Blockchain Specialist Program

Zeeshan Hanif
Qasim Shabbir
Hammad Ahmed

Blockchain and Cryptocurrencies are shaking the system

TECH

Cryptocurrencies are ‘clearly shaking the system,’ IMF’s Lagarde says

PUBLISHED WED, APR 10 2019 • 9:15 PM EDT

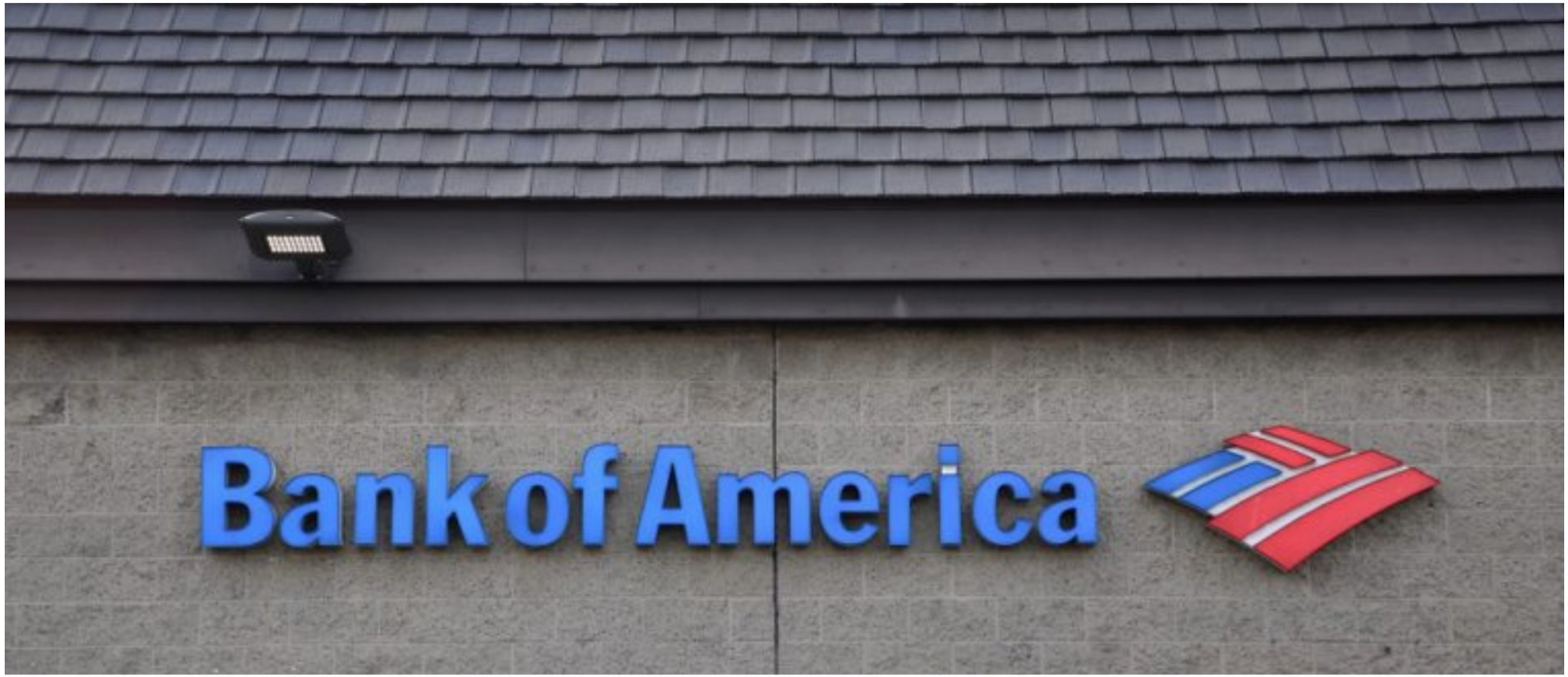
Elon Musk: 'Paper money is going away'

Published Wed, Feb 20 2019 • 11:52 AM EST • Updated Mon, Apr 8 2019 • 10:21 AM EDT

Catherine Clifford
@CATCLIFFORD

BANKING FEBRUARY 23, 2018 16:31

Bank of America Admits Cryptocurrencies Are a Threat to Its Business Model



Is Blockchain Technology the New Internet?

Blockchain is backbone of New type of Internet: The Decentralised Era

1. The main frames with dumb terminals (1960s)
2. The Desktop (1980s)
3. The Internet, all desktops connected (1990s)
4. Walled Gardens, all powers with big companies (Facebook, Google, Apple and Amazon)
5. The Blockchain Era, a decentralised internet (WEB 3.0)

Web 1.0

Web 1.0 was just a set of static websites with a load of information and no interactive content

Web 2.0

The global sharing of information spawned the age of ‘Social Media’. Youtube, Wikipedia, Flickr and Facebook gave voices to the voiceless and a means for like-minded communities to thrive.

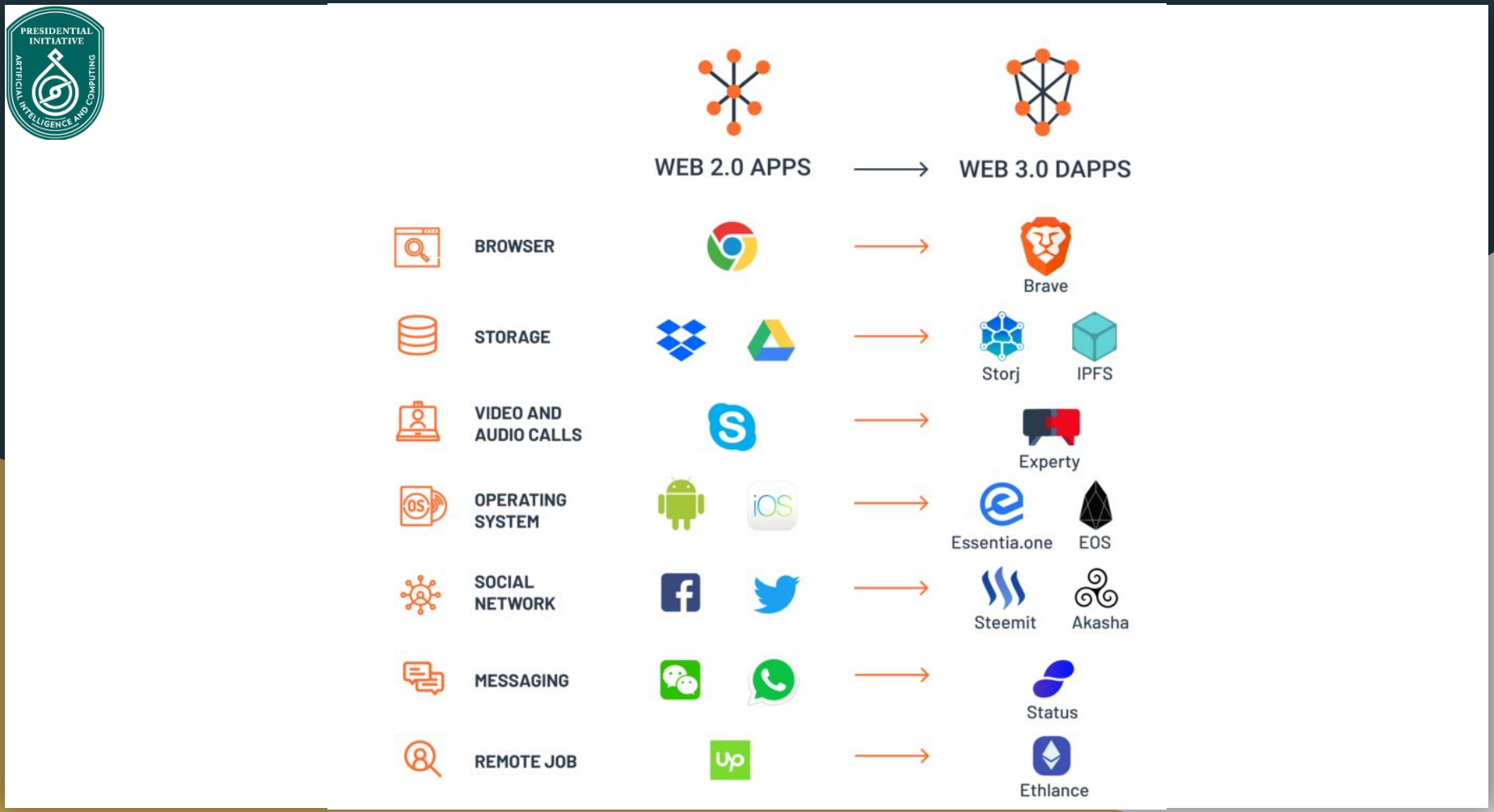
Information is money

As large companies realized the value of personal information they stockpiling the data in centralized server and start selling browsing habits, searches and shopping information to advertisers.

Web 3.0

Rather than concentrating the power (and data) in the hands of huge behemoths with questionable motives, it would be returned the rightful owners.

Decentralization was the idea; blockchain was the means.


WEB 2.0 APPS
WEB 3.0 DAPPS
BROWSER
Brave
STORAGE
Storj
IPFS
VIDEO AND AUDIO CALLS
Experty
OPERATING SYSTEM
iOS
Essentia.one
EOS
SOCIAL NETWORK
Steemit
Akasha
MESSAGING
Status
REMOTE JOB
Ethlance

Blockchain can do for business what the internet did for communication

Every second of every day, businesses exchange value with suppliers, partners, customers and others. By value, we mean goods, services, money, data and more.

Each exchange of value is a transaction. Successful transactions need to be fast, precise and easily agreed on by parties participating in the transaction.

Blockchain for business provides a way to execute many more of these transactions — a much better way.

Industries that can be Disrupted by The Blockchain

- Banking and Payments
- Supply Chain Management
- IOT
- Insurance
- Private Transport and Ride Sharing
- Online Data Storage
- Charity
- Voting
- Government
- Health Care
- Online Music
- Retail
- Crowdfunding

Problem with Traditional System

1. Centralized Control
2. Need to Trust
3. 3rd Party/Middleman
4. No Transparency
5. Mutable

It all started with Idea: A Digital Currency

1. David Chaum first proposed the concept of e-Cash in 1982
2. David Chanm then founded a company called DigiCash.
3. It uses cryptography security and anonymity
4. Idea had same problem as with traditional currency, it requires central clearing house or single point of trust
5. DigiCash declared bankruptcy in 1998
6. Many other tried faced the same fate

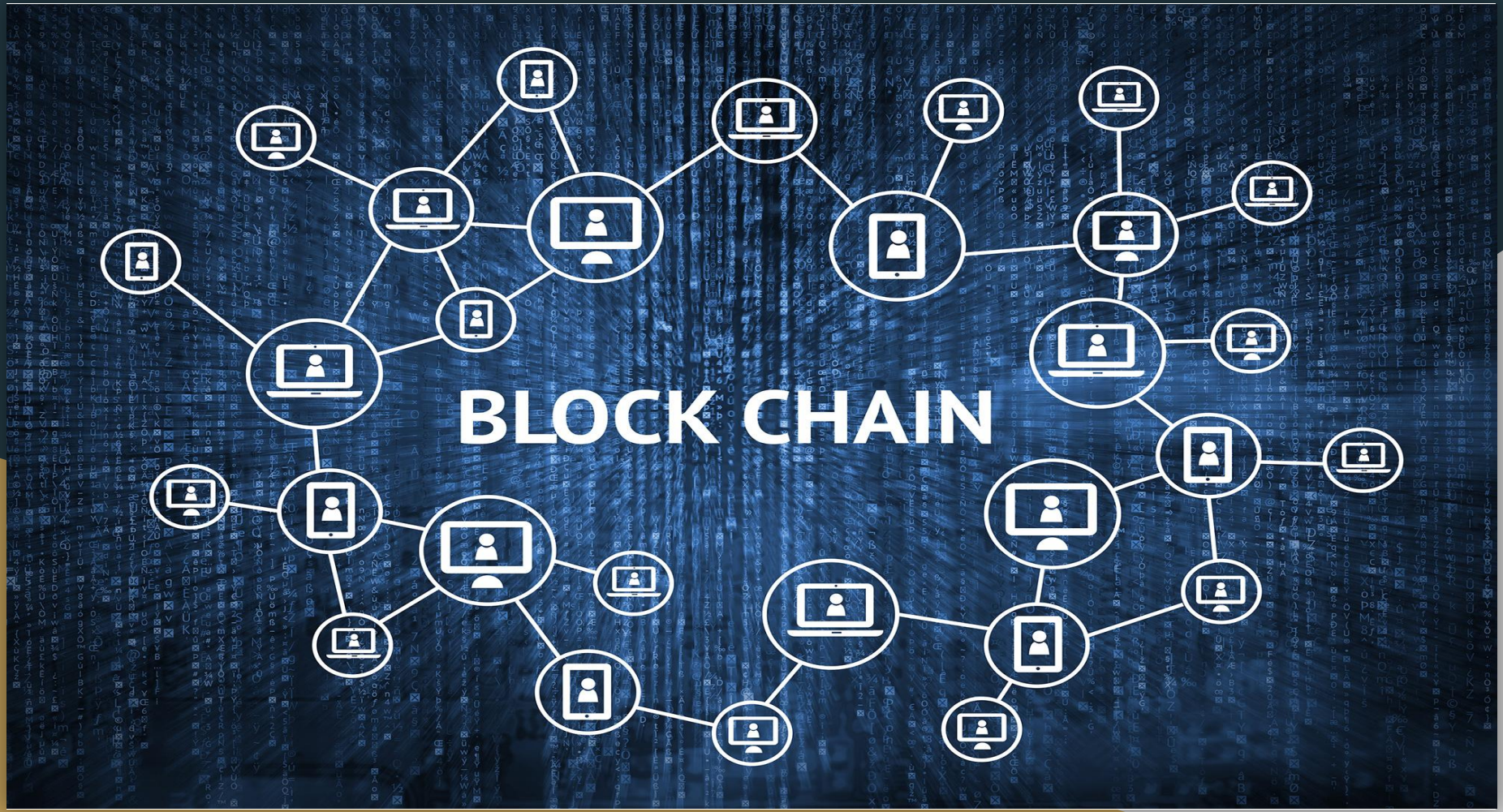
DIGI CASH®

Bitcoin

1. In 2008 a white paper was published: "Bitcoin: A Peer-to-Peer Electronic Cash System." by Satoshi Nakamoto
2. In 2009 first-ever block of bitcoin, known as the Genesis Block, was mined
3. Bitcoin uses:
    a. Secure digital signatures
    b. Not requiring the use of a third party
    c. Proof-of-work
    d. Hashing the transactions together to form a chain
4. Satoshi Nakamoto is unknown person or group of people, wrote the Bitcoin paper
5. Satoshi Disappears in December 2010

Bitcoin Properties

1. Decentralised – peer to peer ledger of balances
2. Immutable – can never be changed, transactions are permanent.
3. Fungible – each btc is equal, maintains it value (not like a banana)
4. Permissionless and without borders – anyone can participate by downloading software.
5. Divisible – down to 8 decimal places
6. Scarcity – 21 million coins ever
7. Transferrable – can send any amount in seconds, compare to gold.


BLOCK CHAIN

What is Blockchain

“The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.” – Don & Alex Tapscott, authors Blockchain Revolution (2016).

What is Blockchain

Many similar definitions

1. Blockchain is a distributed, decentralized, public ledger.
2. In Simplest of terms, Blockchain is a time-stamped series of immutable record of data that is managed by cluster of computers not owned by any single entity. Each of these blocks of data (i.e. block) are secured and bound to each other using cryptographic principles (i.e. chain).

0x8aa1d85a79756bffd81e1811cff21c7dad8aee258dd1de60e116ff0fb8906738


MINE!

The Core Principles of Blockchain

1. Distributed ledgers
2. Security,
3. Trustless
4. Decentralization
5. Group consensus
6. Immutability
7. Transparent

Blockchain Uses Old Technology

1. Accounting Ledger
2. Cryptography
3. Computer Network Technology/Peer-To-Peer network

Key Concepts that make blockchain secure and immutable

1. Hashing
2. Cryptography
3. Mining

1) Hashing, one way encryption

1. A hash function takes some input data and creates some output data.
2. To expand on this concept, a hash function takes an input of any length and creates an output of fixed length.
3. It takes an input string and created a string of random letters and numbers “a0680c04c4eb53884be77b4e10677f2b”.
4. This is referred to as the message digest.
5. It is also known as the digital fingerprint. This is because there is no way this digest can represent any other string. If I try and modify this the message digest will be completely different.

One Way Street

1. Another property of hash functions are they are one way.
2. It is really easy to calculate a message digest but given the digest, it is near impossible to figure out in the input.
3. Again, not impossible but it will take another billion years or so.

SHA-256 Hash Calculator

http://www.xorbin.com/tools/sha256-hash-calculator
https://passwordsgenerator.net/sha256-hash-generator

2) Cryptography -- Public-Key encryption Demo

http://cobweb.cs.uga.edu/~dme/csci6300/Encryption/Crypto.html

3) Mining and Understand Block/ Blockchains

https://anders.com/blockchain/


bitcoin

Forbes Billionaires Innovation Leadership Money Consumer Industry Lifestyle Featured BrandVoice Lists Advisor

37,578 views | Apr 16, 2019, 11:19am

Bitcoin Is The New Gold

Clem Chambers Contributor
Intelligent Investing Contributor Group
Investing

https://www.forbes.com/sites/investor/2019/04/16/bitcoin-is-the-new-gold/#56a24c51239a

What is Bitcoin?

1. A Collection of concepts and technologies.
2. It behaves like conventional currencies.
3. Can be purchased, sold, and exchanged for other currencies at specialized currency exchanges.
4. They are completely virtual with no physical existence.
5. Fast, Secure and Borderless

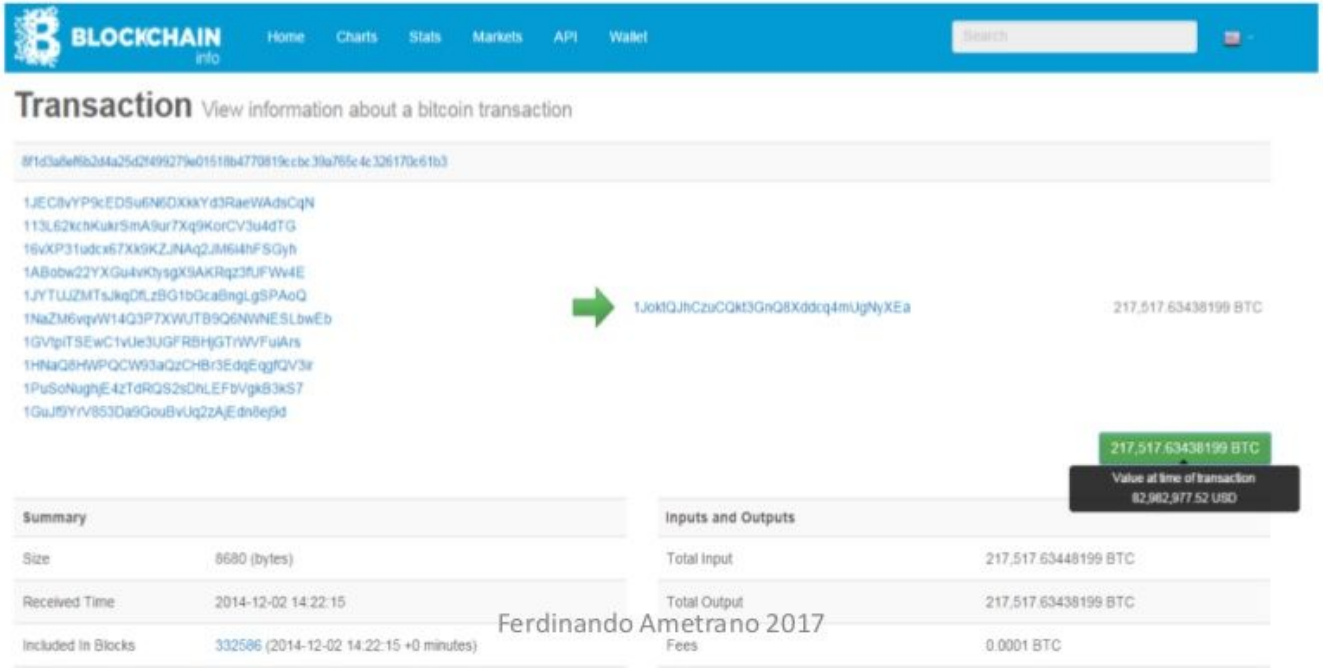
How it works

1. Unlike traditional currencies, bitcoin are entirely virtual
2. The coins are implied in transactions that transfer value
3. Users own keys that proves ownership of bitcoin in the bitcoin network
4. User sign transactions with keys to unlock the value and spend it by transferring it to a new owner.
5. Keys are often stored in a digital wallet
6. Possession of the key is the only prerequisite to spending bitcoin, putting the control entirely in the hands of each user.

A Bitcoin Transaction

https://blockchain.info/tx/8f1d3a8ef6b2d4a25d2f499279e01518b4770819ccbc39a765c4c326170c61b3

About $83M transacted with $0.04 fee



How it works?

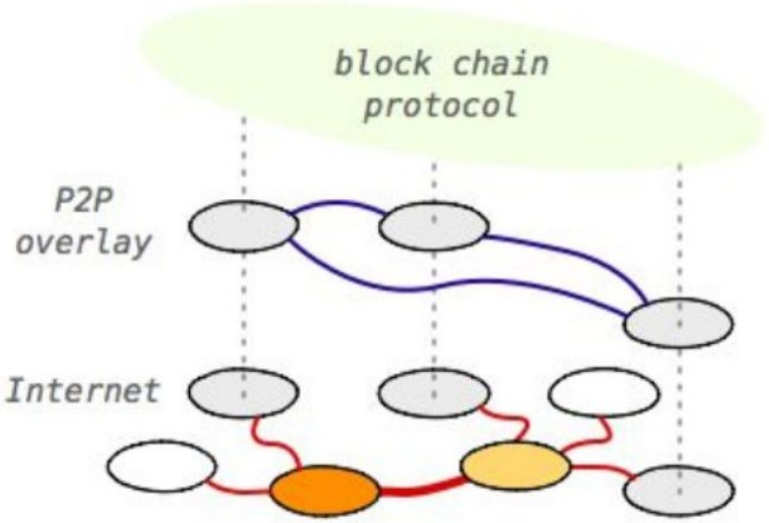
- Peer to Peer System
- Created through a process called “Mining”
- Every 10 minutes (on average)
  - Miner validate transactions
  - Rewarded with brand new bitcoin

What is Mining?

- Decentralizes currency-issuance and clearing function.
- Regulate by built-in algorithm
- Someone succeeds every 10 minutes
- Every 4 years halves the rate of new bitcoin generation.
- Ensures 21 million bitcoin generates by year 2140.

Combination of 4 key innovations

- A decentralized peer-to-peer network (the bitcoin protocol)
- A public transaction ledger (the blockchain)
- A set of rules for independent transaction validation and currency issuance (consensus rules)
- A mechanism for reaching global decentralized consensus on the valid blockchain (Proof-of-Work algorithm)



Why digital money never succeed before?

1. Can I trust that the money is authentic and not counterfeit?

2. Can I trust that the digital money can only be spent once (known as the “double-spend” problem)?

3. Can I be sure that no one else can claim this money belongs to them and not me?

Double Spending Problem

- In digital cash schemes, a single digital token, being just a file that can be duplicated, can be spent twice.
- A centralized trusted party has always been required to prevent double spending.

History of Bitcoin

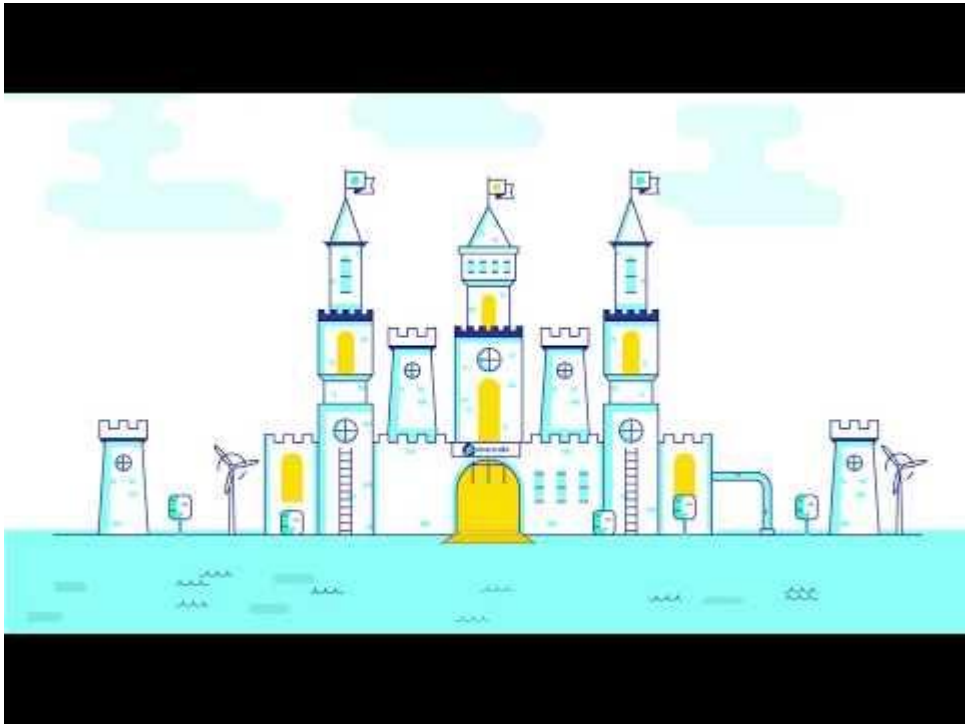
- 2008 Satoshi Nakamoto publish white paper

  “Bitcoin: A Peer to Peer Electronic Cash System” https://bitcoin.org/bitcoin.pdf

- 2009 Bitcoin network started
- 2010 Handed the responsibility to group of volunteers.
- April 2011 Satoshi Nakamoto withdrew from public. Owns 1M bitcoins.
- August 2017, hard-forked named **Bitcoin Cash**
- November 2017, another hard-forked named **Bitcoin-Gold**

Byzantine General Problem - BGP

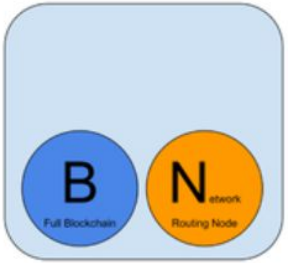
The fundamental question of the BGP is how to establish trust between otherwise unrelated parties over an untrusted network like the internet.



Bitcoin Client Software

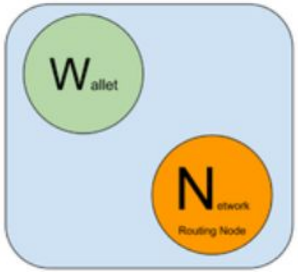
Reference Client (Bitcoin Core)

Contains a Wallet, Miner, full Blockchain database, and Network routing node on the bitcoin P2P network.



Full Block Chain Node

Contains a full Blockchain database, and Network routing node on the bitcoin P2P network.



Lightweight (SPV) wallet

Contains a Wallet and a Network node on the bitcoin P2P protocol, without a blockchain.

Different types of bitcoin wallets

Desktop


Bitcoin-QT


MultiBit


Armory


Electrum

Mobile


Bitcoin Wallet


Mycelium


Blockchain


Coinbase

Cloud


Coinbase


Blockchain

Different types of bitcoin wallets

Different types of bitcoin wallets

HOW A BITCOIN IS MINTED

The birth of a new Bitcoin begins when a number of existing Bitcoins are used in transactions.