The Blockchain and Other Payment Trends

Brad Smith, AAP

Enterprise Payments

Capital One

For decades, cryptocurrencies have struggled with a few key challenges

- Early attempts to develop digital currency required a central authority
- Centralized issuer provided the currency and validated all transactions

- Advent of “proof of work” concept to create money
- Money earned would be relative to amount of computing power provided
- Still required central party to maintain ownership records

- Concept of voting to reach consensus is introduced
- As long as majority of voters are honest, the correct outcome is obtained
- Vulnerable to Sybil attack, where a malicious entity could create fake voting profiles

Key Challenges

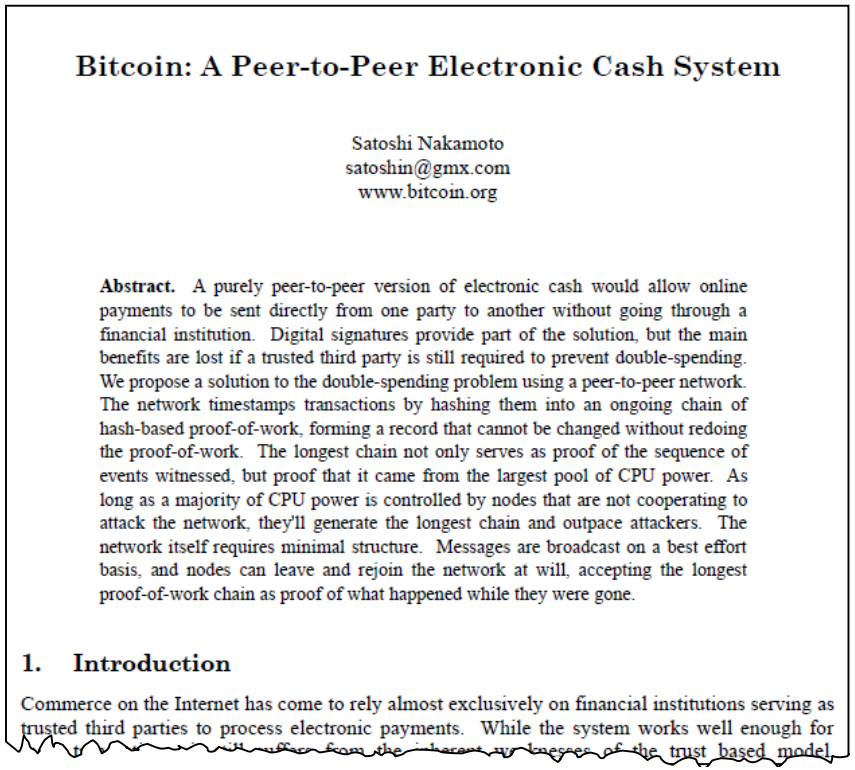
- **Generate currency**
- **Validate ownership of currency**
- **Validate transactions between unrelated entities**
- **Avoid double spend**
- **Accomplishing all these without the need for a central 3rd party**

Source: Technology Strategy

Bitcoin is the first digital currency to use blockchain technology to solve the previous challenges

Bitcoin White Paper

(excerpt)



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

Originally published in 2008 as a proposed alternative to cash

Blockchain as a Solution

- **First practical solution for electronic payment system without a central authority (i.e., Federal Reserve)**
  - Ensures ownership of promised asset
  - Verifies and records all transactions
  - Generates and issues Bitcoins through proof-of-work
- **All computers on the network (nodes) share a living document of all historical network transactions (distributed public ledger)**
- **Nodes are communicating with each other to maintain consensus**

Source: https://bitcoin.org/bitcoin.pdf

Crypto currencies like Bitcoin provide an entirely new approach to payments

Bitcoin is a currency

- Is used to conduct transactions across the globe largely by US, China, Germany and UK
- Daily transaction volume of ~$200M

Bitcoin is a secure, distributed public ledger

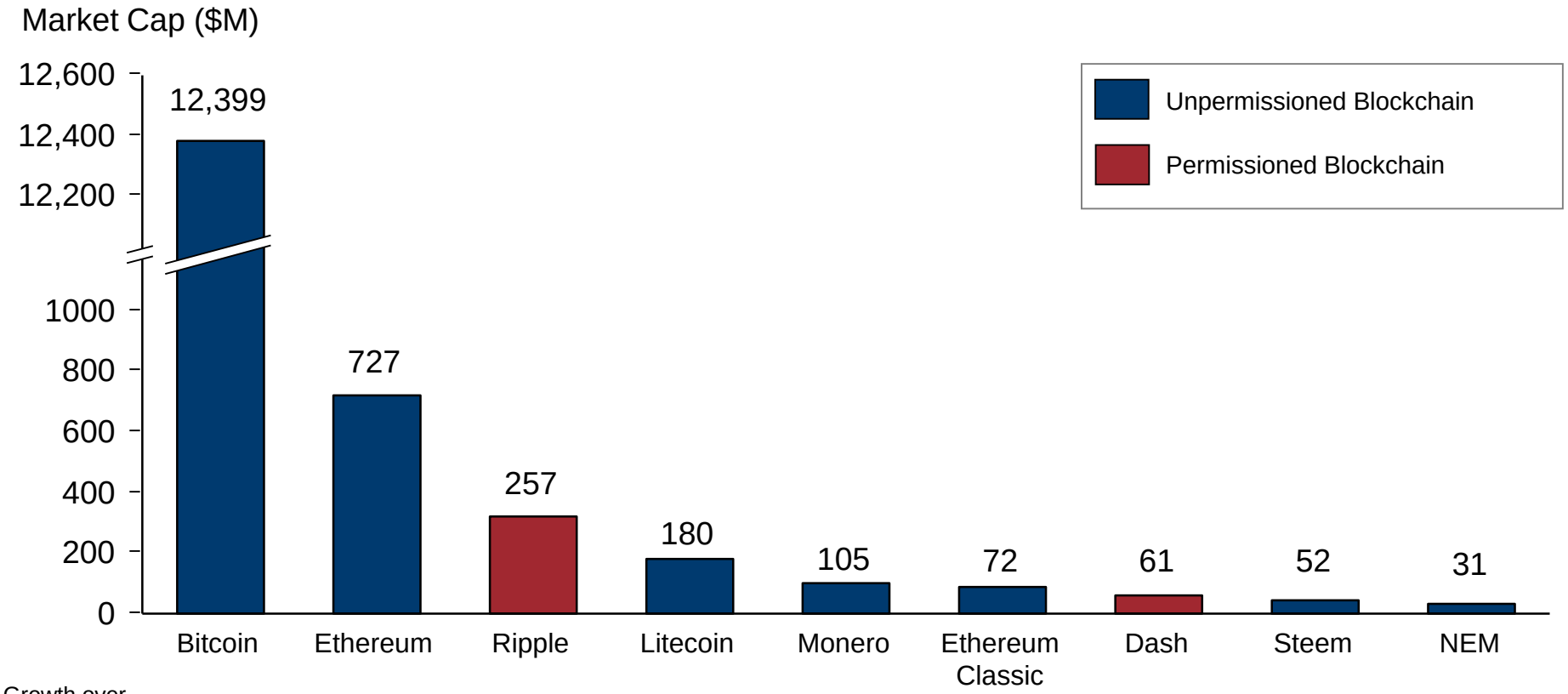
- All bitcoin transactions are maintained in a public ledger called the “blockchain”

Bitcoin is a transaction network

- Merchants and consumers can directly transact
- Exchanges facilitate purchases/sales into other currencies

While Bitcoin is the most established, alternatives are constantly emerging

Top 10 Cryptocurrencies by Market Cap as of December 2016



	Bitcoin	Ethereum	Ripple	Litecoin	Monero	Ethereum Classic	Dash	Steem	NEM
Growth over last 6 months	26%	-37%	28%	-25%	643%	N/A	19%	174%	69%
Year introduced	2009	2015	2012	2011	2014	2015	2014	2016	2015

There are over 630 cryptocurrencies available with a combined market cap in excess of $14.4B

Source: coinmarketcap.com

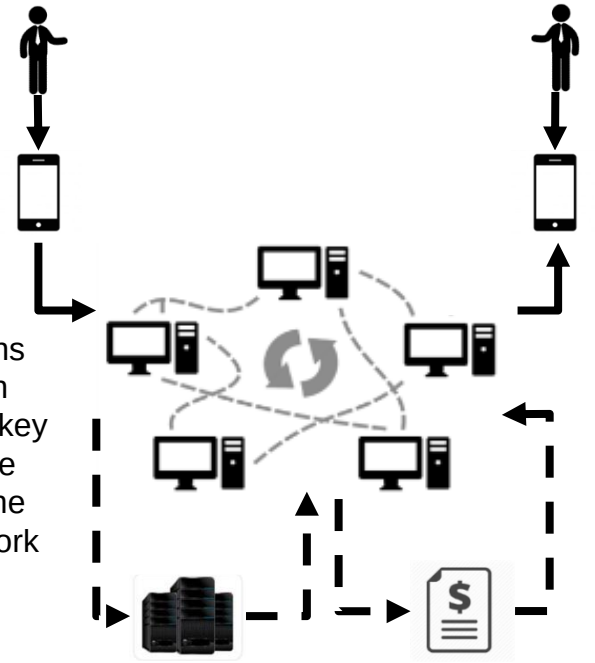
The Bitcoin protocol uses a shared ledger to record transactions and maintain ownership of assets

What is a blockchain?

- **A blockchain is a public ledger that records transactions**
- **Each network node stores its own copy of the shared ledger**
- **Network nodes can validate transactions, add them to their copy of the ledger, and then broadcast these ledger additions to other nodes**
- **Periodically, a new group of accepted transactions (a "block") is created, added to said blockchain, and published to all nodes**

How do transactions on the Bitcoin blockchain work?

The sender and receiver enter the blockchain through a digital wallet or exchange service



The sender signs the transaction using his private key and submits the transaction to the blockchain network

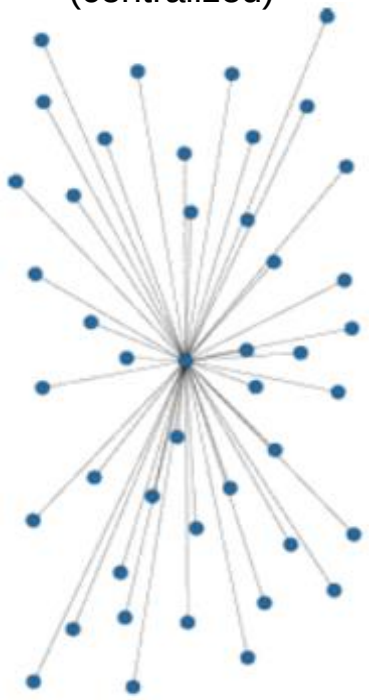
The nodes in the network individually verify that this transaction is legitimate, and then record the transaction in the ledger

Computers set up to verify transactions using cryptographic hashing ("mining"), compete to be the first to validate a set of transactions ("block")

Blockchain technology presents a possible solution to trust problems that exist in transactions today

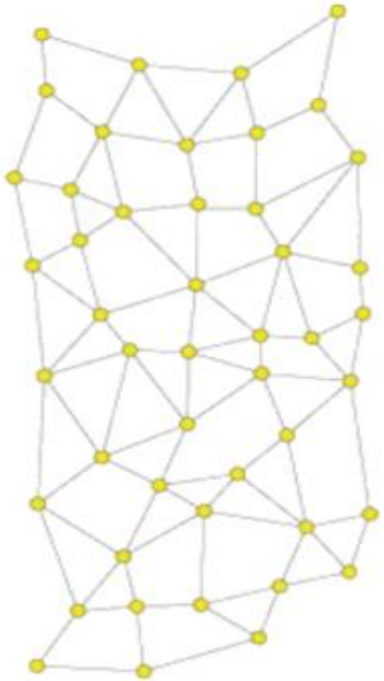
Today we overcome the problem of trust between market participants by using trusted third-parties (intermediaries)
(e.g., banks, attorneys, governments)

Current payment processing network
(centralized)



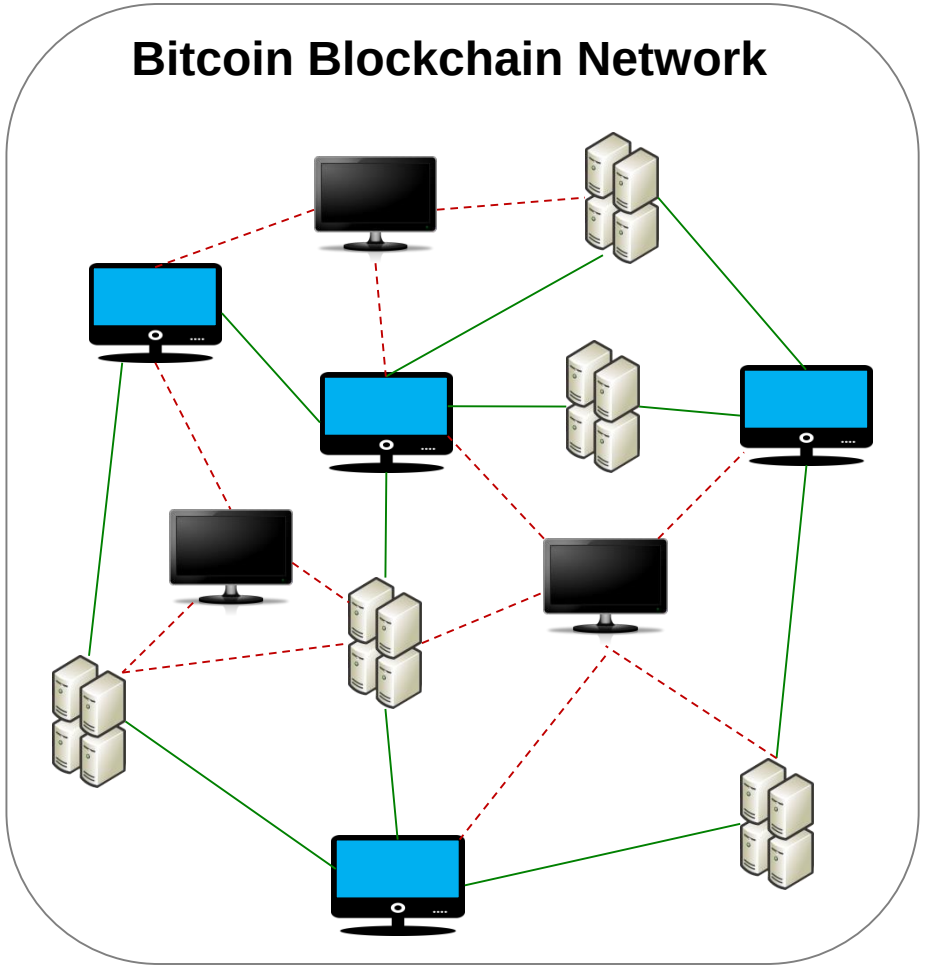
Block chain technology eliminates the need for third-parties by creating a real-time, shared digital record of all transactions (shared public ledger)

Block chain-based network
(distributed)



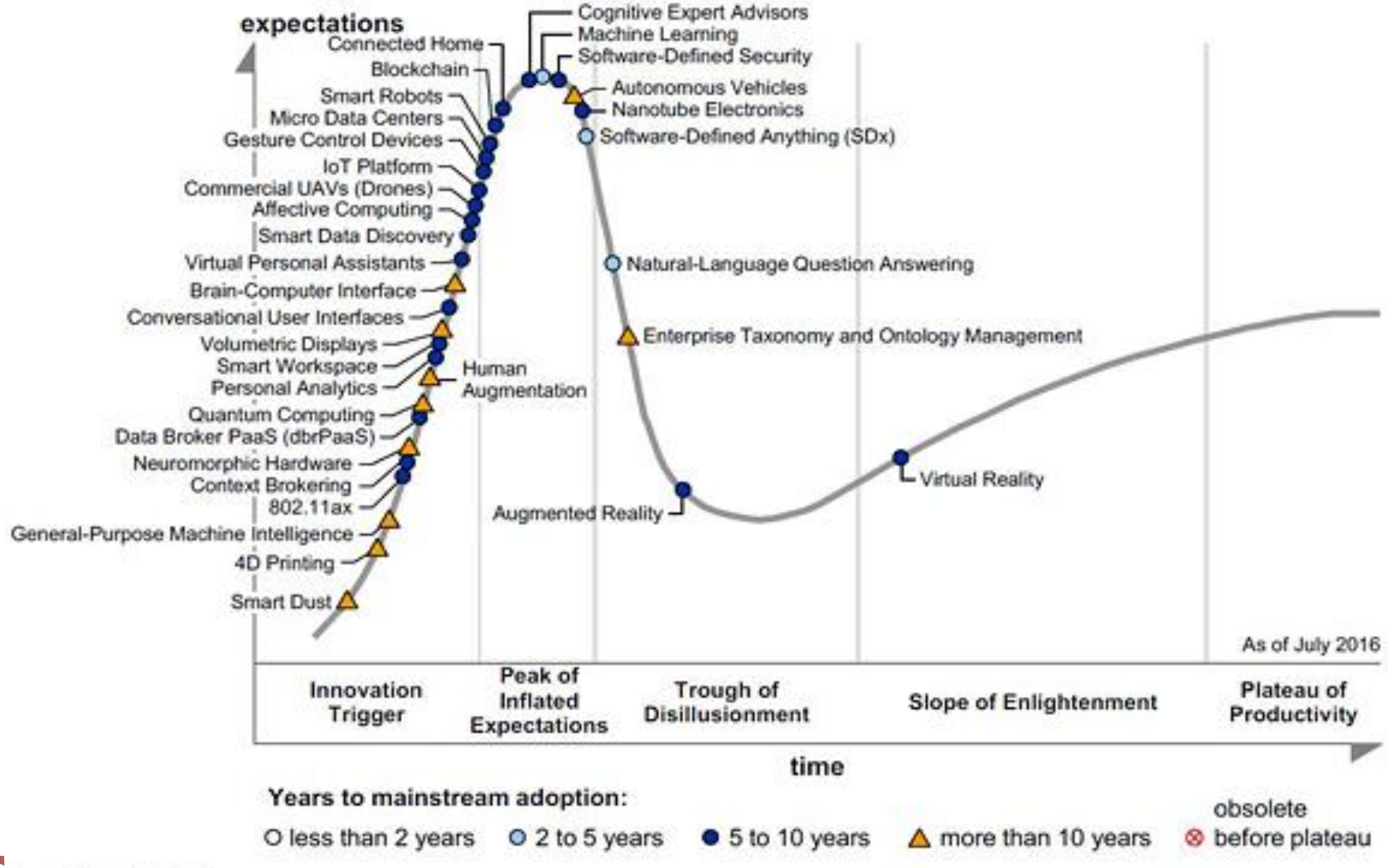
The network needs a decentralized method of maintaining consensus on the ownership and transaction of assets

- **When Bob sends Alice bitcoins, the transaction is transmitted to the peer-to-peer network**
- **However, this does not guarantee it shows up on the ledger**
  - Some nodes may not be connected to the network
  - Bob may have promised that same asset to another user or never owned it
- **The network needs a method to verify transactions and communicate those transactions to all nodes**



Because the ownership and transfer of bitcoins is nothing more than other nodes agreeing that a given party owns those bitcoins, it is necessary to maintain consensus on the state of the ledger

Gartner Hype Cycle for Emerging Technologies - 2016



Source: Gartner (July 2016)

The applications for blockchain technology span far beyond virtual currencies

NOT COMPREHENSIVE

Applications of Blockchain Technology

Payments and Lending

- Virtual currencies
- Global money movement (remittance)
- Payment infrastructure (e.g.., ACH replacement)
- Peer-to-peer lending
- Micro-finance

Smart Contracts
(contracts executed by computer protocols)

- Trade finance / escrow services
- Financial instruments (e.g.., stocks, bonds, options)
- Digital autonomous corporations (DACs)
- Transaction platform for the Internet of Things (IoT)

Records and Asset Management

- Public and private record keeping
- Land/ vehicle titling
- Asset identification, management, and transfer

Distributed Activities

- Crowd-funding
- Digital voting

Investment Platforms

- Currency exchange
- Stock exchange
- Securities trading
- Clearing platform

For Banks, the biggest opportunities are in applications of Federated (or Private) Blockchains

	Public Blockchain	Federated (or Private) Blockchain	Central Infrastructure (not Blockchain tech)
	Fully decentralized network without any third-party ownership	Decentralized network is managed and controlled by a group of organizations	Central network is managed and controlled by a single organization
Advantages	• **Leverage existing public Blockchain network resulting in lower cost** • **Network effect** (including transactions across multiple industries) • **Open network** (anybody can join easily)	• **Access can be tightly controlled, leading to less regulatory concerns** • **Faster due to lack of need for proof of work** • **Allows for interoperability between private blockchains**	• **Most efficient (no need for cryptographics)** • **Full privacy can be ensured** • **Mature technology with minimal unknown risks**
Disadvantages	• **Relatively inefficient compared to Private Blockchains leading to capability limitations** (e.g.., limited transactions per second, long settlement times) • **Regulatory concerns due to anonymity**	• **Requires some level of trust between nodes/organizations** • **More expensive to develop and manage than Public Blockchain** • **Closed network**	• **Requires trusted party to operate network** • **Limited application** (usually built for specific use cases) • **Single point of attack risk / poor resiliency** • **Likely more expensive to own and maintain**
Key Application Areas	• Applications without trusted intermediaries • Open marketplaces (where anybody can join) • Distributed activities such as voting for in areas without trust	• Transaction network and marketplaces between fairly trusted parties (e.g.., banks)	• Applications requiring highest performance (transaction throughput, settlement time) • Desire for full control and privacy

We are moving to a world where customers will engage with many different blockchains for different purposes

Each customer-based use case has one commonality: the need for authenticating identity of the customers

Could the issuance of fiat currency be digitalized too?

Payments Technology and Trends

Chatbots for Banking and Commerce

Increased Operational Efficiency

- Technology improvements allow for automation of mundane tasks
- May alleviate costs for expensive physical call centers
- Allow associates to spend time on more complex tasks and issues

Improved Customer Experience

- Provides seamless digital banking experience
- Chatbots can work on multiple messaging platforms allowing customers to use their preferred messaging app
- Due to insights gained from messaging apps, authentication will be easier

Unique Data Insights

- Data. So. Much. Data.
- Digitization of the customer data will improve the UX
- Conversational AI can help banks better analyze the data

The Invasion of the “Pays”

Multiple Payment Offerings

- **Apple Pay, Samsung Pay, Mercedes Pay, WalMart Pay, Android Pay, Chase Pay, PayPal, Masterpass, VISA+Honda, Mobile Pay (BofA), Capital One Wallet, Target, Starbucks, Venmo, LevelUp, Square Cash**

Why So Many?

- **Stickiness**
- **Fewer swipes**
- **Loyalty and Rewards**
- **Contextual Data**
- **Marketing**

The End State

- **Still to be determined**

Brad Smith, AAP

Payment Industry Engagement

Capital One

Bradley.Smith2@capitalone.com