
Blockchain

Hodl

Consensus

Fork

Fiat

Hyperledger

ICO

DLT

Crypto

Miners

STO

Node

DAO

PoW

Smart Contract

Stablecoin

dApp

Bitcoin

MARINSTEIN & COMPANY

Money = Power >

"software is eating the world"

- Marc Andreessen


$721B


$740B


$812B


$417B


$794B

Technology = Power >

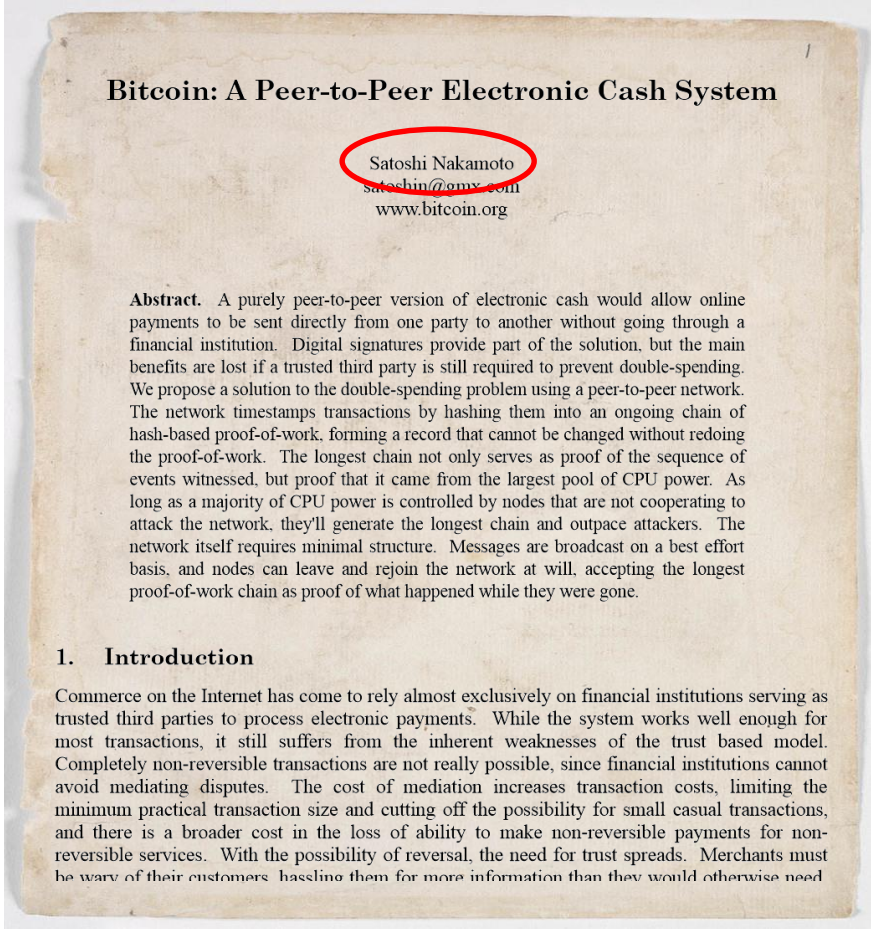

UBER


Alibaba.com


airbnb

Money = Technology

- **P2P electronic cash**
- **Solved Double Spend Problem**
- **Transfer money without 3rd parties**
- **No government control**



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

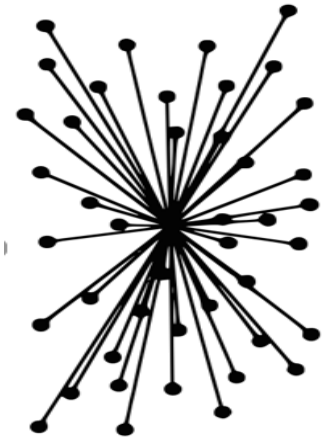
Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible 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

1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

bitcoins

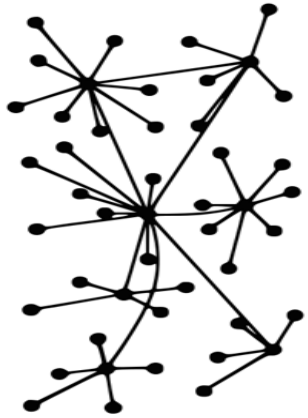
blockchain

Centralized



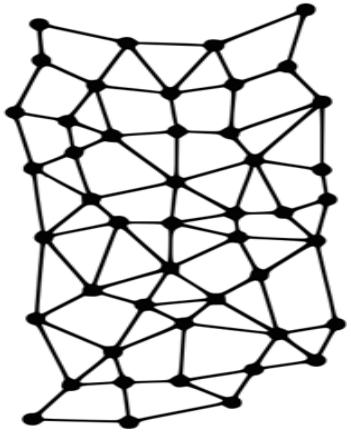
- Central body controls transactions and records
- Other parties maintain their own copies

De-Centralized



- Intermediaries maintain local records of transactions
- Other parties maintain their own copies

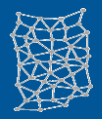
Distributed Ledger



- Nodes hold their own copy of all transactions

Properties of blockchain

Secure – based on 20+ years of cryptography research



Resilient – no single point of failure in the network

Immutable – auditable history of blocks, highly tamper proof

Integrity – consensus is reached among the majority of participants

Logic – programmable, automatically trigger transactions

ethereum

- 2014 - Improved upon Bitcoin protocol
- Added Smart Contracts and decentralized application platform
- Allows developers to build applications – “dApps”
- World computer powered by blockchain
- Enables services (payments, computing, storage) without a central party

Public

ethereum litecoin augur IOTA

- Anyone can join
- Transactions visible to all
- Anonymous
- Use tokens
- Heavily forked
- Slower

Private

ripple HYPERLEDGER part of Digital Asset Holdings SETL corda HASHED HEALTH

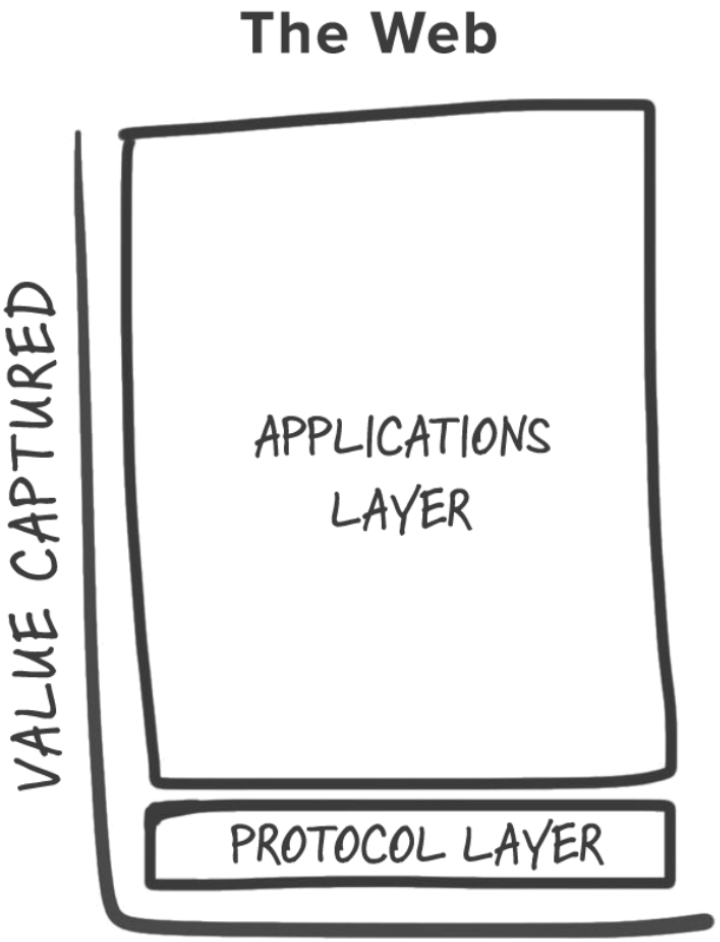
- Requires invitation to join
- Transactions are confidential
- Identity is known
- Don't need tokenization
- Industry consortia
- Faster

Use Cases

- Banking
- Healthcare
- Supply Chain
- Voting
- Real Estate
- Cryptocurrency
- Music
- IoT

- Ecommerce
- Payments
- Remittance
- Micro-lending
- P2P lending
- Digital rights
- Wagers
- Escrow
- Equity
- Debt
- Derivatives
- .....

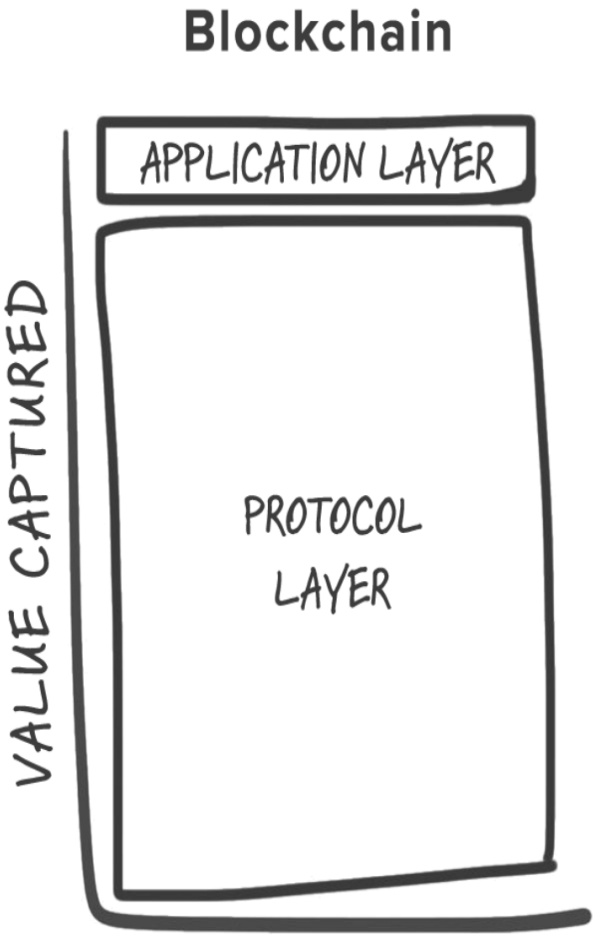
Web Protocols



- Highly centralized
- Proprietary data layer
- Value captured at the application layer
- Could not invest in protocol layer
- Winner take all

Google
amazon
NETFLIX

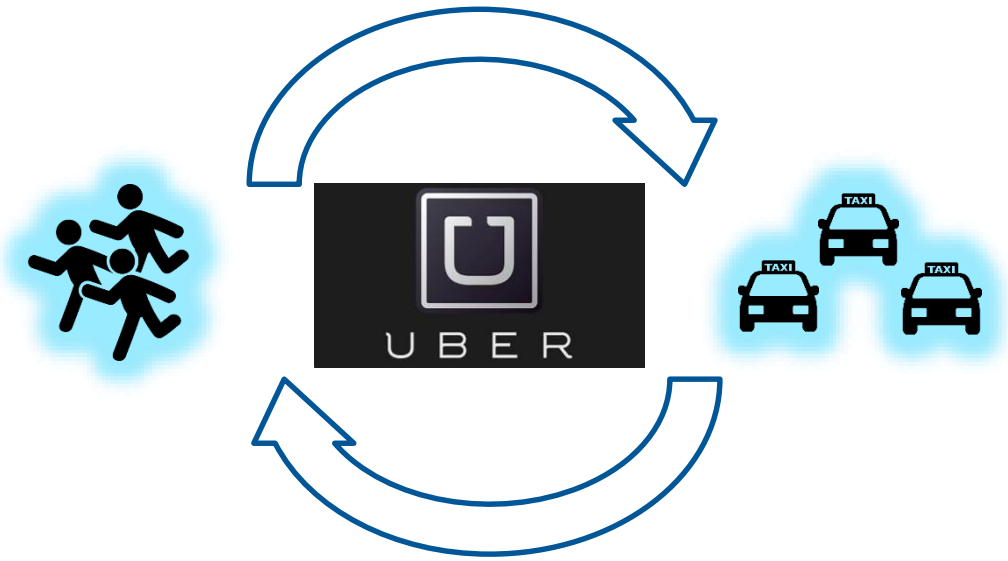
Blockchain – a New Web Protocol



- Shared data layer - democratized
- Reduced barriers to entry – open source
- Value captured at the protocol layer
- Token ecosystem creates incentives
- Value of protocol grows faster than applications

bitcoin

Current Market Dynamic



- Coordination platform
- Uber stores credit card
- Users download app
- Eventually creates higher switching costs
- Market consolidates around a single leader
- Value captured by shareholders

Blockchain "Transit Protocol"

1. 

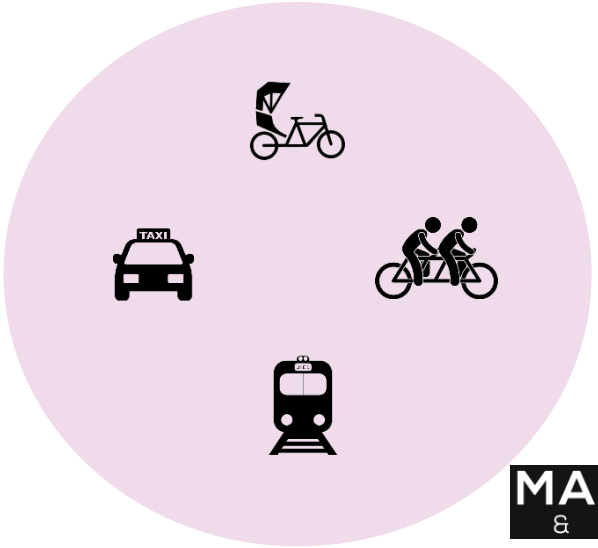
   Blockchain stores metadata

   past trips, credit card, favorite locations

2. 

   "I'm here and I want to go there"

3. **Receive competing offers**



MARINSTEIN & COMPANY

Digital Token Economics

1 Developer builds transit app

2 Riders and drivers purchase tokens & use service

4 Attracts more developers, riders, drivers

3 Market makers create liquidity

- Token supply is controlled by an algorithm
- Economic value captured by developers, riders, users, speculators
- Value is created by improving the protocol, maintaining ledger, using the service
- Moves away from winner take all economies

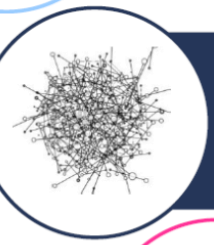
Security Tokens – Tokenization of Assets

- Participation rights for real-world assets
- Ownership recorded on blockchain
- Fractional ownership of real estate, gold, fine art, securities
- Democratized investing
- Legal and regulatory hurdles to overcome

Evolution of Crypto – Autonomous Next

Bitcoin
Global macro trade

2008
Store of value
$7-100 Trillion



Enterprise Blockchain
Private consortia within industries

2014
$500 Billion of costs
in financial services alone

Decentralized Apps
Smart contracts and ICOs

2015
All digital economies
and their operations

POLYMATH

Smart Securities
Institutionalization and tokenization

2018
$500 Trillion
All asset classes

Central Bank Digital Currency

- Address the impact of digitization
- Payments are undergoing significant change
- Use of banknotes and coins declining in society
- IMF framework for central banks
- Sweden issuing e-Krona

The Pain

Blockchains are a technological innovation that will fundamentally change how we exchange value

Upcoming Classes

Feb. 26 – Blockchain Use Cases

Mar. 26 – Blockchain Strategies for Success

https://citi.uconn.edu/BlockchainDevelopment

Thank You !

https://citi.uconn.edu/

jeff@marinsteinandco.com

203-918-8408