Blockchain & Money

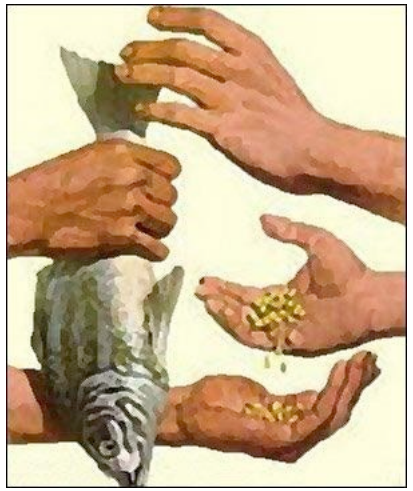
Class 24

December 11, 2018

Overview

- Money and Ledgers
- Satoshi Nakamoto’s Innovation
- Economics of Blockchain Technology
- Financial Sector Opportunities
- Crypto Finance
- Public Policy Frameworks
- Conclusions & Pay it Forward

What is the Role of Money?



Medium of Exchange

Store of Value

Unit of Account

Early Money

Image by Bertramz on Wikimedia. License: CC BY

Salt Bars - Ethiopia

Image by Sandstein on Wikimedia. License CC-BY

Tally Sticks - England

Image in the public domain by Gary Todd.

Cowrie Shells - Nigeria

Image by Yusuke Kawasaki on Wikimedia. License: CC BY

Rai Stones - Yap

Early Money

Cooper Plate - Sweden

Image by Scott Semans World Coins. License: CC BY

Bronze Yuan - China

Image is in the public domain.

Gold Aureus - Rome

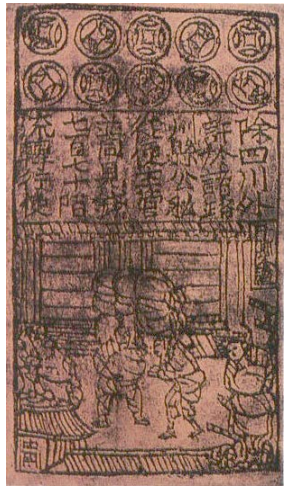


Image is in the public domain.

Jiaozi Promissory Note - China

Image is in the public domain.

5 Pound Note - England

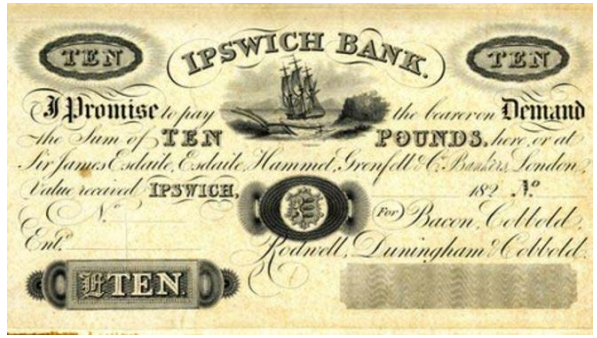
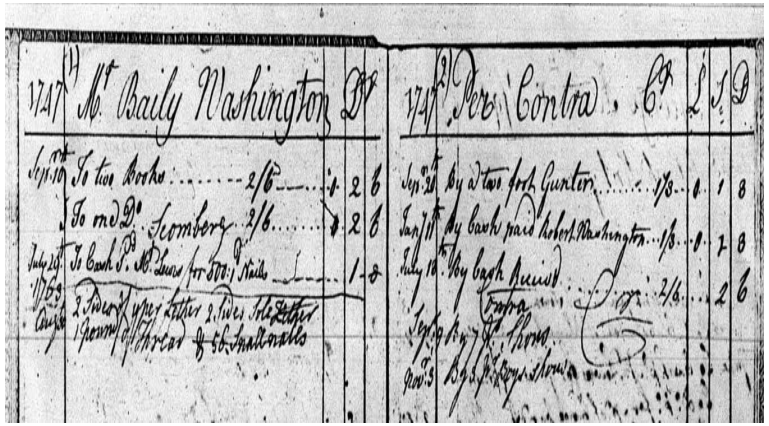


Image is in the public domain.

Private Bank Note – U.S.

Ledgers

Proto Cuneiform
Uruk, ca 3000 B.C



Personal Ledger
George Washington
1747

IBM 360
1961

Cunieform and Ledger are in the public domain.

Fiat Currency

Image by epSos.de on Wikimedia. License CC BY.

- Represented by:
  - Central Bank Notes
  - Central Bank Reserves &
  - Commercial Bank Deposits
- Relies upon System of Ledgers
- Accepted for Taxes
- Legal Tender for All Debts Public & Private
- Very Significant Network Effects from being Unit of Account

Satoshi Nakamoto: Bitcoin P2P e-cash paper October 31, 2008

“I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.”

Failure of Cryptographic Digital Currencies

Early Attempts

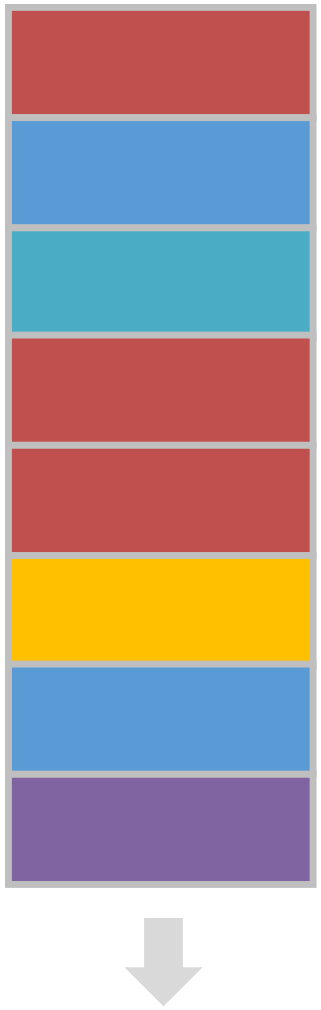
- DigiCash (1989), Mondex (1993), CyberCash (1994), E-gold (1996), Hashcash (1997), Bit Gold (1998), B-Money (1998), Lucre (1999)

Unsolved Challenges

- Centralization, Double spending, & Merchant adoption

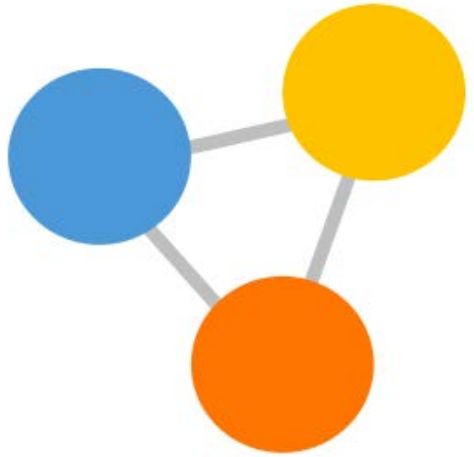
Blockchain Technology

timestamped
append-only log



auditable database

consensus protocol



Secured via cryptography

- Hash functions for **tamper resistance** and **integrity**
- Digital signatures for **consent**
- Consensus for **agreement**

Addresses '**cost of trust**' (Byzantine Generals problem)

- Permissioned
- Permissionless

Timestamped Append-only Log

‘How to Time-Stamp a Digital Document’ - Habor & Stornetta (1991)

Surety 1995 - present

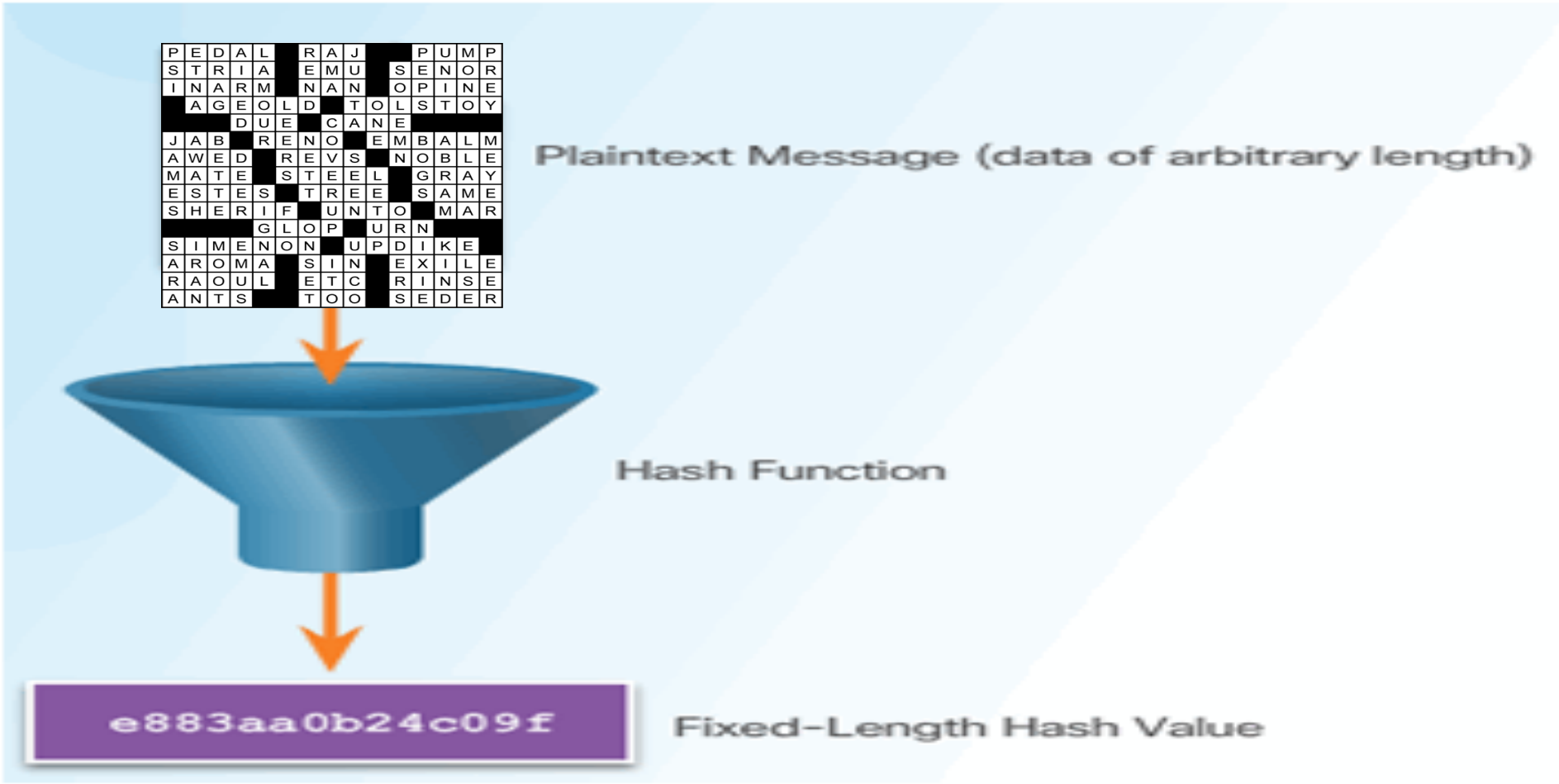
Courtesy of Ittai Abraham. Used with permission.

NOTICES & LOST AND FOUND
(5100-5102)

Universal Registry Entries:
Zone 2 -
dS8492cgVOFAoP9kvE1XzMOrQ
HgEwzkVbVafNvIkUz99qvq8/ME
p5v9EFSG8XxzMBaIGQQ==
Zone 3 -
JnFCg+HCmvhj8GmmUP7VZna71
NgZup/RfuKUQNzCHWXMuqLK
durxHQV5pSHLqBGPRIy+mg==
These base64-encoded values represent the combined fingerprints of all digital records notarized by Surety between 2009-06-03Z 2009-06-09Z.
www.surety.com 571-748-5800

Cryptographic Hash Functions

One-Way Data Compression

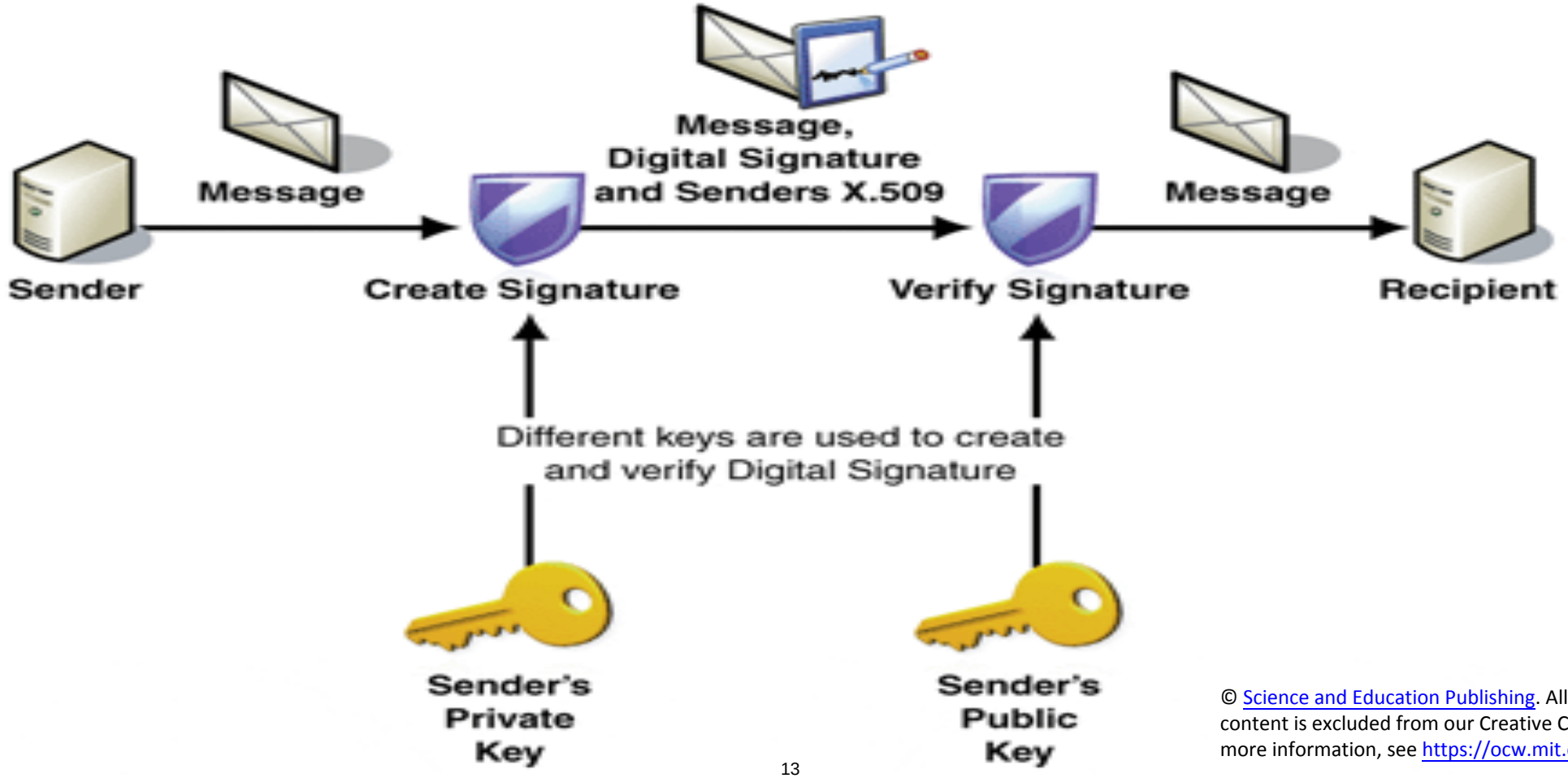


Data Commitment

Asymmetric Cryptography & Digital Signatures

Guarding against Tampering & Impersonation

Digital Signature without Hash

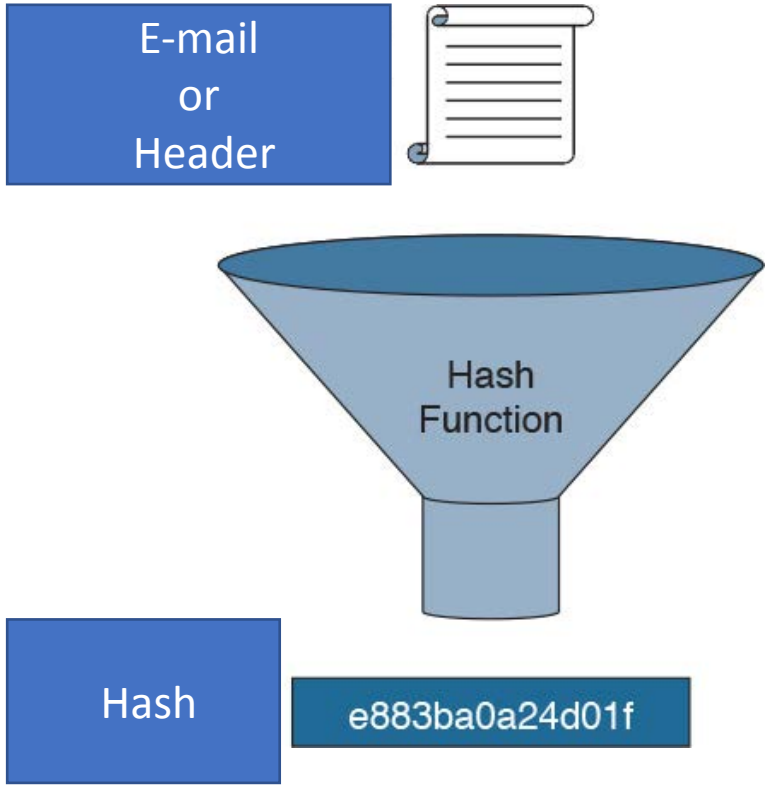


Shyam Nandan Kumar et al. Review on Network Security and Cryptography.

Proof of Work

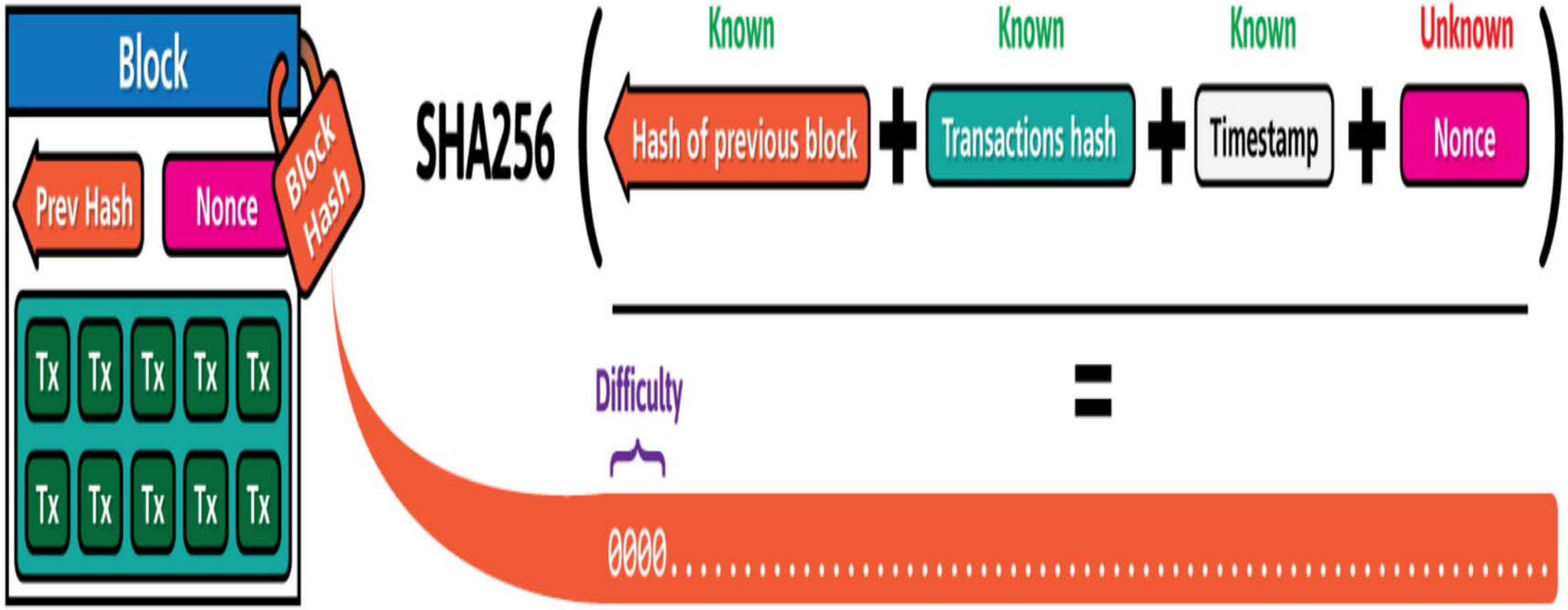
Proposed to address E-mail Spam and Denial of Service attacks (Adam Back, 1997)

- Requires computational work to find a Hash within predetermined range
- Difficulty defined by Hash outputs' # of leading zeros
- Can be Efficiently Verified

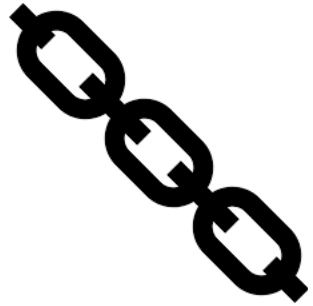


Blockchain – Proof of Work

Innovation – Chained Proof of Work for Distributed Network Consensus & Timestamping



Smart Contracts



- “A set of promises,
- specified in digital form,
- including protocols
- within which the parties perform on these promises.”

Nick Szabo, 1996

However ….

- Smart Contracts may not be ‘**Smart**’
- Smart Contracts may not be ‘**Contracts**’

Economics of Blockchain Technology

- Verification Costs:
  - Direct Costs
  - Privacy Costs
  - Censorship Risks
  - Settlement and Finality Risks
  - Costs of Trust
  - Economic Rents

- Networking Costs:
  - Token Incentive Systems - Reward, Affinity or Identity
  - Start-up Costs
  - Operating Costs

Assessing Use Cases

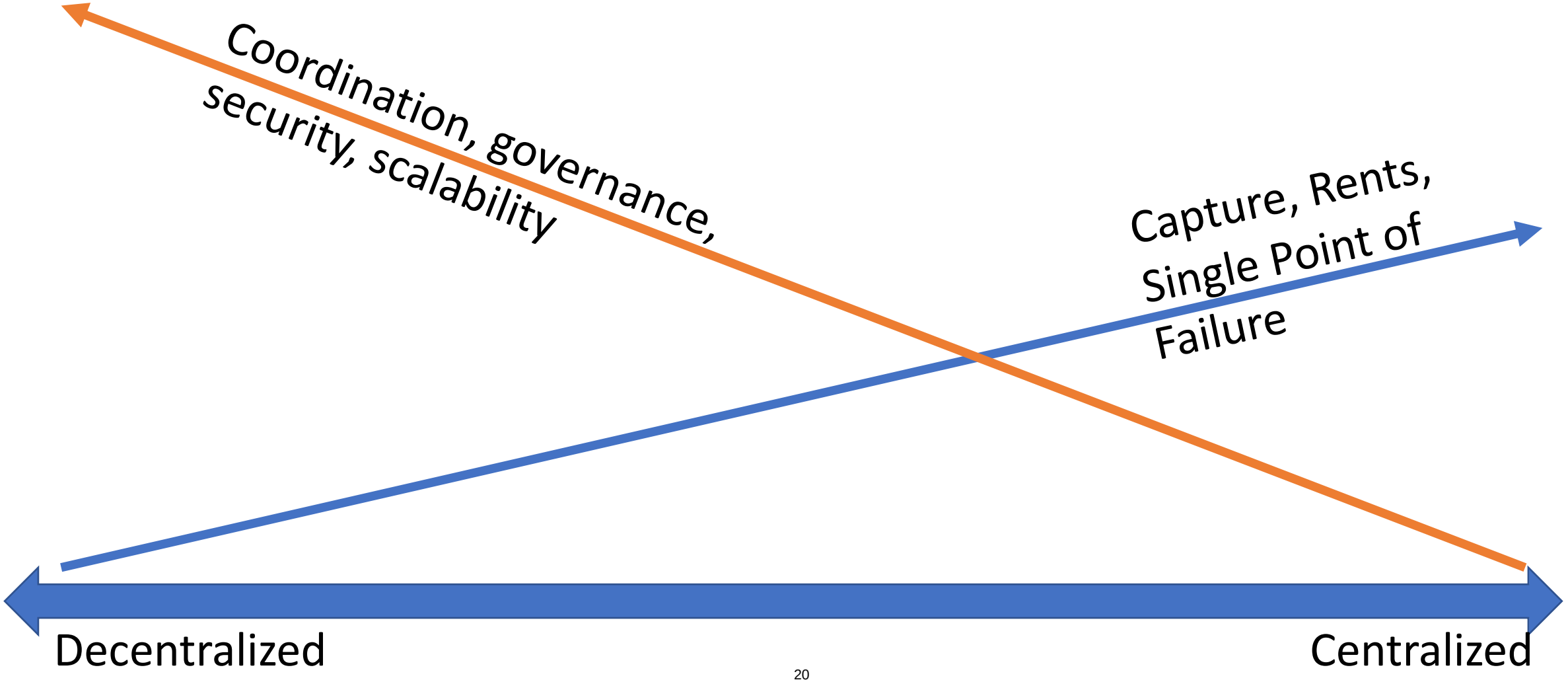
- What is the value creation proposition and ‘pain point’ being solved?
- Which costs of verification or networking can be reduced?
- What are competitors doing to address similar value propositions?

- Why are append only logs and multiple party consensus the best solution?
- Why not use a traditional data base?
- Which transactions and data need recording?
- Which multiple stakeholders need write and read access to ledgers?

Assessing Use Cases

- If a permissionless application, why is native token the best solution?
- What are Tradeoffs of Performance, privacy, security, & coordination?
- How can broad adoption be realized?
- What is the customer experience and user interface?

Framework for Comparing Costs & Trade-offs



Financial Sector

Moves, Allocates & Prices Money and Risk

- Relies upon Systems of Ledgers and Trust
- Has a Symbiotic Relationship with Technology

Financial Sector => Opportunities

- Legacy Customer Interface, Data, & Processing Systems
- Economic Rents
- Centralized Concentrated Risks
- Infrastructure Systems' Costs & Counterparty Risks
- Repeated Crises and Instability
- Financial Inclusion

- Financial sector costs: **7 ½ %** of U.S. GDP
- Payment system costs: **½ - 1 %** of Global GDP

Technologies of our Time Affecting Finance

Image by Tokumeigakarinoashima . CC0

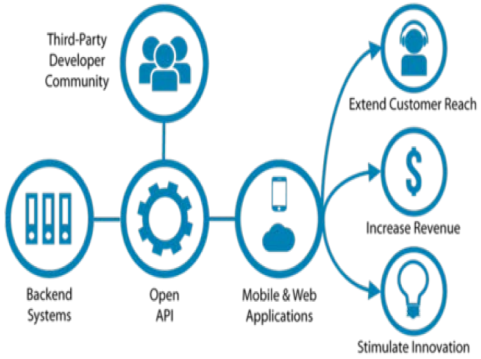
AI & ML

Image by Scott Robinson. CC BY.

Blockchain

Image by Jacob Gube. CC BY.

Cloud



Courtesy of RestCase. Used with permission.

Open API

Image by NEC Corporation of America. CC BY

Biometrics

Image by Mike Seyfang. CC BY.

Chatbots

Image by Hakan Dahlstrom. CC BY

Mobile

RPA

Financial Sector Issues with Blockchain Technology

- Performance, Scalability, & Efficiency
- Privacy & Security
- Interoperability
- Governance

Financial Sector Currently Favors

permissioned blockchains vs. permissionless blockchains

Access

Client Server	Permissioned	Permissionless
Traditional Databases	**Private Blockchain**	**Public Blockchain**
Trusted Party Hosts Data	Known Participants	Unknown Participants
Trusted Party can Create, Read, Update, & Delete (CRUD)	Private Write Capability	No Central Intermediaries
Client Server Architecture	Append Only Timestamped Log	Public Write Capability
	Publicly Verifiable	Peer to Peer Transactions
	No Native Currency	Token Economics

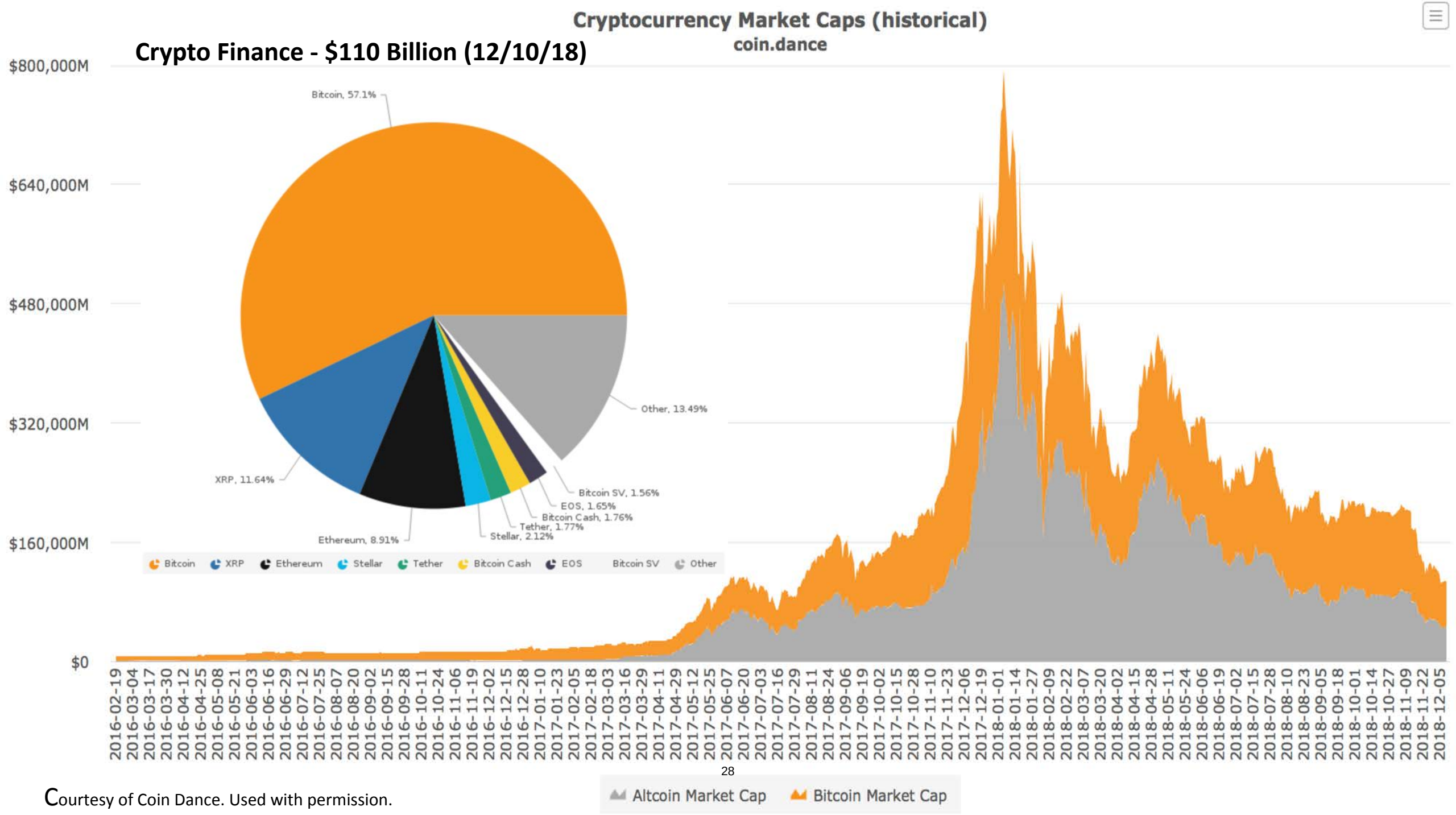
Financial Sector Potential Use Cases

- **Venture Capital -** Crowdfunding through Initial Coin Offerings
- **Payment Systems -** Cross border, Large interbank, & Retail
- **Loan Issuance & Trade Finance -** Digitizing paper-based processes
- **Clearing, Settlement and Processing –** Securities & Derivatives
- **Data Reporting**
- **Central Bank Digital Currency & Private Stable Value Tokens**

Non-Financial Potential Use Cases

- **Supply Chain Management**
- **Digital Identity**
- **Property and Asset Registries**
- **Device-to-device transactions in the ‘Internet of Things’**
- **Medical records**

Crypto Finance - $110 Billion (12/10/18)



Courtesy of Coin Dance. Used with permission.

Crypto Finance Investor Challenges

- Assessing Viability of Token Use Cases
- Markets Readily subject to Fraud, Scams, and Manipulation
- Custodial Arrangements of Private Keys
- Definitions – Securities, Commodities or Derivatives?
- Tax Compliance and Reporting

Crypto Exchanges

- Centralized - Matching Agents, Counterparties & Custodians
- Decentralized - Networks for Peer-to-peer Trading
- Responsible for over 95% of Crypto Secondary Market
- Greater than 30 Million direct Members
- Lack Intermediated Access or Meaningful Market Integrity Rules

Initial Coin Offerings

- Proceeds used to build networks
- Purchasers anticipate profits through appreciation
- Tokens issued prior to being functional
- Development, while open source, is largely centralized
- Promoters allocate themselves ‘premined’ tokens
- Tokens are fungible & transferable
- Scarcity is fostered with preset ‘Monetary policy’

Public Policy Framework

- Guarding Against Illicit Activity
- Financial Stability
- Protecting the Investing Public

U.S. Securities Law

Courtesy of Florida State Archives. Image is in the public domain.

- The Howey Test (1946):
  - Is it an investment of money or assets?
  - Is the investment in a common enterprise?
  - Is there a reasonable expectation of profits?
  - Is it reliant on the efforts of a promoter or others?

The Duck Test

"When I see a bird that walks like a duck and swims like a duck and quacks like a duck, I call that bird a duck."

James Whitcomb Riley, poet

Crypto Exchanges – Path Forward

- Custodial Duties - Fix or Spin-Off
- Illicit Activity – Comply with AML and Tax Laws
- Promote Market Integrity – Individually, SRO or Regulatorily
- Registration and Remediation – Determine and Comply

- Margin and Fee Compression
- Consolidation
- Decentralized Exchanges – Enhanced Customer UI & Adoption

ICOs – Path Forward

- Continued High Failure Rates
- Likely Further Decline in Funding Totals

- Increased Numbers of Enforcement Cases and Private Litigation
- Regulators & Courts Bring Added Clarity to ICO Security Definition
- More ICOs brought into Compliance

- Early Tokens will be Tested as Platforms may become Functional
- Markets Better Differentiate Viability of ICO Use Cases

Central Banks and Financial Stability

- Monitor and Study
- Restrict Use
- Payment System Experimentation
- Central Bank Digital Currency Initiatives

Conclusions – Blockchain & Money

- Blockchain Technology Provides Peer to Peer Alternative
- Addresses Verification and Networking Costs
- Use Cases Must Address why vs. Traditional Data Base?

- Money is but a Social & Economic Construct
- Financial Sector's Characteristics, Challenges and Scale Present Opportunities
- Incumbents Largely Looking at Private Permissioned Systems
- Crypto Finance Markets are Rive with Scams, Fraud and Manipulation

- Adoption rests on addressing Technical, Commercial and Policy Challenges
- The Potential, though, to be a Catalyst for Change is Real

Pay it Forward

I do not pretend to give such a deed; I only lend it to you.

When you [...] meet with another honest Man in similar Distress, you must pay me by lending this Sum to him; enjoining him to discharge the Debt by a like operation, when he shall be able, and shall meet with another opportunity.

I hope it may thus go thro' many hands, before it meets with a Knave that will stop its Progress.

This is a trick of mine for doing a deal of good with a little money.

- **Benjamin Franklin, 1784**

15.S12 Blockchain and Money
Fall 2018