Blockchain & Money

Class 4

September 18, 2018

Class 4 (9/18): Study Questions

- What is the Byzantine Generals problem? How does proof-of-work and mining in Bitcoin address it? More generally how does blockchain technology address it?

- What other consensus protocols are there? What are some of the tradeoffs of alternative consensus algorithms – proof-of-work, proof-of-stake, etc.?

- How do economic incentives work within blockchain technology to maintain decentralized ledgers and avoid double spending? What are the incentives of consensus protocols and mining? (Moved from 9/20)

Class 4 (9/18): Readings

- *‘Geneva Report*’ Chapter 1 (pages 1 – 7); Casey, Crane, Gensler, Johnson, and Narula
- *‘Blockchain Technology Review’* NIST (pages 23 - 32, sections 3 & 4)
- *‘The Byzantine Generals Problem’* Lamport, Shostak, & Pease (382-387)
- *‘A Short Guide to Consensus Protocols’* CoinDesk

Class 4 Overview

- Review of Blockchain Design

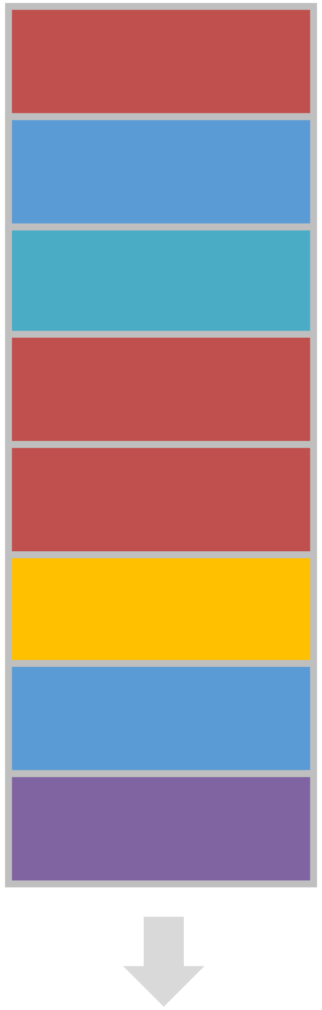
- Consensus through Proof of Work
- Bitcoin Mining
- Native Currency
- Network

- Other Consensus Protocols

- Conclusions

Review - Blockchain Technology

timestamped
append-only log



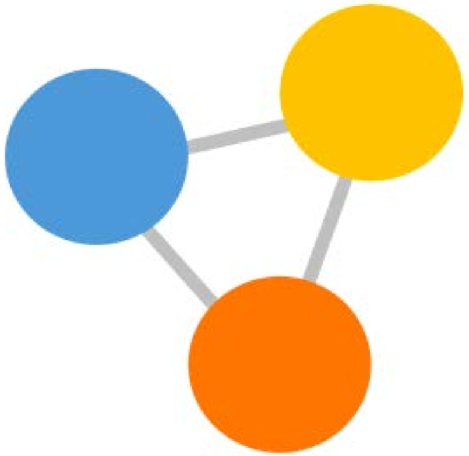
auditable database

Secured via cryptography

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

Consensus for **agreement**

network consensus protocol



Addresses ‘**cost of trust**’ (Byzantine Generals problem)

- Permissioned
- Permissionless

Bitcoin – Technical Features

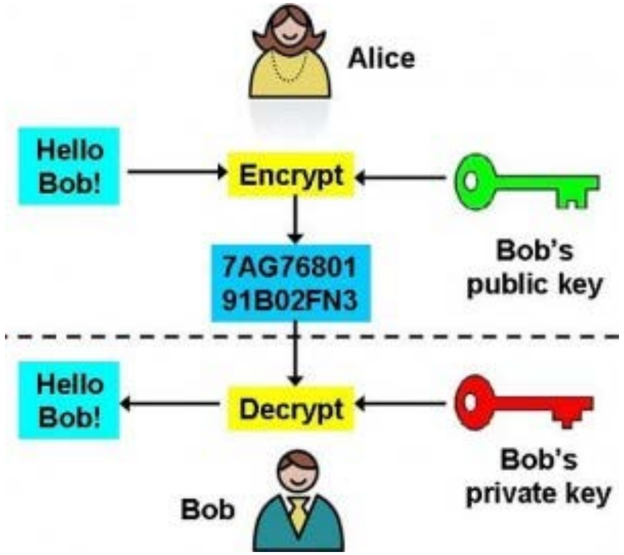
- Cryptography & Timestamped Logs
  - Cryptographic Hash Functions
  - Timestamped Append-only Logs (Blocks)
  - Block Headers & Merkle Trees
  - Asymmetric Cryptography & Digital Signatures
  - Addresses
- Decentralized Network Consensus
  - Proof of Work
  - Native Currency
  - Network
- Transaction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

Cryptography:

Communications in the presence of adversaries

Scytale Cipher
Ancient Times

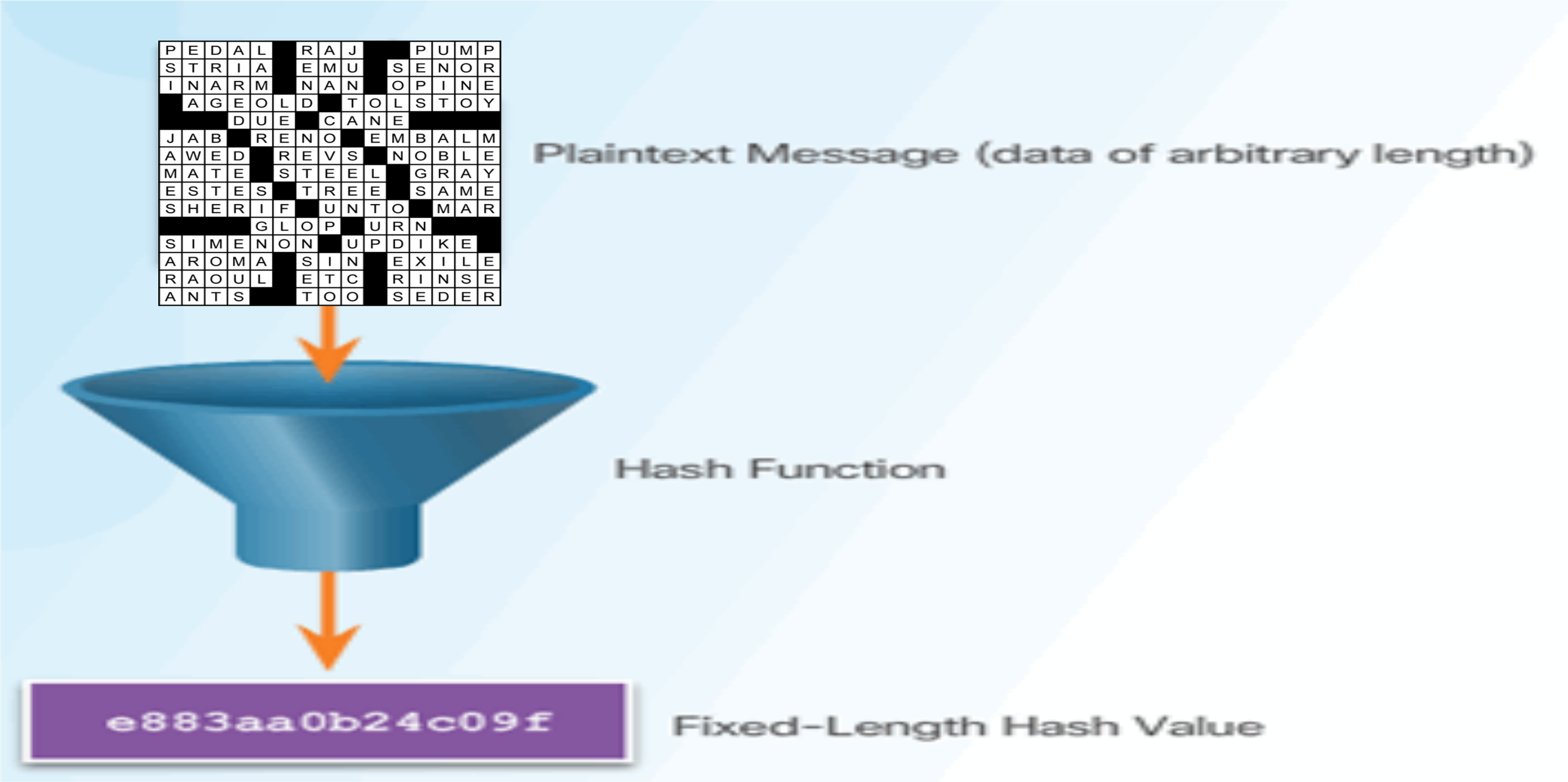
Enigma Machine
1920s - WWII



Asymmetric Cryptography
1976 to today

Cryptographic Hash Functions

One-Way Data Compression



P	E	D	A	L		R	A	J			P	U	M	P
S	T	R	I	A		E	M	U		S	E	N	O	R
I	N	A	R	M		N	A	N		O	P	I	N	E
	A	G	E	O	L	D		T	O	L	S	T	O	Y
			D	U	E		C	A	N	E				
J	A	B		R	E	N	O		E	M	B	A	L	M
A	W	E	D		R	E	V	S		N	O	B	L	E
M	A	T	E		S	T	E	E	L		G	R	A	Y
E	S	T	E	S		T	R	E	E		S	A	M	E
S	H	E	R	I	F		U	N	T	O		M	A	R
				G	L	O	P		U	R	N			
S	I	M	E	N	O	N		U	P	D	I	K	E	
A	R	O	M	A		S	I	N		E	X	I	L	E
R	A	O	U	L		E	T	C		R	I	N	S	E
A	N	T	S			T	O	O		S	E	D	E	R

Data Commitment

Timestamped Append-only Log - Blockchain

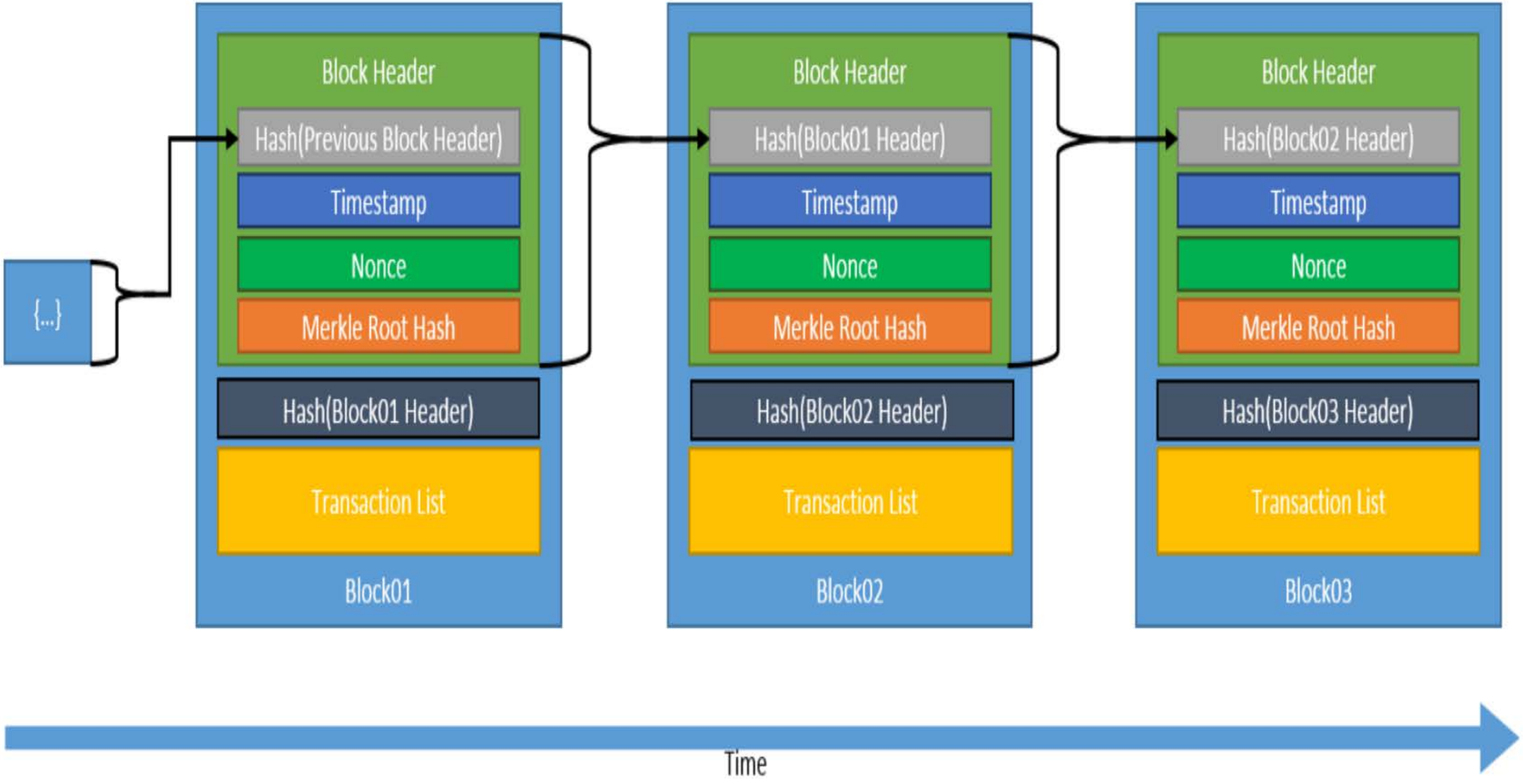


Image is in the public domain.

Merkle Tree – Binary Data Tree with Hashes

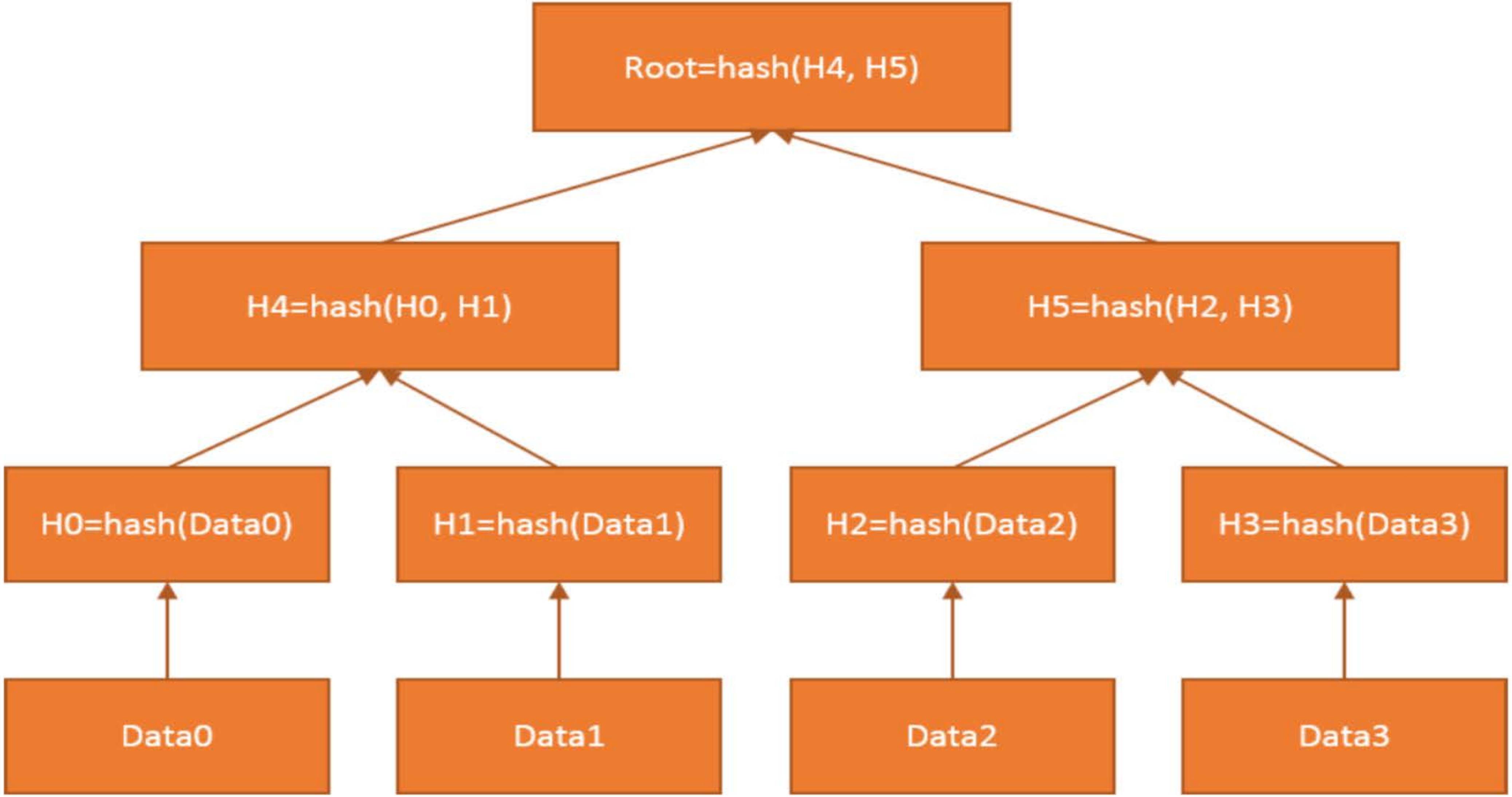
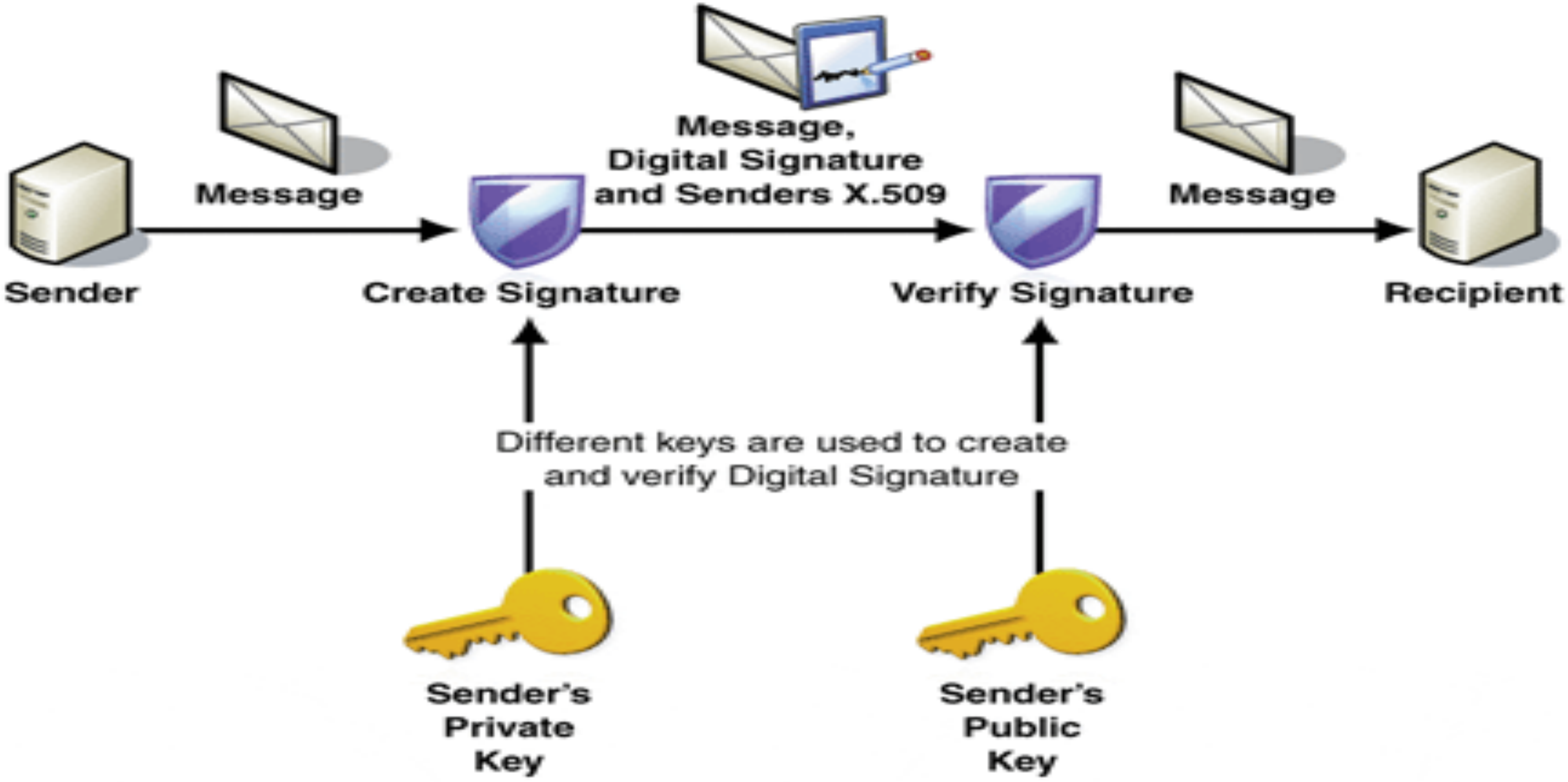


Image is in the public domain.

Asymmetric Cryptography & Digital Signatures

Guarding against Tampering & Impersonation

Digital Signature without Hash

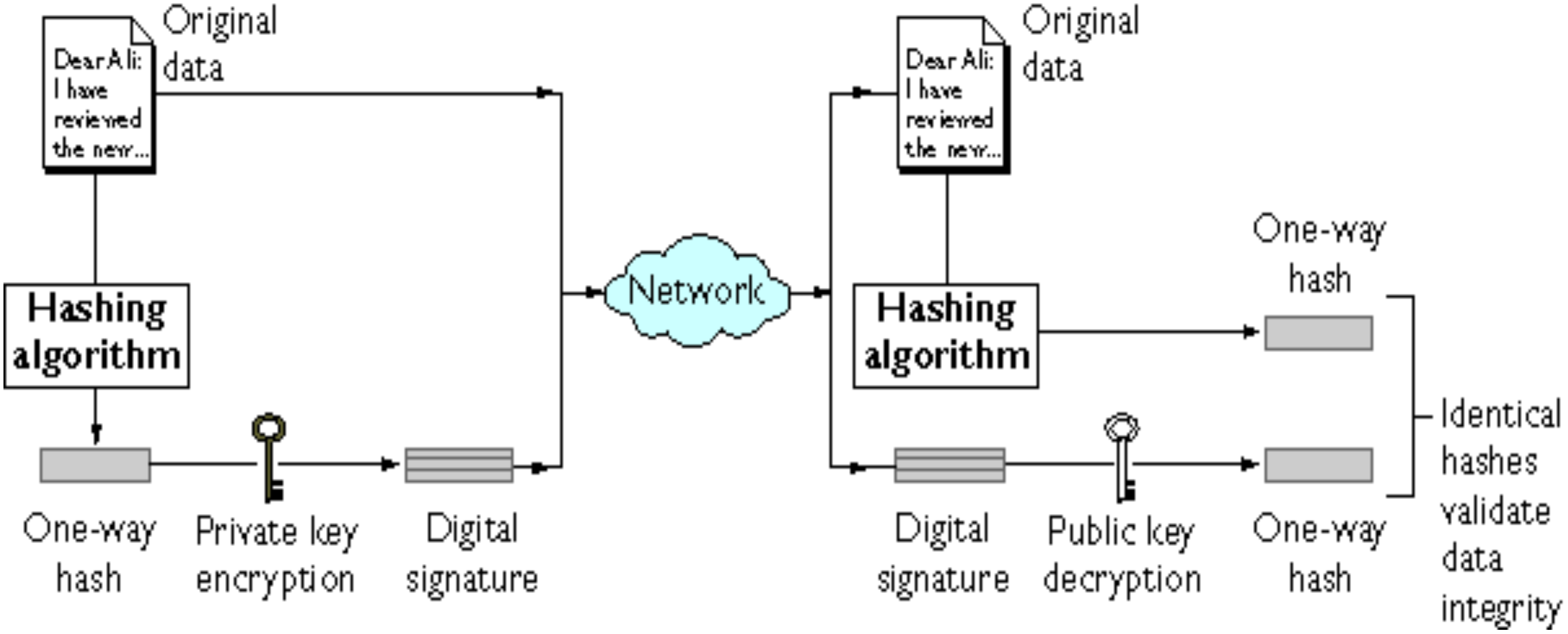


Shyam Nandan Kumar et al. Review on Network Security and Cryptography.

Asymmetric Cryptography & Digital Signatures

Guarding against Tampering & Impersonation

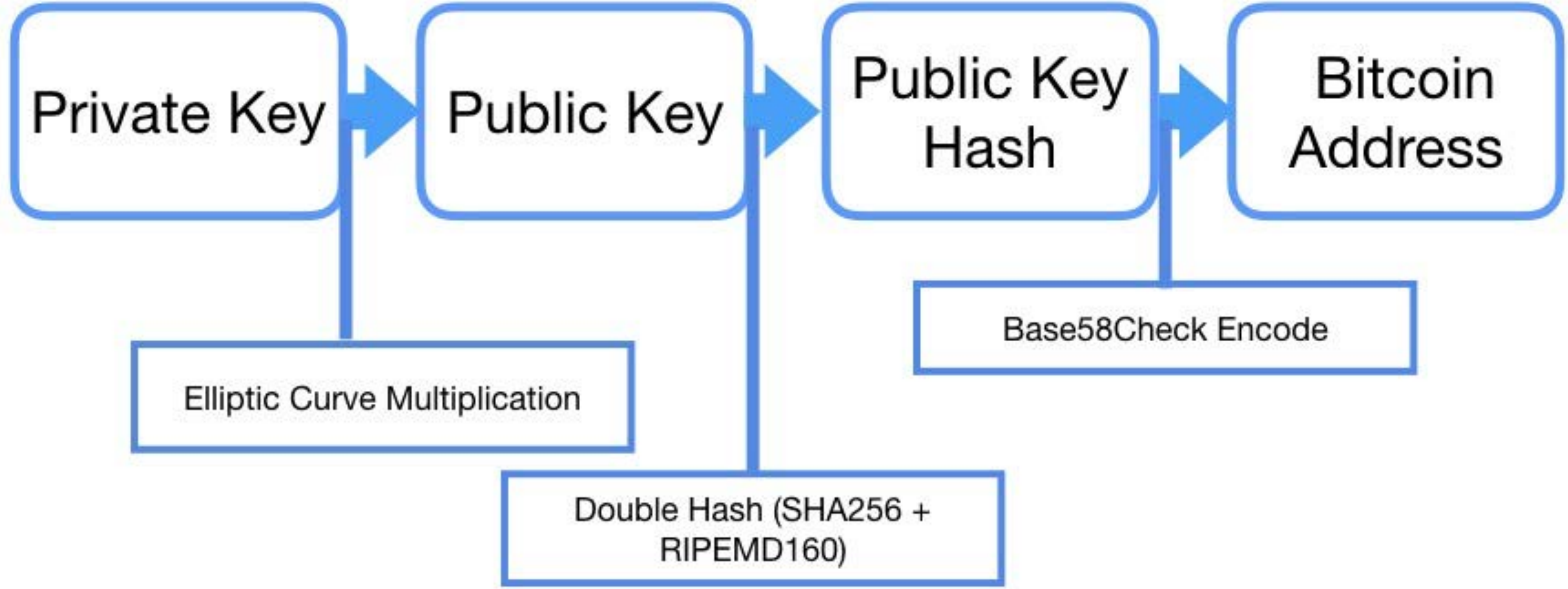
<u>Digital Signature with Hash</u>



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

Bitcoin Address

Determined by – but not identical to - Public Key

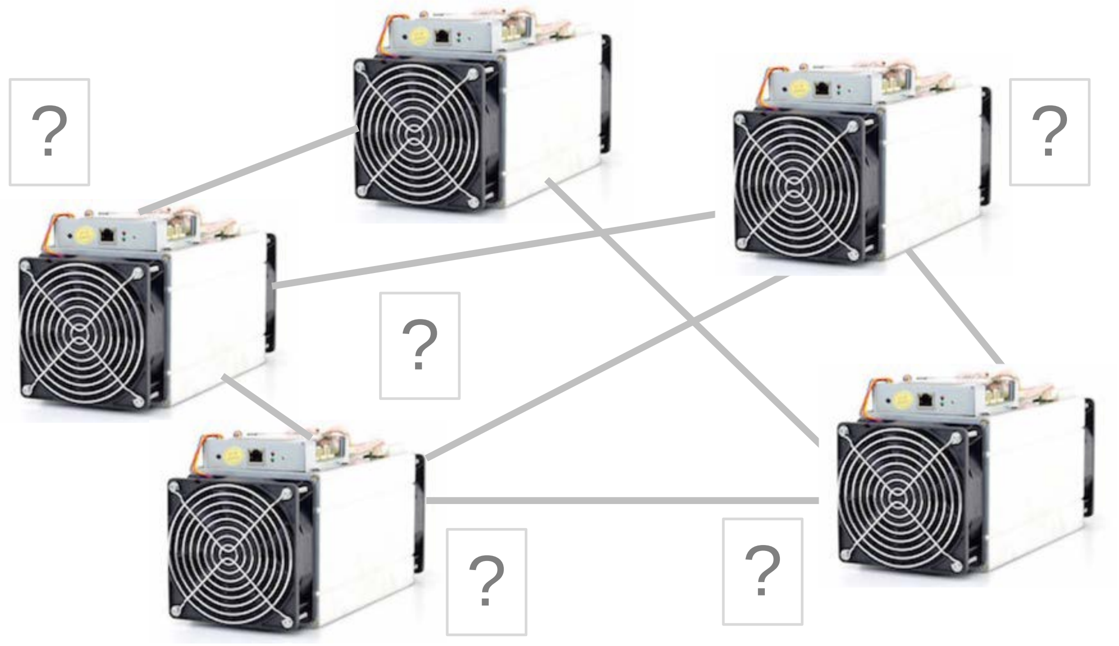


Decentralized Networks

Byzantine Generals Problem

Attack!
Attack!
Retreat
Retreat
Attack!

Permissionless Blockchains - **Unknown** participants



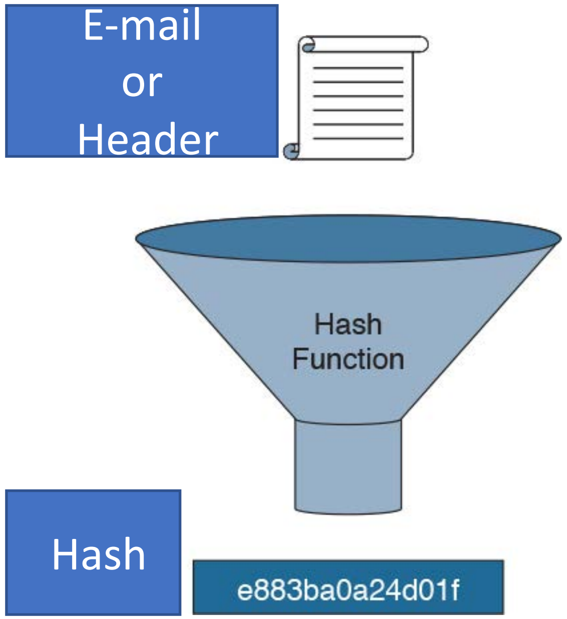
Security based on:

- Consensus protocol &
- Native currency

Hashcash – Proof of Work (Adam Back, 1997)

Proposed to address E-mail Spam and Denial of Service attacks

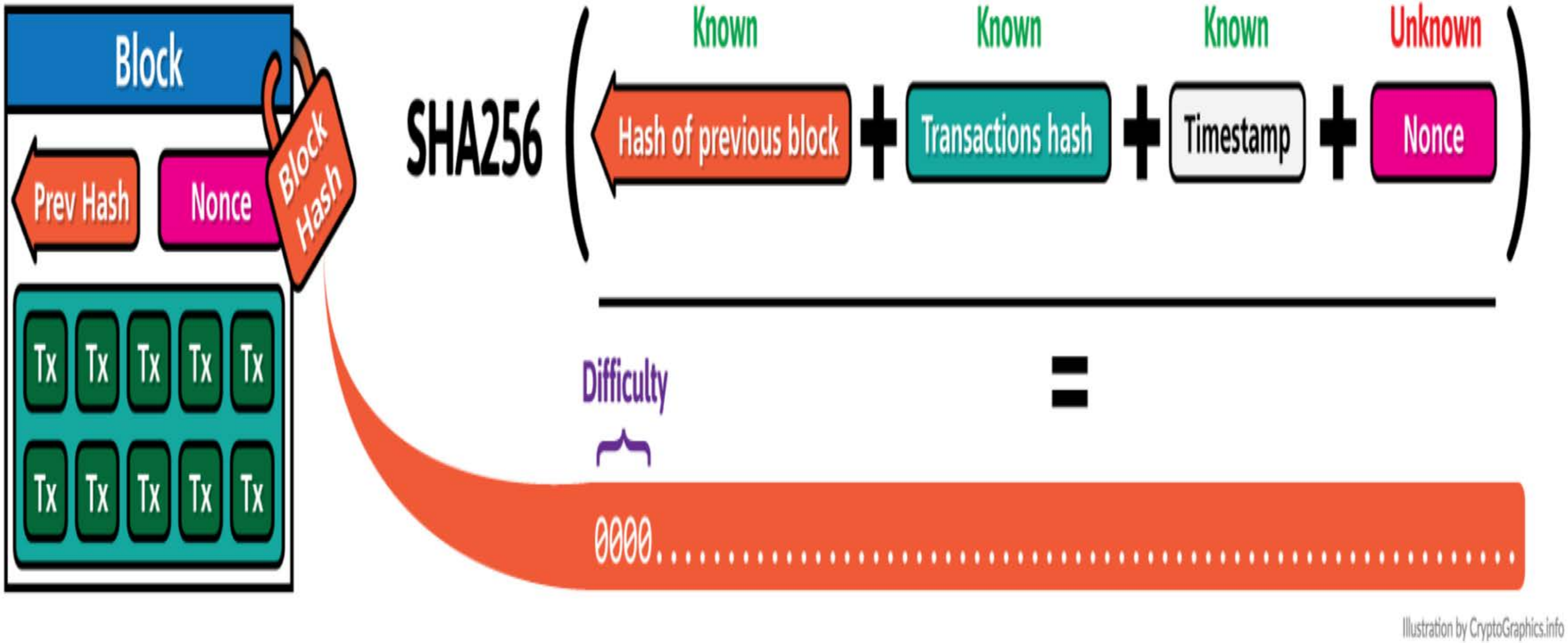
- Requires computational work to find a hash within predetermined range



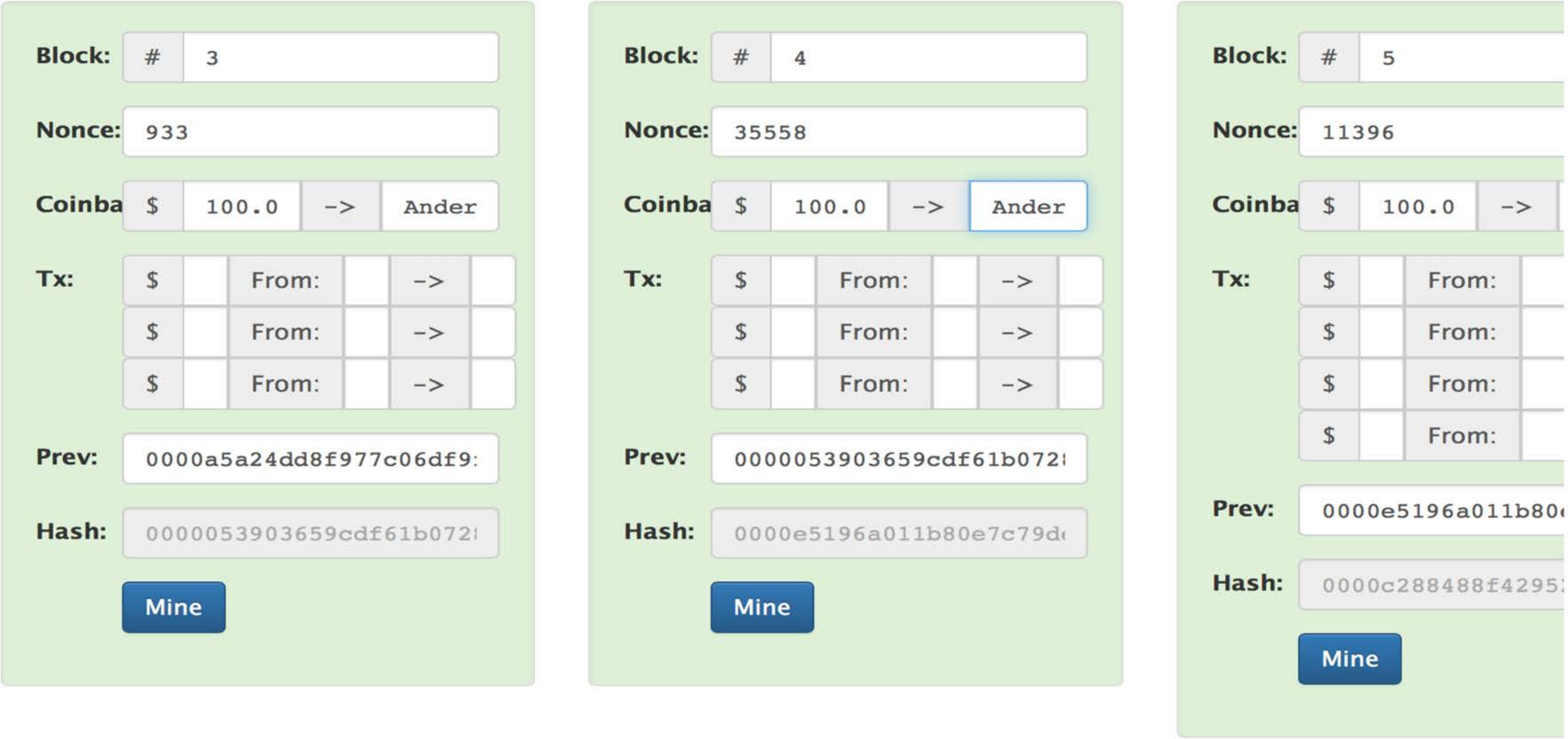
- Difficulty defined by Hash outputs' # of leading zeros
- Proof of Work can be Efficiently Verified

Blockchain – Proof of Work

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



Blockchain – Proof of Work



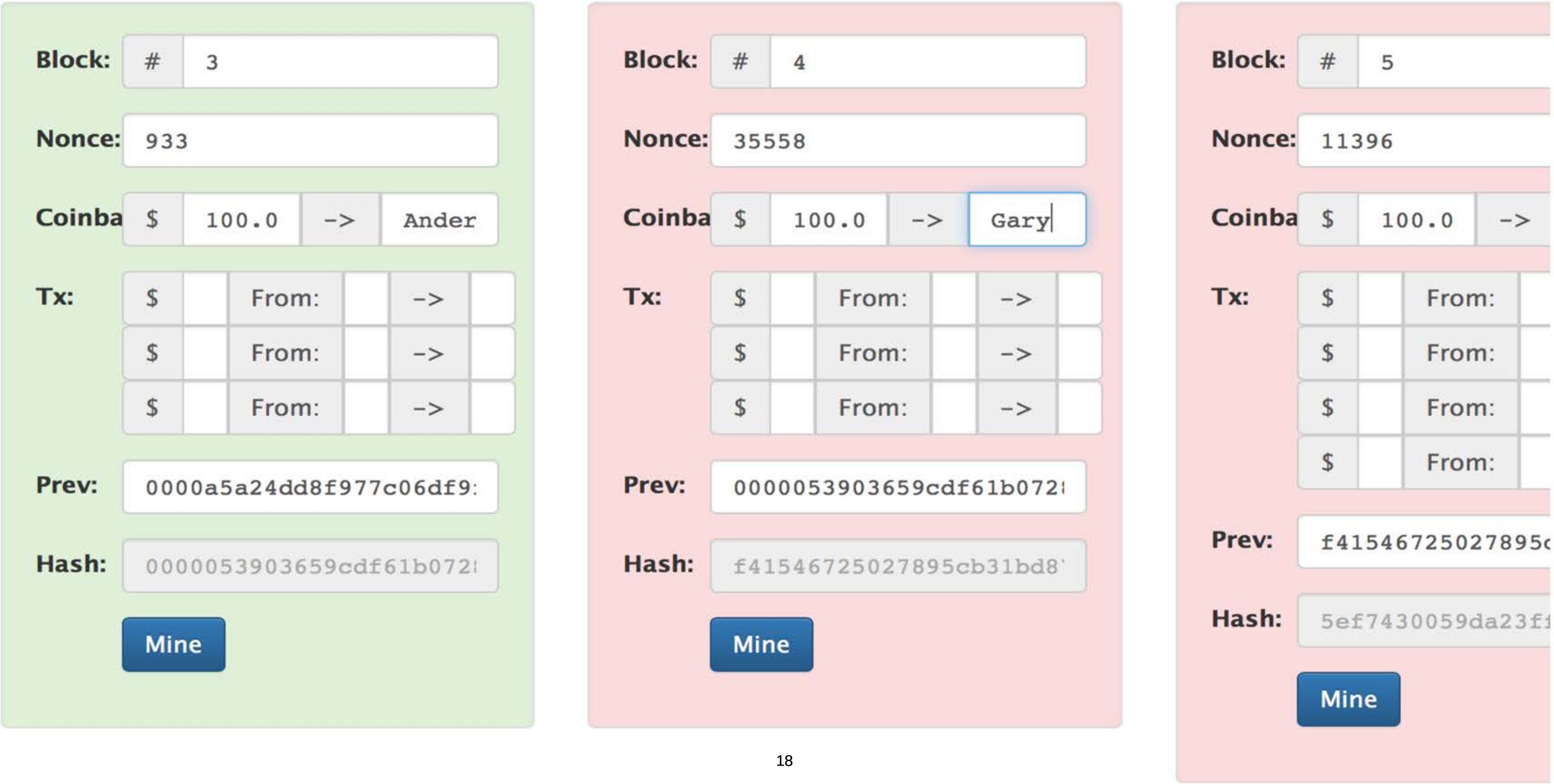
Block: # 3
Nonce: 933
Coinba $ 100.0 -> Ander
Tx: $ From: ->
$ From: ->
$ From: ->
Prev: 0000a5a24dd8f977c06df9
Hash: 000053903659cdf61b072
Mine

Block: # 4
Nonce: 35558
Coinba $ 100.0 -> Ander
Tx: $ From: ->
$ From: ->
$ From: ->
Prev: 000053903659cdf61b072
Hash: 0000e5196a011b80e7c79d
Mine

Block: # 5
Nonce: 11396
Coinba $ 100.0 ->
Tx: $ From:
$ From:
$ From:
$ From:
Prev: 0000e5196a011b80
Hash: 0000c288488f4295
Mine

Image by Anders Brownworth. Used with permission.

Blockchain – Proof of Work



Block: # 3

Nonce: 933

Coinba $ 100.0 -> Ander

Tx: $ From: ->
$ From: ->
$ From: ->

Prev: 0000a5a24dd8f977c06df9

Hash: 0000053903659cdf61b072

Mine

Block: # 4

Nonce: 35558

Coinba $ 100.0 -> Gary

Tx: $ From: ->
$ From: ->
$ From: ->

Prev: 0000053903659cdf61b072

Hash: f41546725027895cb31bd8

Mine

Block: # 5

Nonce: 11396

Coinba $ 100.0 ->

Tx: $ From:
$ From:
$ From:
$ From:

Prev: f41546725027895c

Hash: 5ef7430059da23f

Mine

Image by Anders Brownworth. Used with permission.

Blockchain – Consensus supports Longest Chain

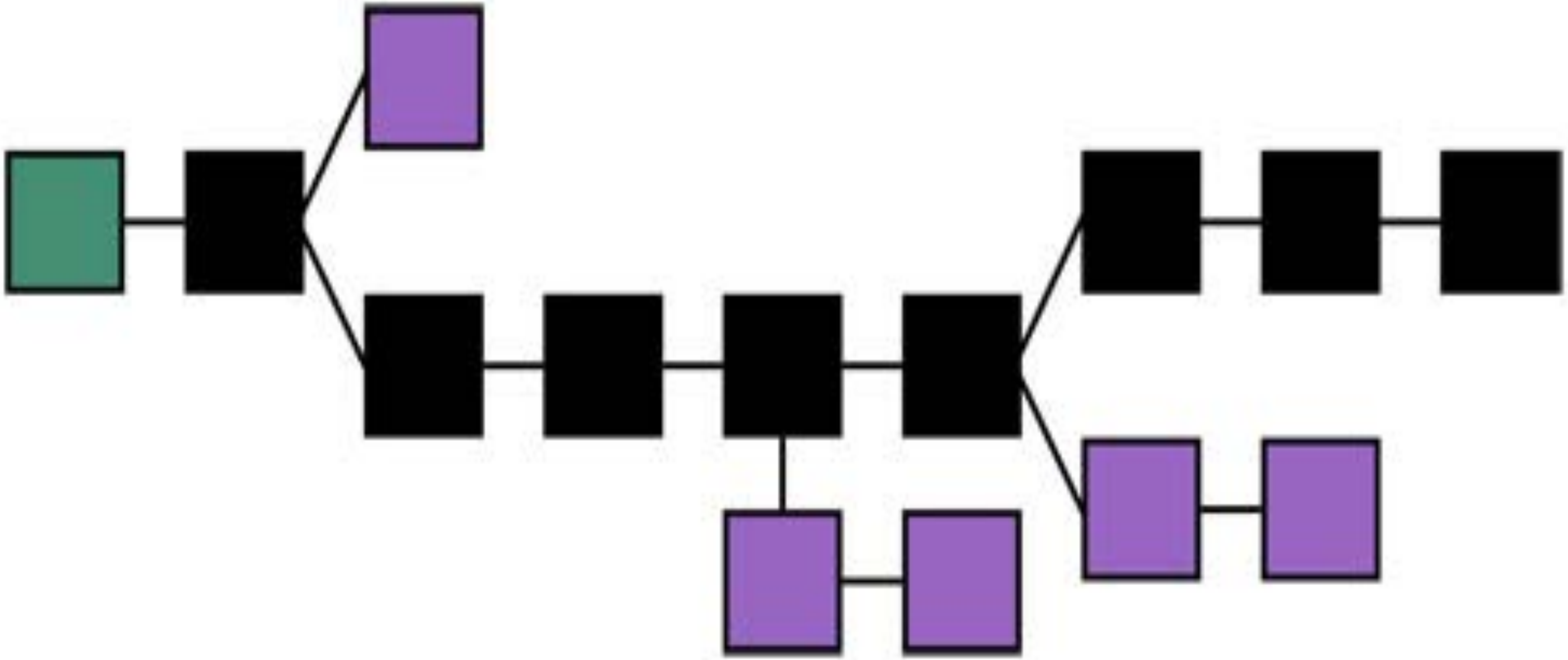


Image by Meek Mark on Wikipedia . CC BY.

Bitcoin Proof of Work Difficulty

- Targets 10 minute average block generation time

- Defined by the # of leading zeros Hash output requires to solve proof of work

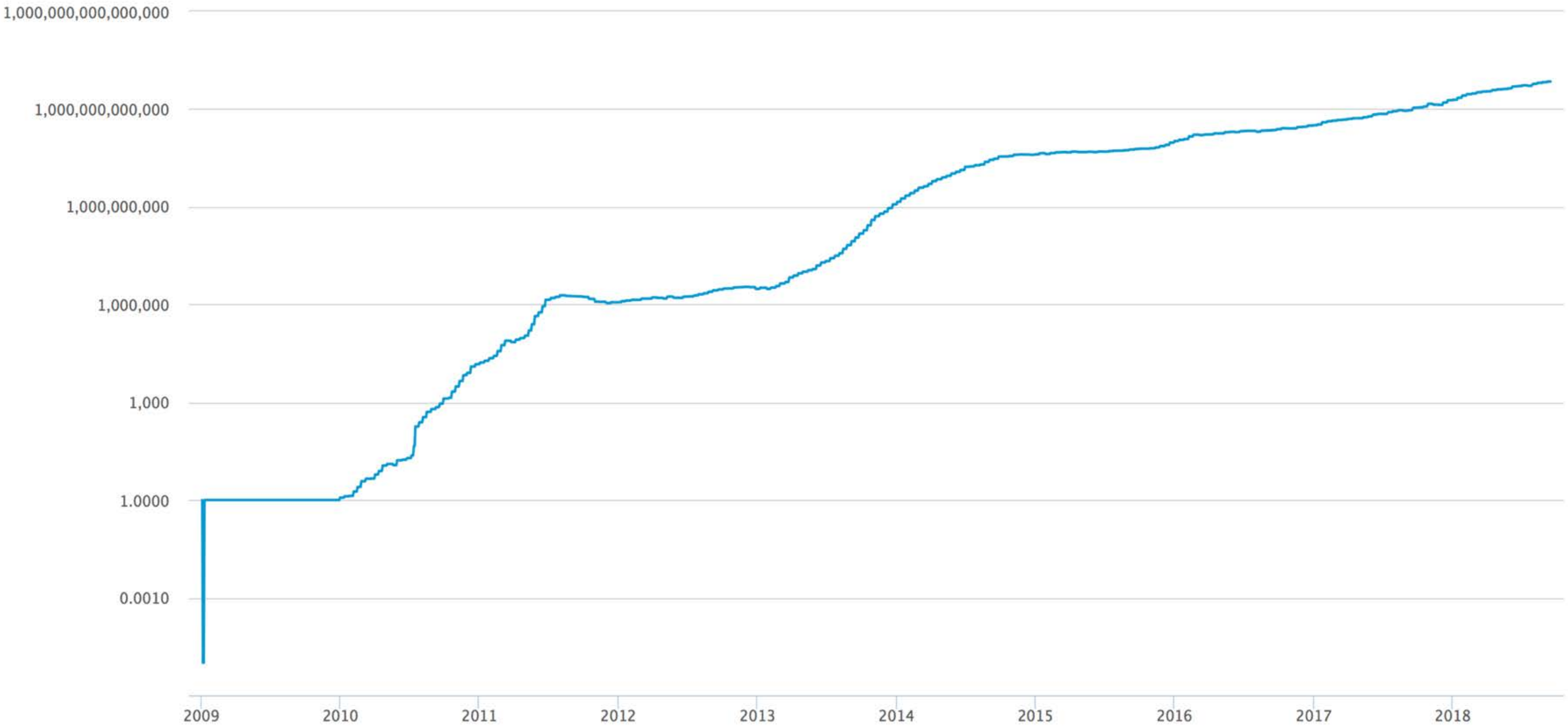
- Adjusts every 2016 blocks - about every two weeks

- Currently, ≥ 18 leading zeros (out of 64 hexadecimal characters)

- Block 541974 (9/18/18)- 18 leading zeros
  0000000000000000001104a863046dfbad1a2941128815669623ff93c2a3945f

- Genesis Block (1/3/09) – 10 leading zeros, though only required 8
  000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

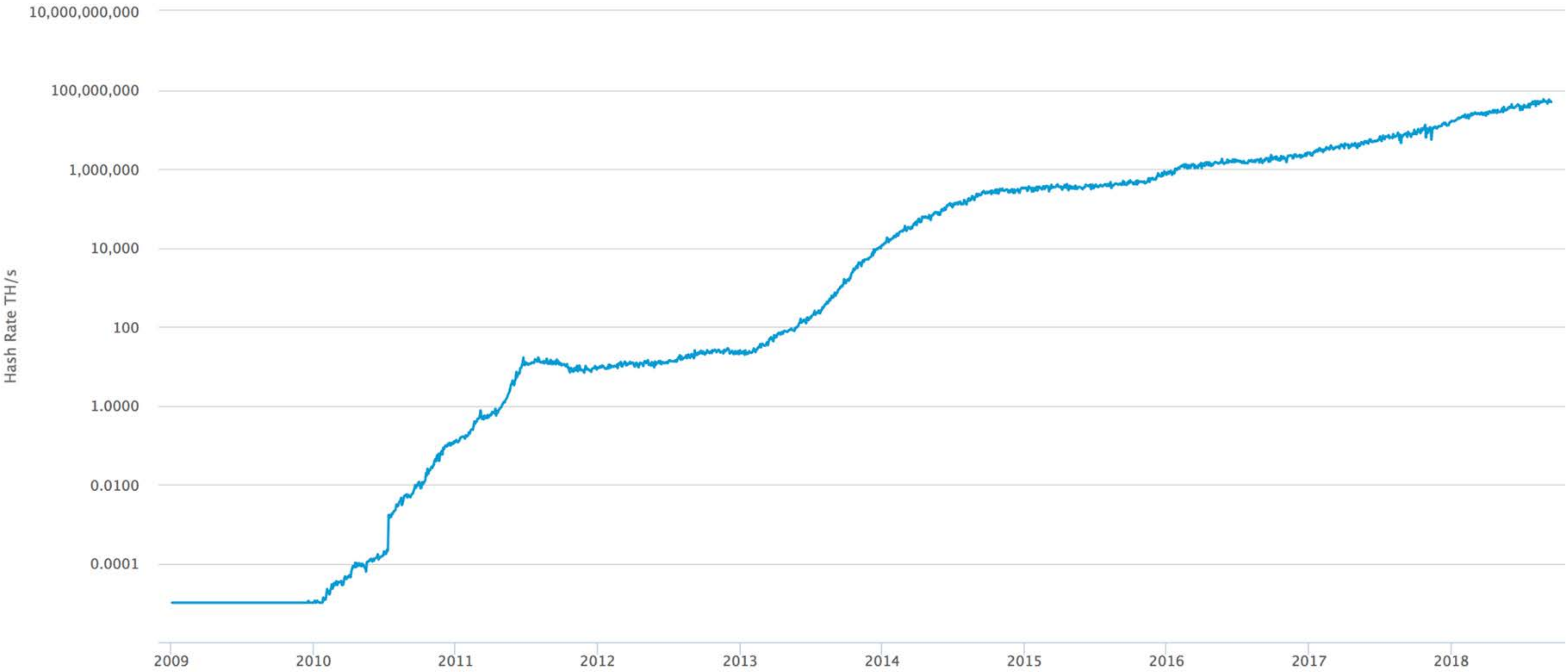
Bitcoin Mining Difficulty



Source: Blockchain.com

Courtesy of Blockchain Luxembourg S.A. Used with permission.

Bitcoin Network Hash Rate



Source: Blockchain.com

Courtesy of Blockchain Luxembourg S.A. Used with permission.

Bitcoin Mining Evolution

Central Processing Units (CPUs) 2009 – 2010
2 - 20 MH/S

Image by MiNE on flickr. CC BY

Graphics Processing Units (GPUs) 2010 – 2013
20 - 300 MH/S

Image is in the public domain.

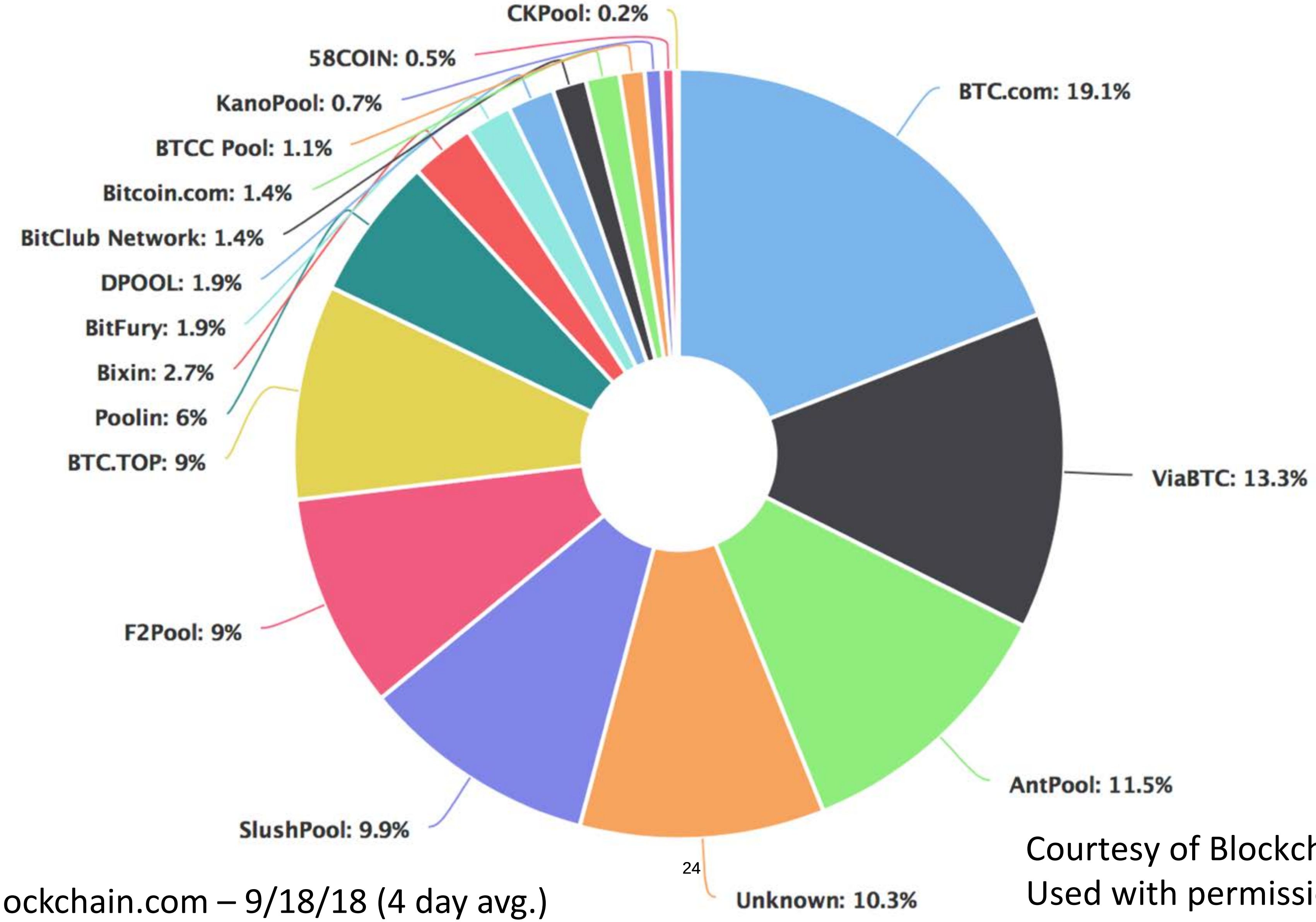
Application Specific Integrated Circuit (ASICs) 2013 – 2018
4 – 16 TH/S

Image by InstagramFOTOGRAFIN on Pixabay.

Modern Mining Factory

Image by Axel Castillo. CC0 Public Domain.

Bitcoin Mining Hashrate Distribution



Source: Blockchain.com – 9/18/18 (4 day avg.)

Courtesy of Blockchain Luxembourg S.A.
Used with permission.

Native Currency

Economic Incentive System
‘Monetary Policies’ vary widely

- Bitcoin - BTC
  - Created through Coinbase Transaction in each block
  - ‘Monetary Policy’ preset in Bitcoin Core
  - Creation originally 50 Bitcoin per block
  - Reward halves (1/2s) every 210,000 blocks
  - Currently 12.5 BTCs created per block – thus ‘inflation’ 4.1%
  - Currently 17.3 million BTC; capping at 21 million BTC in 2040
  - Market based transaction fee mechanism also provided for in Bitcoin Core
- Ethereum
  - Currently 3 ETH per block – thus ‘inflation’ 7.4%
  - Recent proposal to decline to 2 ETH per block in 11/18
  - Fees paid in Gas (10^9 Gas per ETH) for computation are credited to miners

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

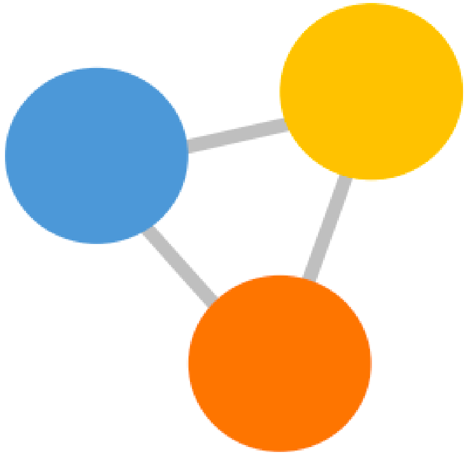
Alternative Consensus Protocols

Generally Randomized or Delegated Selection of Nodes to Validate next Block

- May have added mechanism to confirm Block Validators’ Work

Randomized Selection May be Based upon:

- Proof of Stake – Stake in Native Currency
- Proof of Activity - Hybrid of POW and POS
- Proof of Burn – Validation comes with Burning of Coins
- Proof of Capacity (Storage or Space) – Based upon Hardware Space



Delegated Selection May be Based upon Tiered System of Nodes

Major Permissionless Blockchain Applications still use Proof of Work – though:

- DASH is a hybrid of POW with a tiered system of ‘Masternodes’
- NEO uses a Delegated protocol of ‘Professional Nodes’

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? (Moved from 9/18)

- As many design features – public key cryptography, hash functions, append-only timestamped logs, digital cash, and proof-of-work – 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

Conclusions

Reviewed Bitcoin Design Features

- Timestamped Append-only Logs (Blocks)
- Secured through Cryptographic Hash Functions & Digital Signatures

Decentralized Network Consensus

- Consensus through Proof of Work
- Native Currency
- Network

Transactions Ledgers

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

15.S12 Blockchain and Money
Fall 2018