Blockchain & Money

Class 5

September 20, 2018

Class 5 (9/20): Study Questions

- How does Bitcoin record transactions? What is unspent transaction output (UTXO)? What is script code embedded in each Bitcoin transaction and how flexible a programming language is it?

- As many design features pre-date Bitcoin, what was the novel innovation of Santoshi Nakamoto?

- Who is Satoshi Nakamoto? (Only kidding a bit.)

Class 5 (9/20): Readings

- *'Bitcoin's Academic Pedigree'* Narayanan and Clark

- *'Making Sense of Cryptoeconomics'* CoinDesk

Class 5 Overview

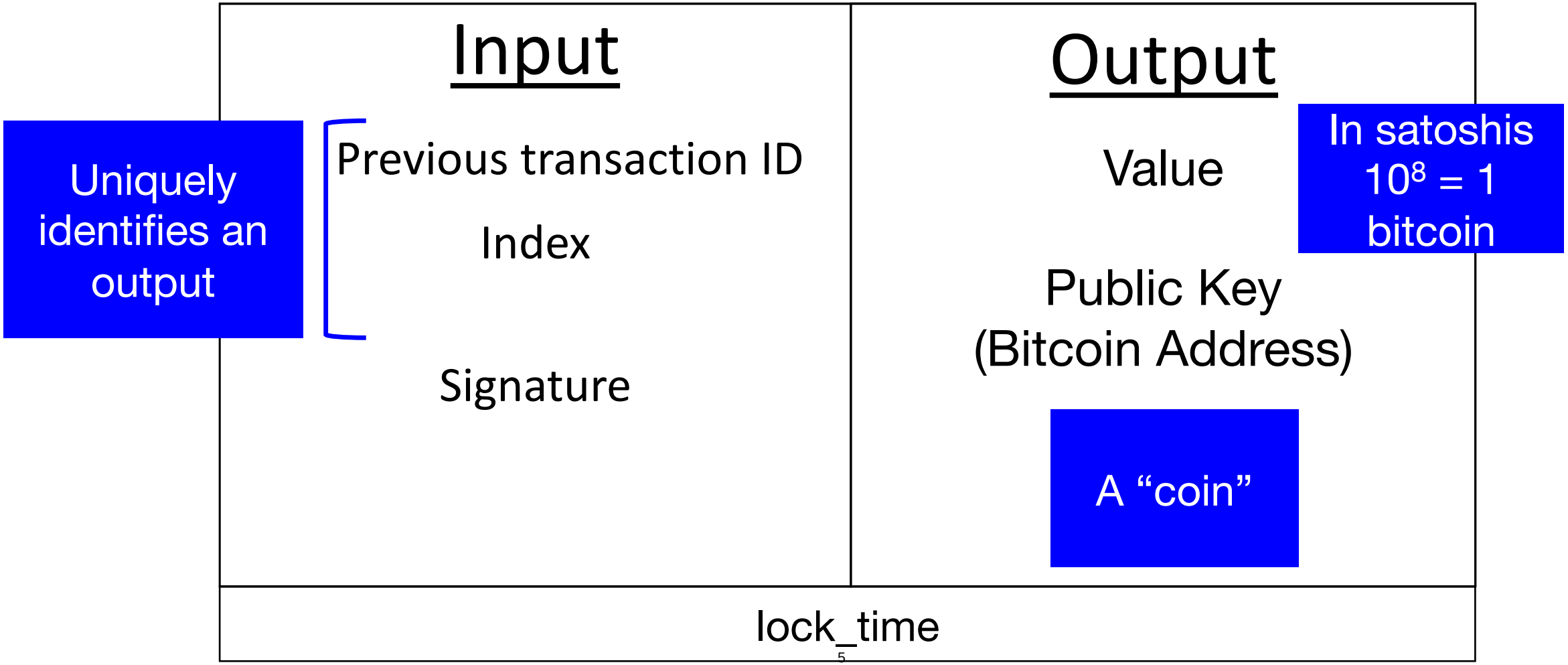
- Transaction Inputs & Outputs
- Unspent Transaction Output (UTXO)
- Scripting language

- Blockchain Design – Putting it All Together
- Bitcoin’s Academic Pedigree

- Who is Satoshi Nakamoto?

- Conclusions

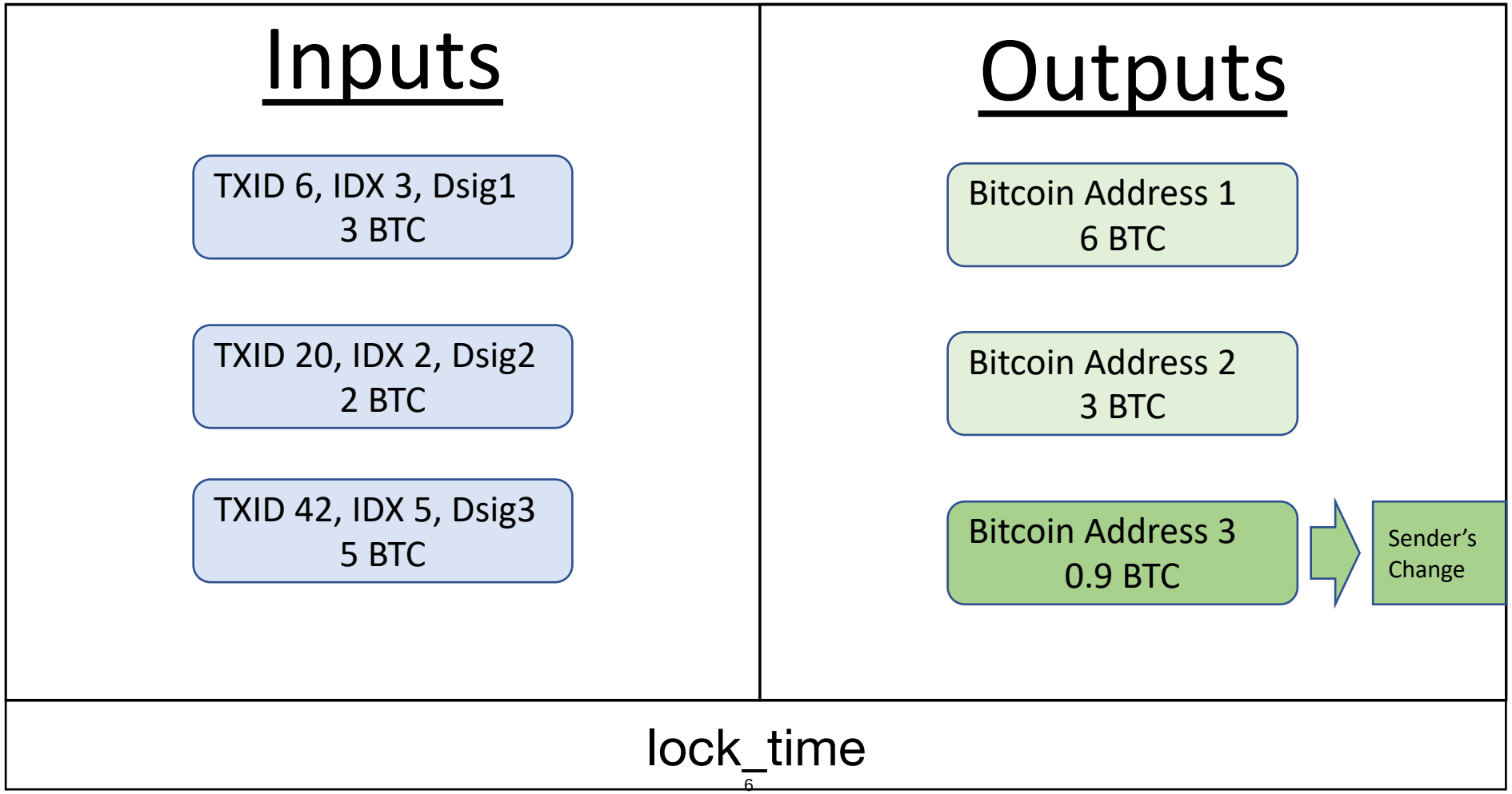
Transaction format



Transaction format

Multiple Inputs & Outputs

Inputs ≥ Outputs
Inputs – Outputs = Fees



Coinbase Transaction

Reward for Solving Proof of Work

- Only Input is the Coinbase Block Reward
- Reward halves (1/2s) every 210,000 blocks
  - Currently 12.5 Bitcoins per block
  - Originally 50 Bitcoin per block
- Output may not be used as a Transaction Input until another 100 Blocks
- Recorded as First Transaction in Merkle Tree
- May Include 100 bytes of arbitrary data
  - Used for Additional Nonce
  - Genesis Block included Headline from Financial Times:

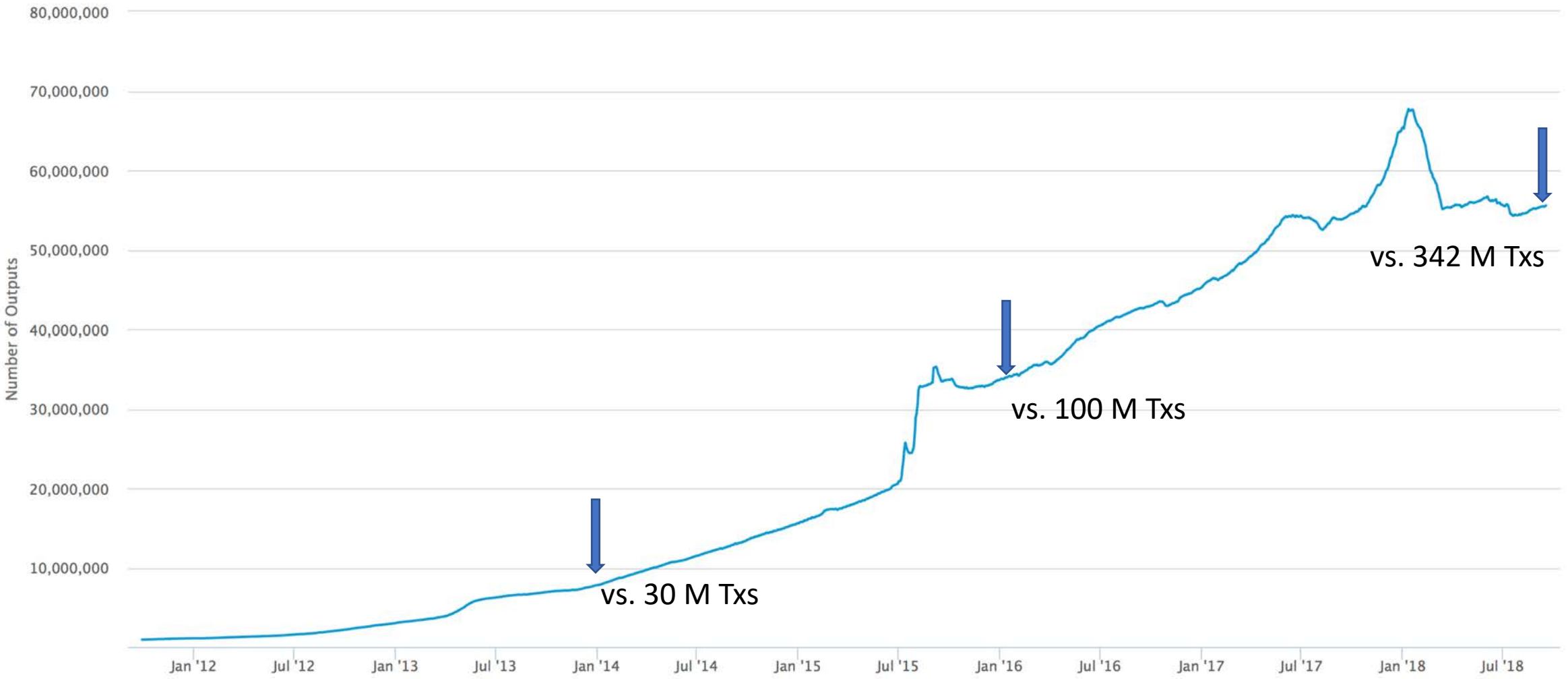
    ‘The Times 03/Jan/2009 Chancellor on brink of second bailout for banks’

Unspent Transaction Output (UTXO) Set

Bitcoin transaction outputs that have not been spent at a given time

- Contains All Currently Unspent Transaction Outputs
- Speeds up Transaction Validation Process
- Stored using a LevelDB database in Bitcoin Core called ‘chainstate’

Unspent Transaction Output (UTXO) Set



Source: Blockchain.com – 9/17/18

Bitcoin Script

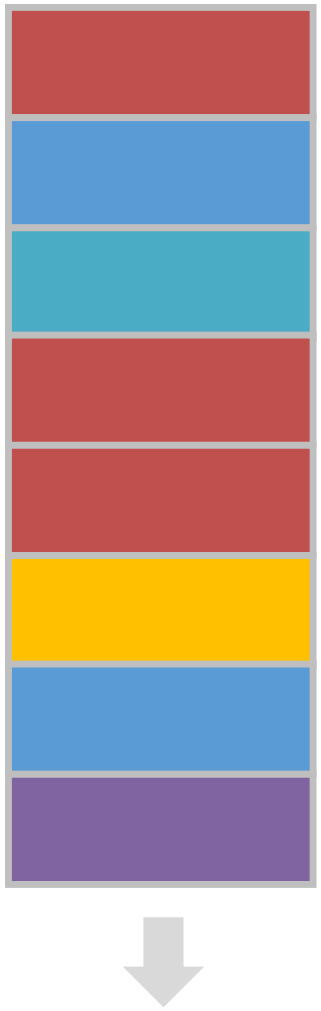
Programing Code used for Transactions

- Stack-based Code, with no Loops (not Turing-complete)
- Provides a Flexible Set of Instructions for Transaction Validation and Signature Authentication
- Most Common Script Types in UTXO:
  - Transaction sent to Hash of Bitcoin Address – ‘Pay-to-PubkeyHash’ (81%)
  - Transaction sent to Hash of Conditional Script – ‘Pay-to-ScriptHash’ (18%)
  - Transaction subject to Multiple Signatures – ‘M of N Multisig’ (0.7%)
  - Transaction sent to Bitcoin Address – ‘Pay-to-Pubkey’ (0.1%)

    (Source: Perez-Sola, Delgado-Segura, et al.)

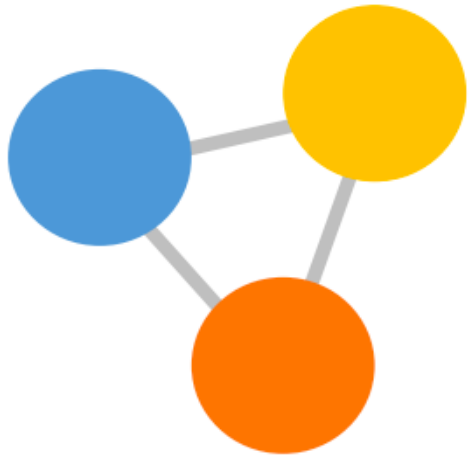
Blockchain Technology

timestamped
append-only log



auditable database

network 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)

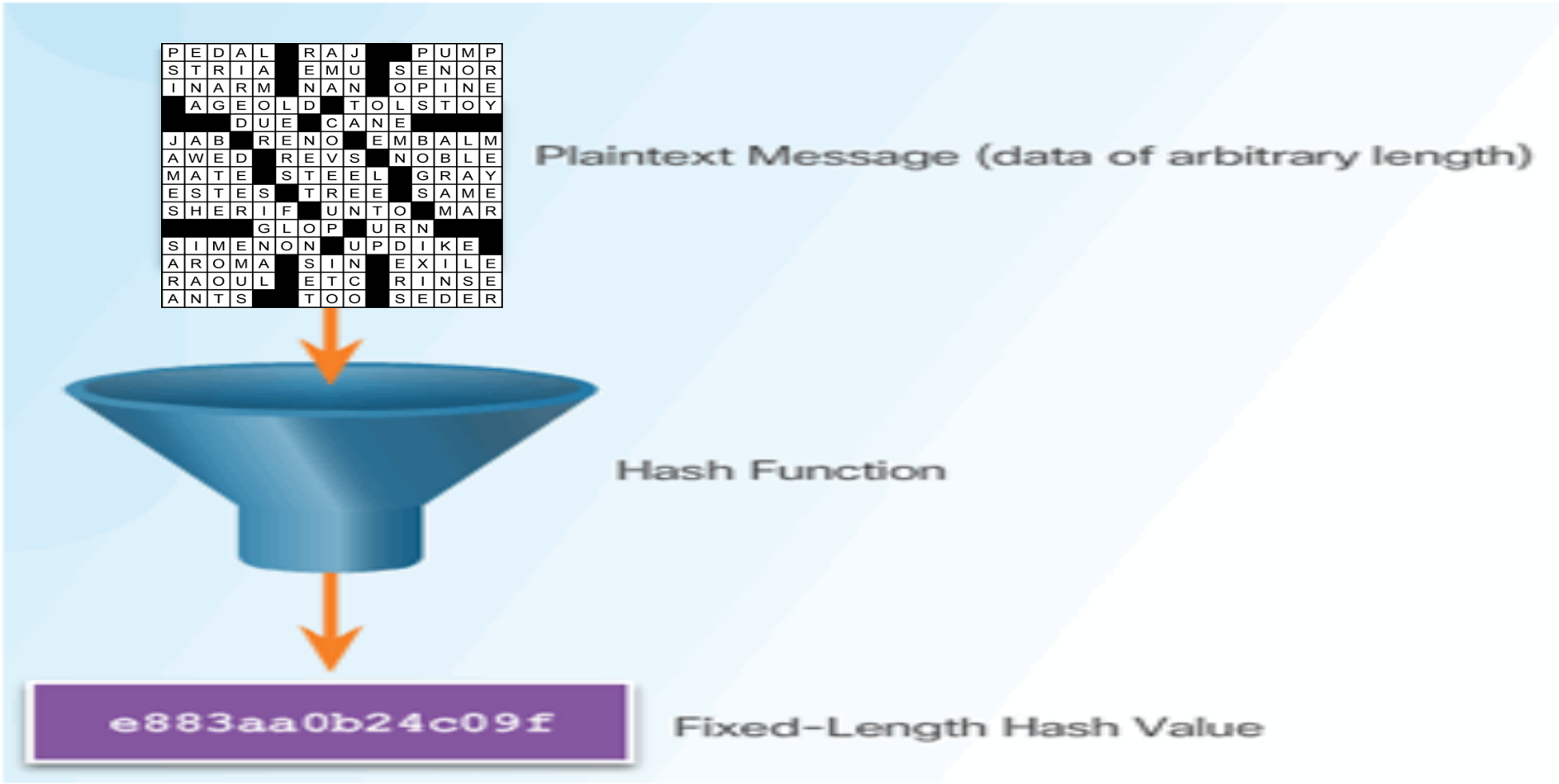
- Permissioned
- Permissionless

Bitcoin – Technical Features

- Cryptography & Timestamped Logs
  - Cryptographic Hash Functions
  - Timestamped Append-only Logs (Blocks)
  - Block Headers & Merkle Trees
  - Asymmetric Cryptography & Digital Signatures
  - Addresses
- Decentralized Network Consensus
  - Proof of Work
  - Native Currency
  - Network
- Transaction Script & UTXO
  - Transaction Inputs & Outputs
  - Unspent Transaction Output (UTXO) set
  - Scripting language

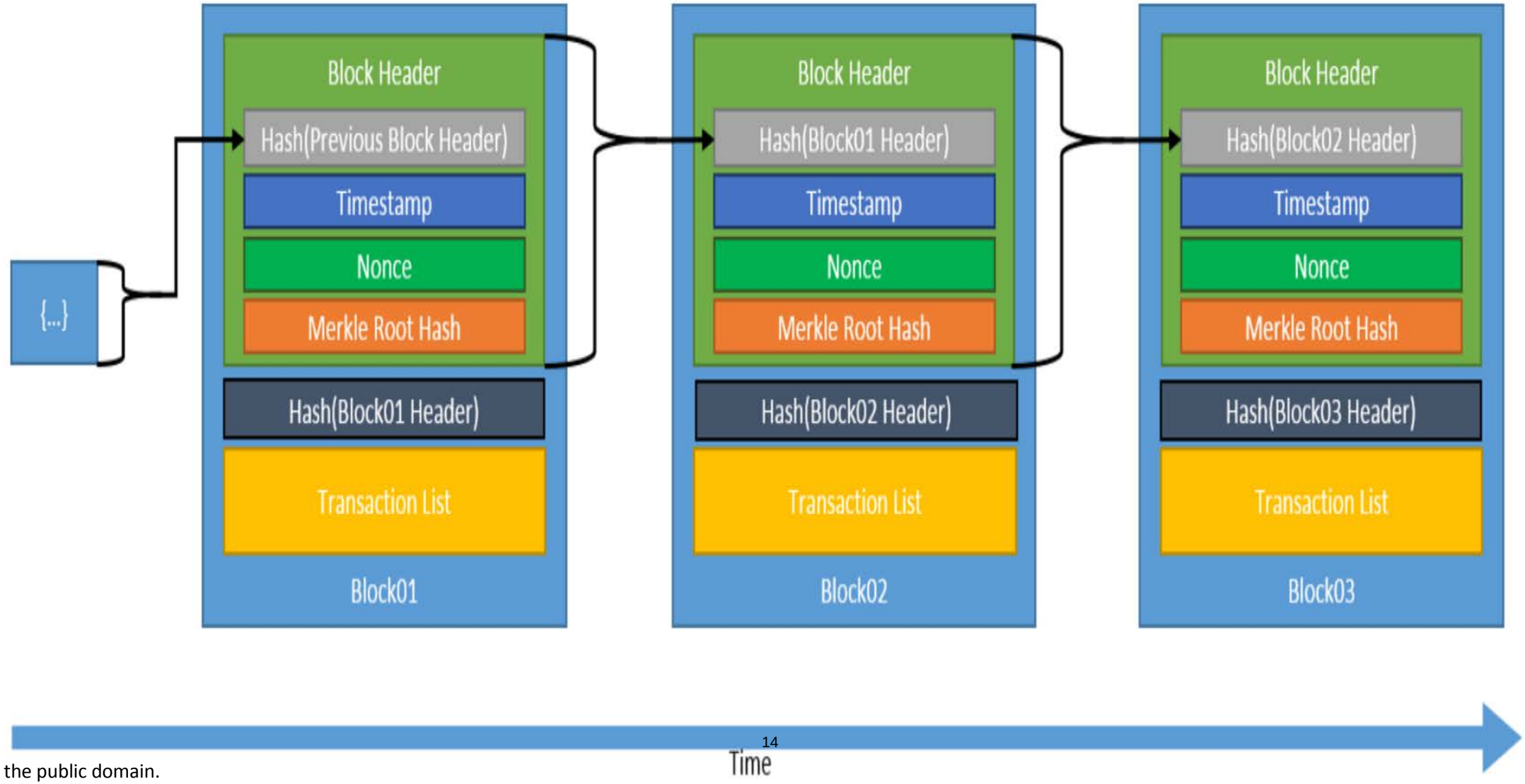
Cryptographic Hash Functions

One-Way Data Compression

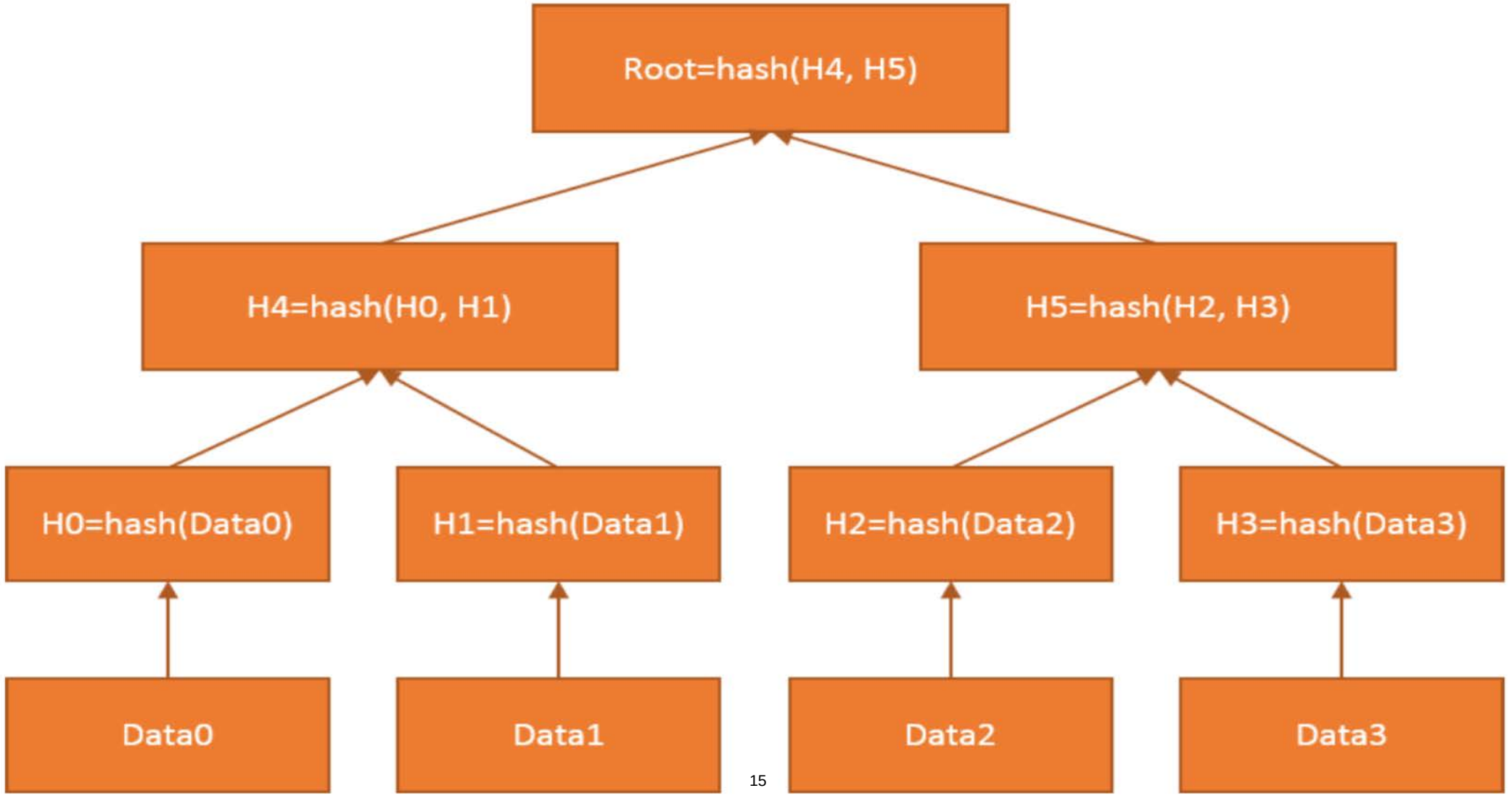


Data Commitment

Timestamped Append-only Log - Blockchain



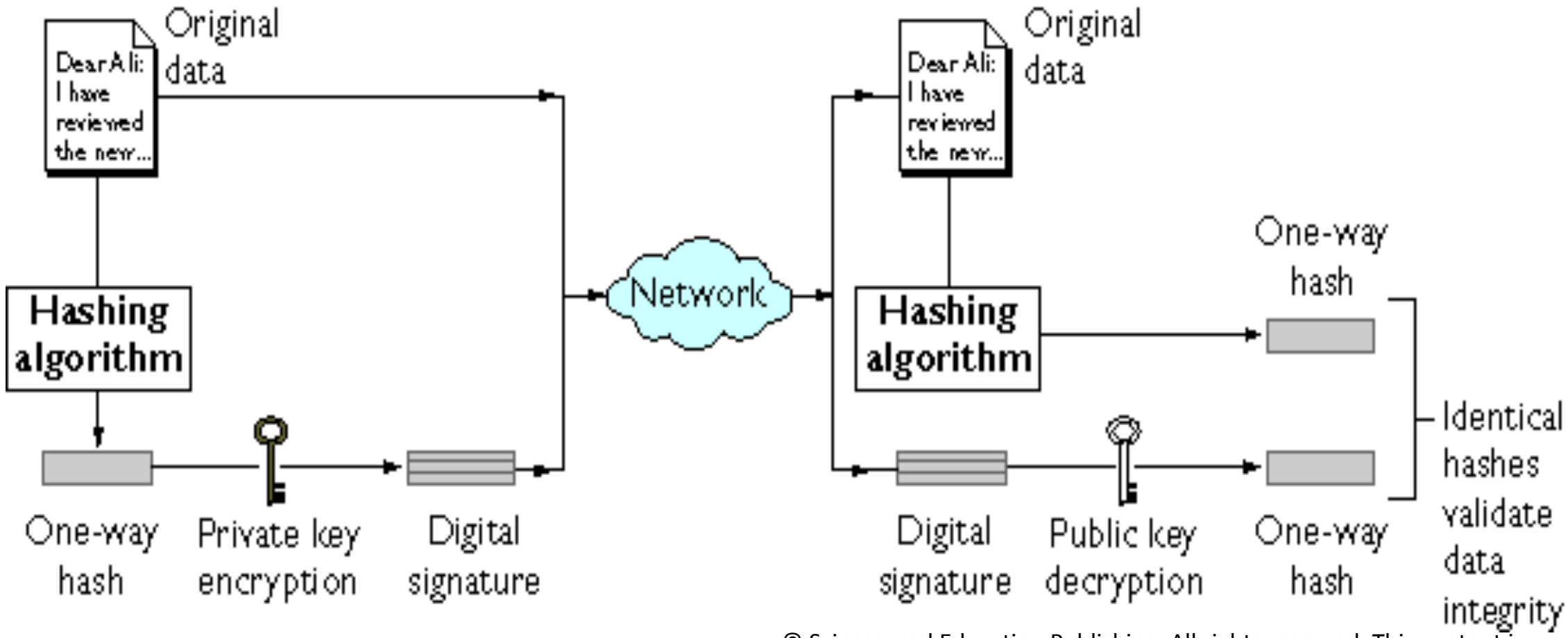
Merkle Tree – Binary Data Tree with Hashes



Asymmetric Cryptography & Digital Signatures

Guarding against Tampering & Impersonation

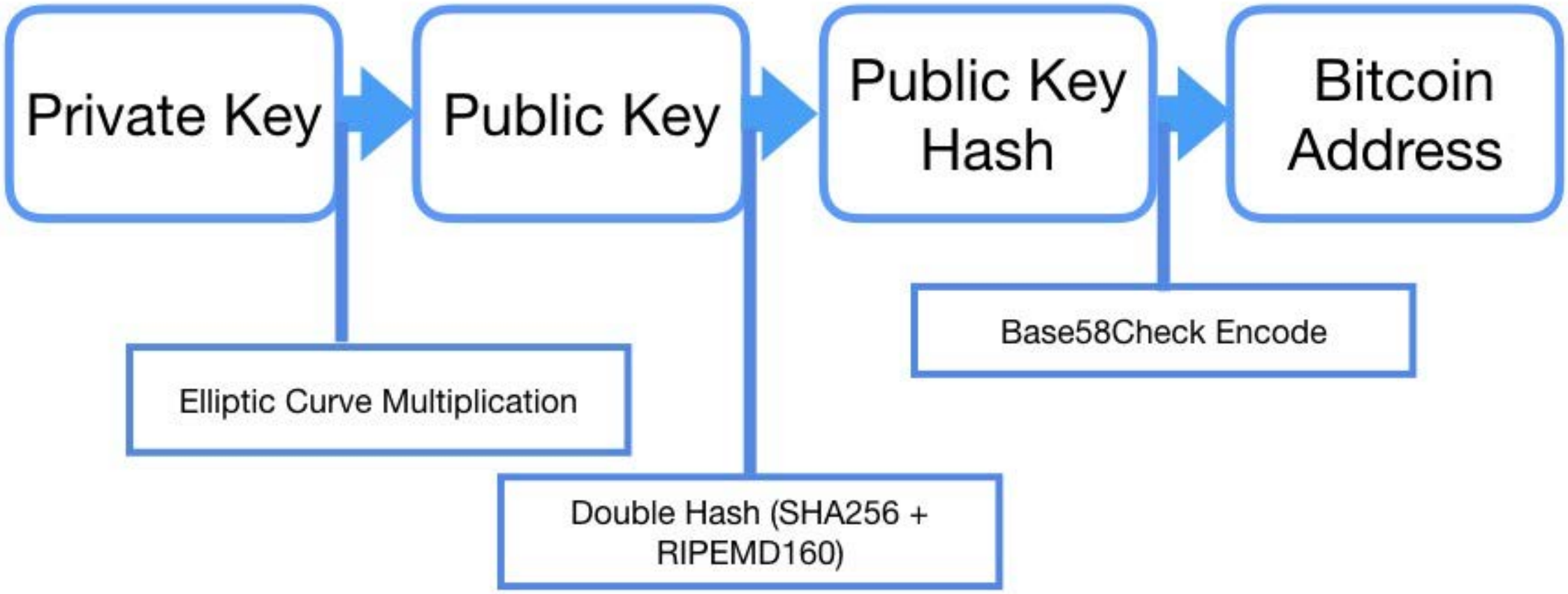
Digital Signature with Hash



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

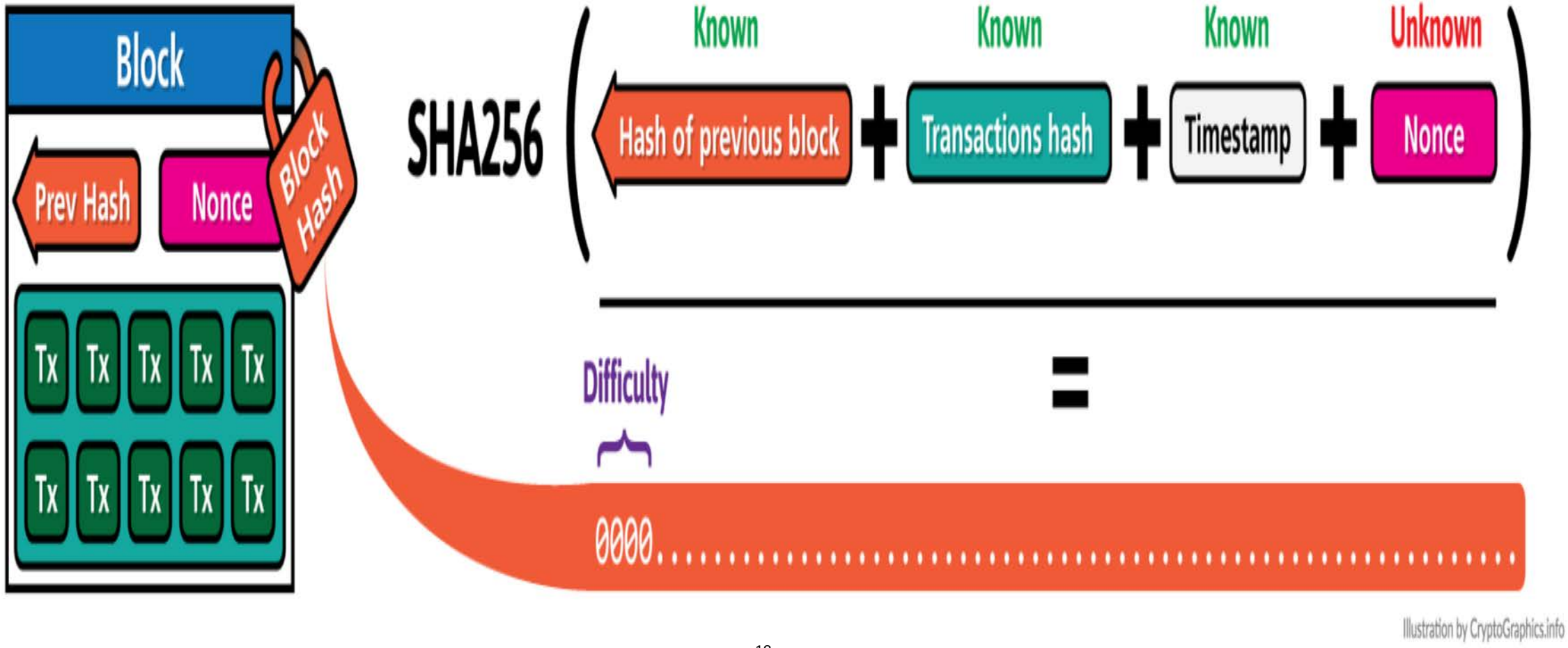
Bitcoin Address

Determined by – but not identical to - Public Key



Blockchain – Proof of Work

Chained Proof of Work for Distributed Network Consensus & Timestamping



Native Currency

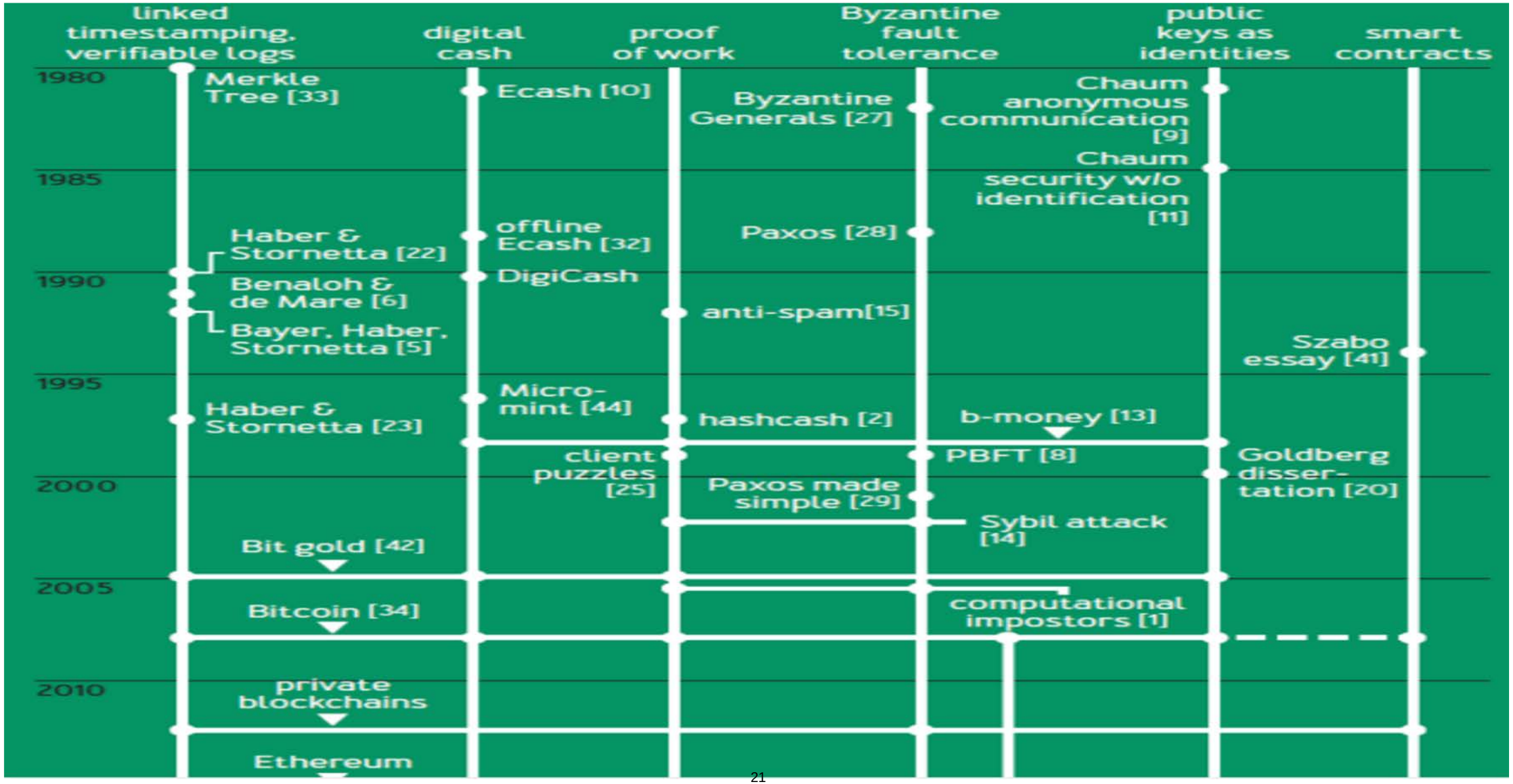
Economic Incentive System

- Bitcoin – BTC
  - Reward Created through Coinbase Transaction in each block
  - Overall ‘Monetary Policy’ preset in Bitcoin Core
  - Reward halves (1/2s) every 210,000 blocks
  - Currently 17.3 million BTC; capping at 21 million BTC in 2140
  - Market based transaction fee mechanism also provided for in software

Network

- Full Nodes – Store full Blockchain & able to Validate all Transactions
- Pruning Nodes – Prune transactions after validation and aging
- Lightweight Nodes - Simplified Payment Verification (SPV) nodes – Store Blockchain Headers only
- Miners – Performs Proof of Work & Create new Blocks - Do not need to be a Full Node
- Mining Pool Operators
- Wallets – Store, View, Send and Receive Transactions & Create Key Pairs
- Mempool – Pool of unconfirmed (yet validated) Transactions

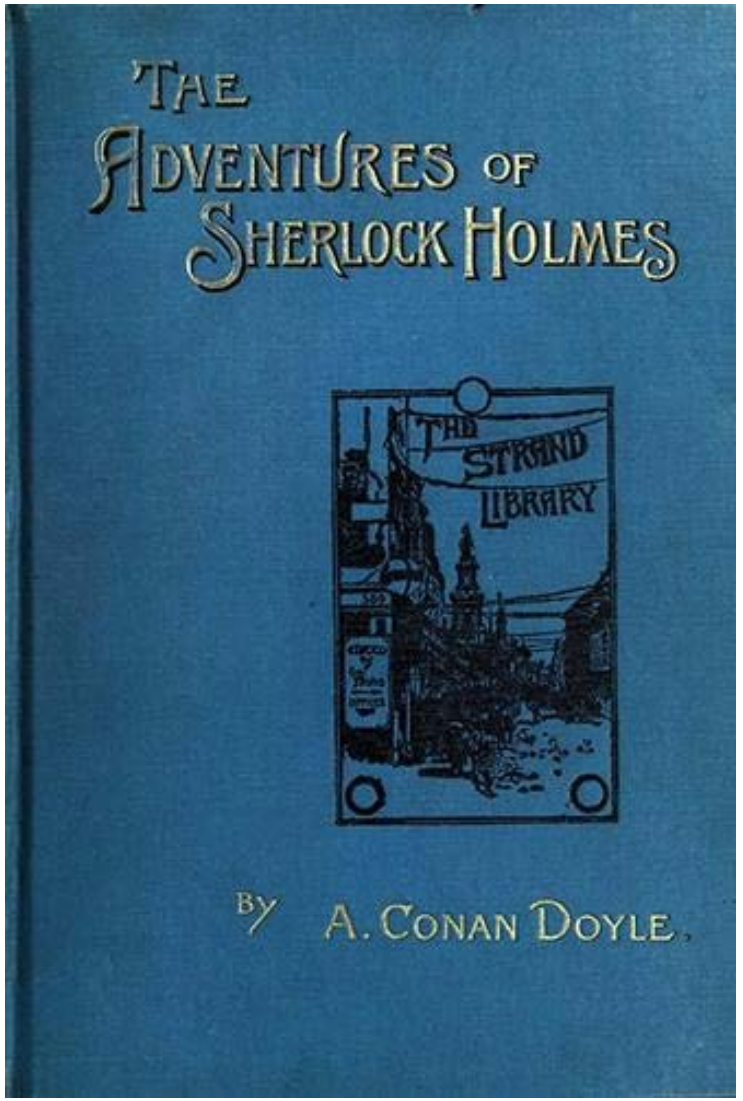
Narayanan and Clark's Chronology of Ideas in Bitcoin



Who is Satoshi Nakamoto?

Results of Ad Hoc Survey of Students

Group Led by Hal Finney
Nick Szabo
Craig Wright
Dorian Nakamoto
State Actor - US Government (NSA) or Otherwise



Class 6 (9/25): Study Questions

- What are smart contracts? How do they compare to traditional contracts? What are tokens?

- What are smart contract platforms such as Ethereum? What generally distinguishes them from Bitcoin?

- What are decentralized applications (DApps)? What has been the usage and why haven’t any DApps yet received wide consumer adoption?

Class 6 (9/25): Readings

Required

- *'Smart Contracts: 12 Use Cases for Business & Beyond'* Chamber of Digital Commerce
- *'State of the Dapps: 5 Observations from Usage Data'* McCann
- *'Ethereum Competitors: Guide to the Alternative Smart Contract Platforms'* Blockonomi

Optional

- *'Smart Contracts: Building Blocks for Digital Markets'* Szabo
- *'A Next-Generation Smart Contract and Decentralized Application Platform'* Ethereum
- *'Blockchain Technology as a Regulatory Technology'* De Filippi & Hassan

Guest Lecturer – Larry Lessig

- **Harvard Professor of Law and Leadership.**
- **Founder of Stanford Law's Center for Internet and Society.**
- **Clerked for Justice Antonin Scalia and for Appeals Court Judge Richard Posner.**
- **Awards include the Free Software Foundation's Freedom Award, Fastcase 50 Award and being named one of Scientific American's Top 50 Visionaries.**

'Code and Other Laws of Cyberspace'

- **Code/architecture** – physical or technical constraints
- **Market** – economic forces
- **Law** – explicit mandates by government
- **Norms** – social conventions

Conclusions

- Nakamoto's Bitcoin brought us Blockchain Technology
- Blockchain technology is within long history of Money & Ledgers
- Its Design Features also can be placed within history of technology
  - Timestamped Append-only Logs (Blocks)
  - Cryptographic Hash Functions & Digital Signatures
  - Network Consensus
- Key Innovation – Decentralized Chained Consensus Protocol
  - Addresses 'Costs of Trust'
  - Provides Peer-to-Peer alternative for Money, Ledgers & Computation

15.S12 Blockchain and Money
Fall 2018