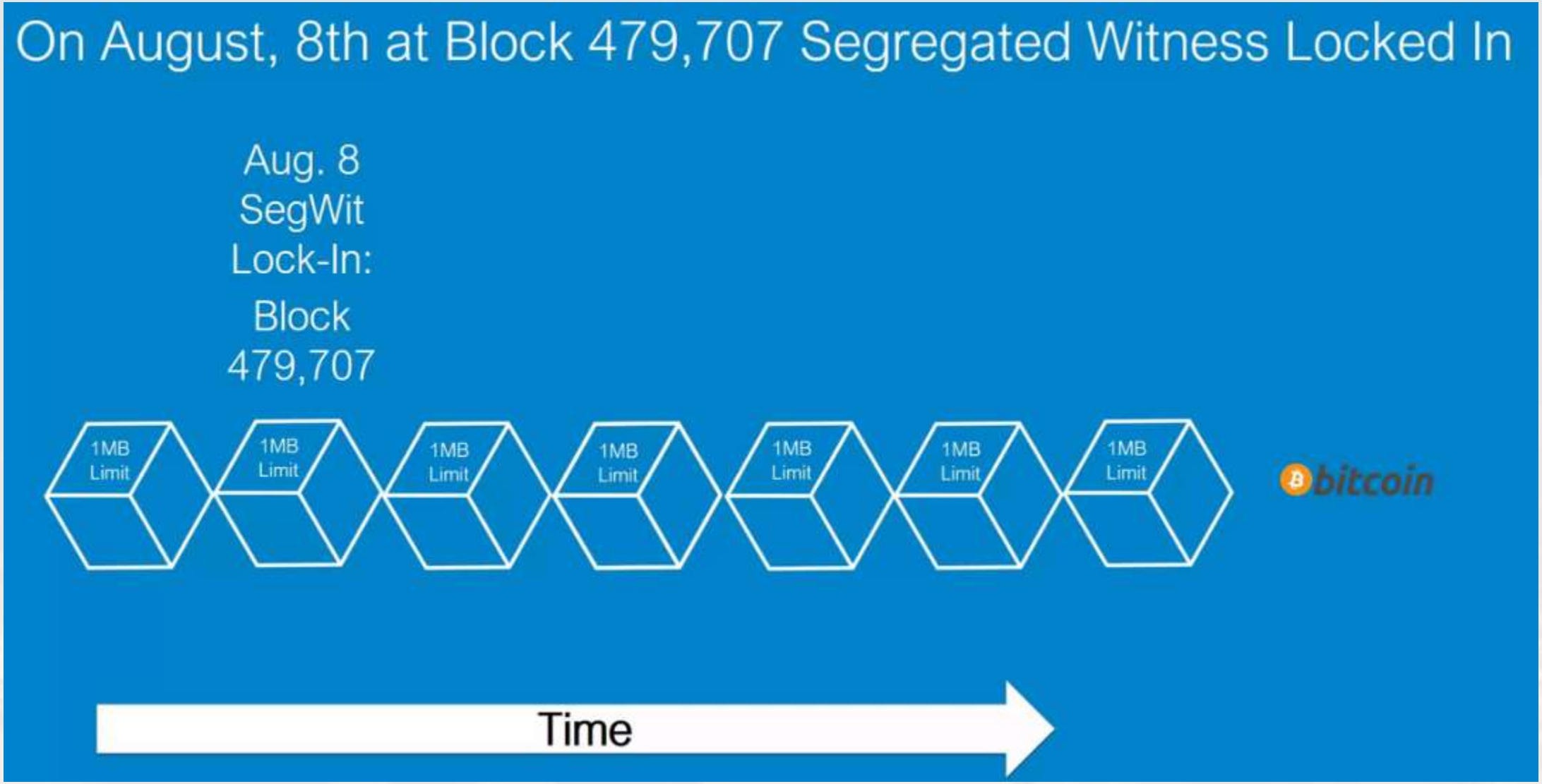
Locked In on 8th August 2017, at block #479,707

Official Activation on August 24th at block #481,824

Did not cause a split in chain

Replaces Block Size Limit with Block Weight Limit

SegWit [Segregated Witness]



SegWit [Segregated Witness] [Cont.]

SegWit [Segregated Witness] [About]

Protocol Upgrade

Improves scalability without increasing Block size

Addresses Transaction Malleability

Does not require upgrading to remain on the Blockchain

Did not cause a split in chain

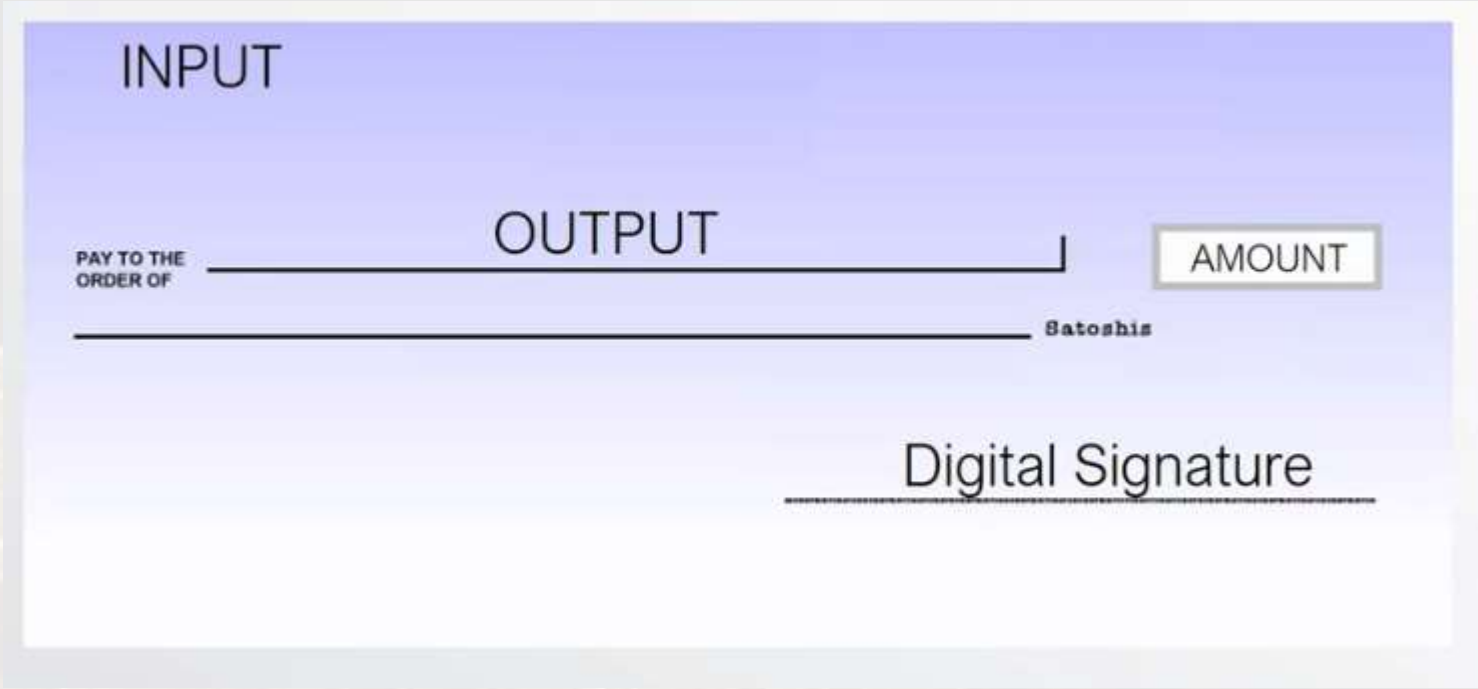
Components of Bitcoin Transections

Three Main Components:

Input

Amount

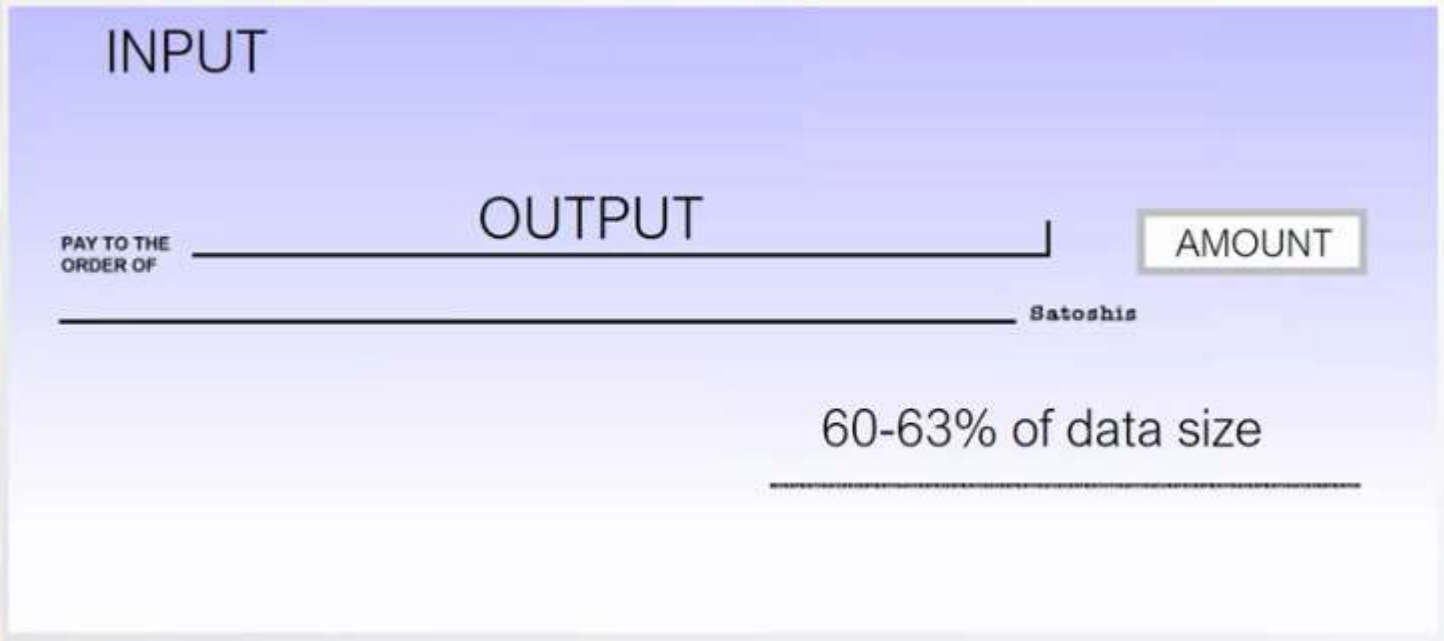
Output



Digital Signature: Transaction must be digitally signed using the owner's private key (the private key is a secret and never shared.)

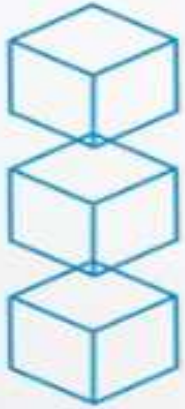
SegWit [Segregated Witness] [Works]

In a SegWit Transaction:
Signature data (Witness) is “segregated” to an extended block.



Digital Signature
Extended Block

Important Dates for Bitcoin



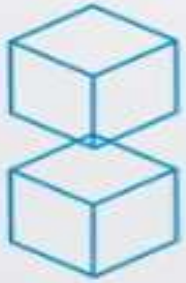
October 31st, 2008: Bitcoin Whitepaper

January 3rd, 2009: Genesis Block

May 22nd, 2010: First Retail Purchase

2 pizzas for 10,000 bitcoin (+/- $25 USD)

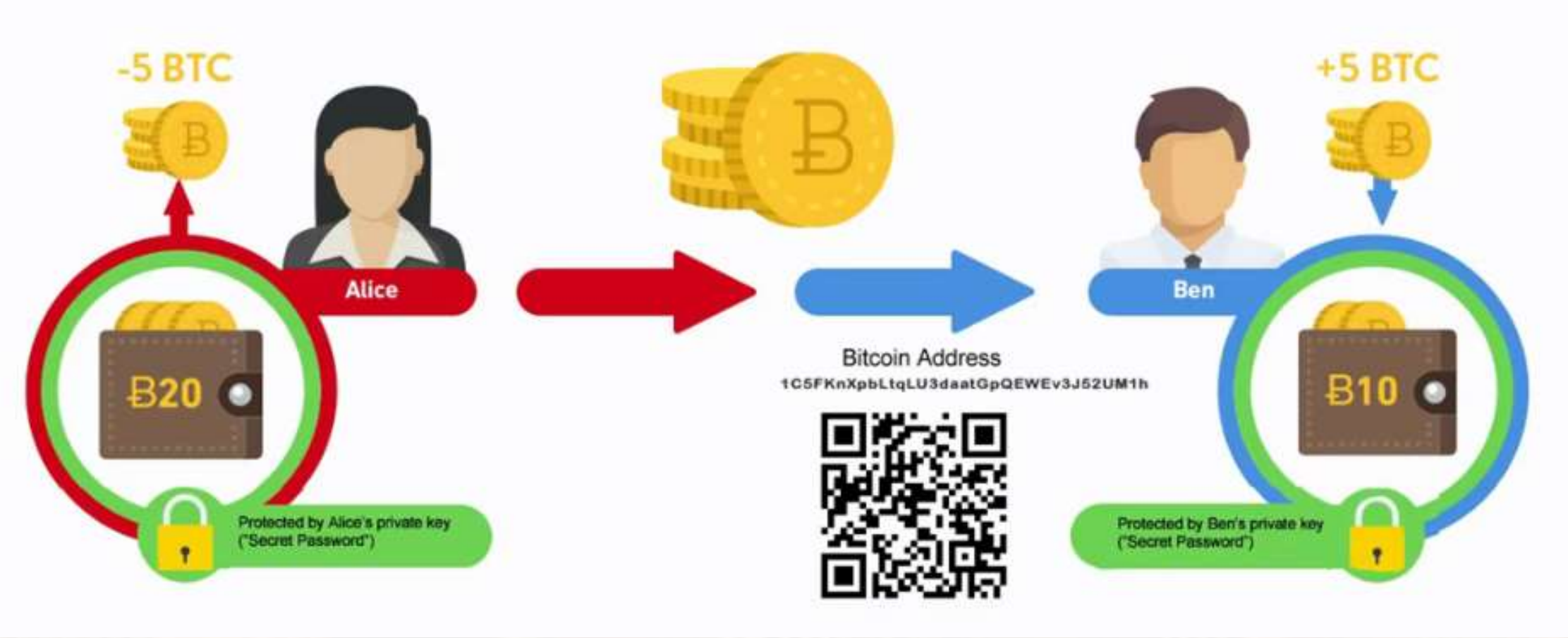
1BTC = $.0025 USD



November 28th, 2013: 1 BTC > $1,000 USD

March 2nd, 2017: 1 BTC > 1 Oz of Gold

:Sending Bitcoins:




Thank
you