Consensus and Next generation blockchains

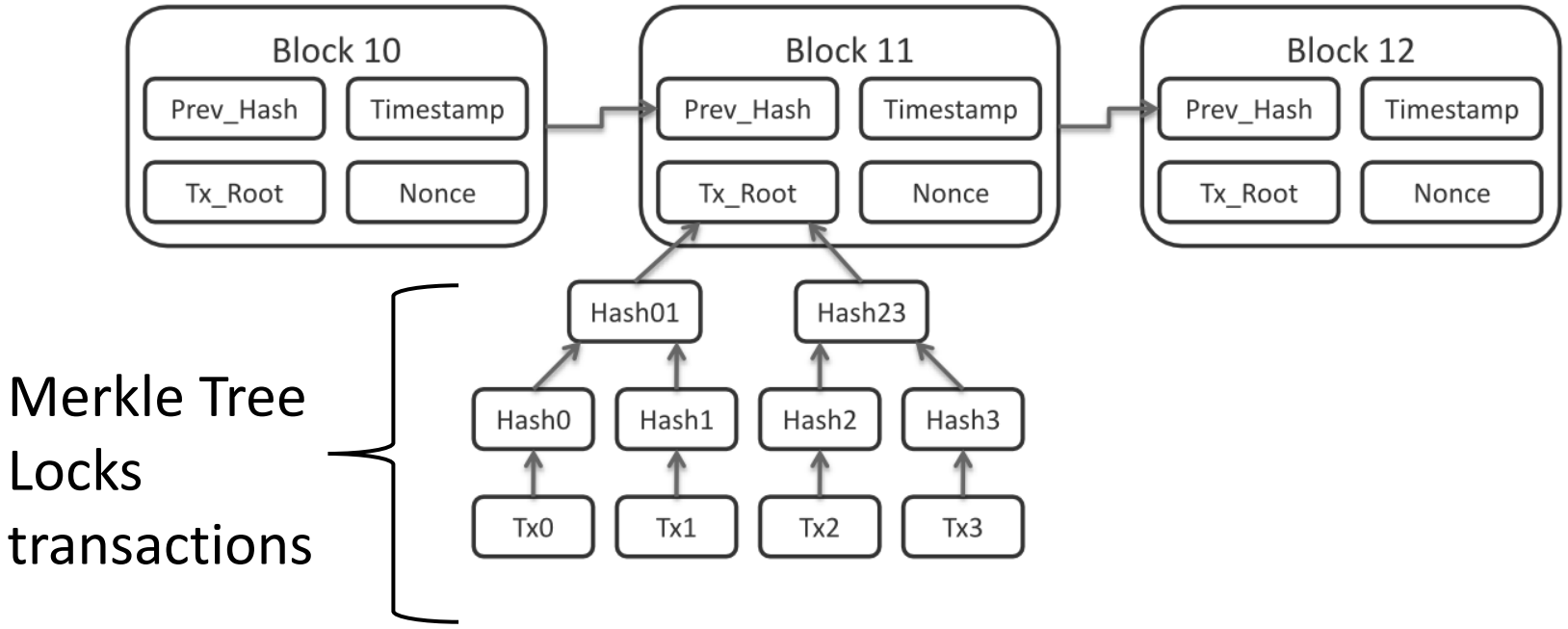
John R Williams, MIT

The FinTech Revolution

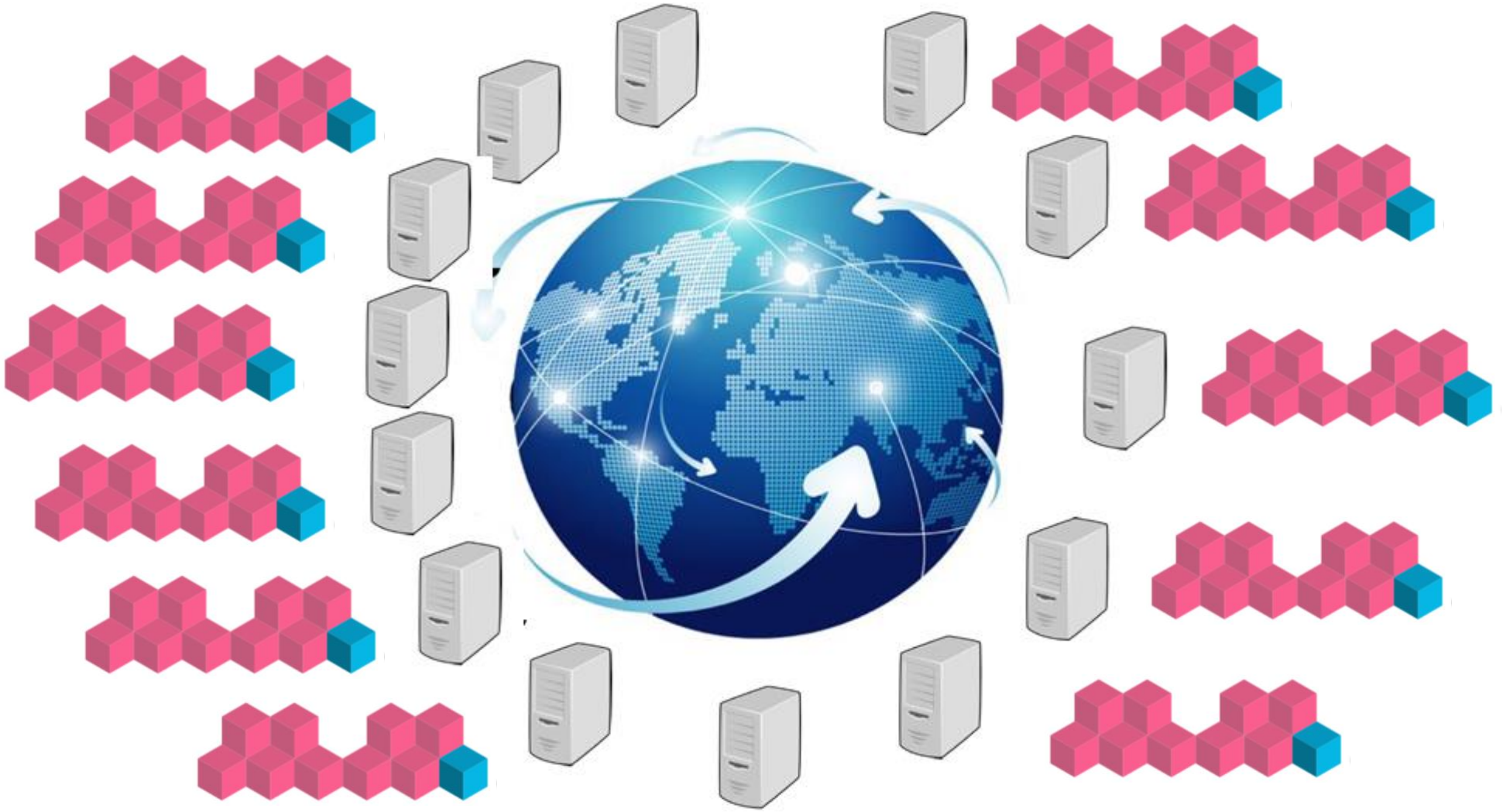
jrw@mit.edu

Proof of Work – Guess the Nonce that gives a hash starting 0000

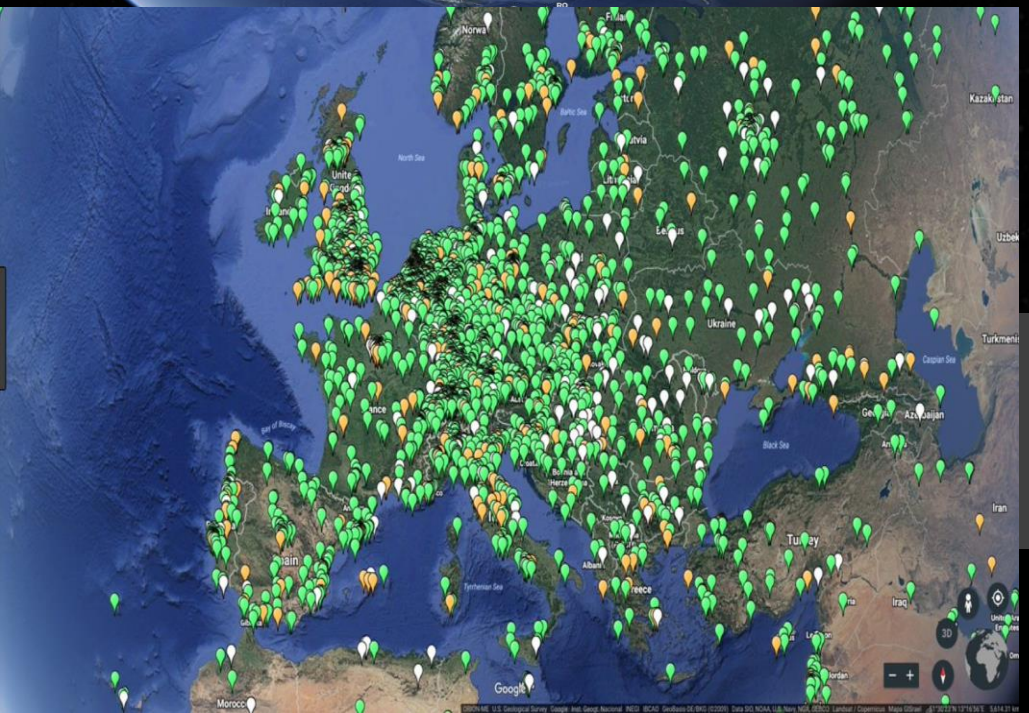
Hash(Prev_Hash + Tx_Root + Nonce) → 000000bc9xxx



Design Decision - All nodes must run exactly the same software



Choose one node to “mine” new block – then broadcast to all



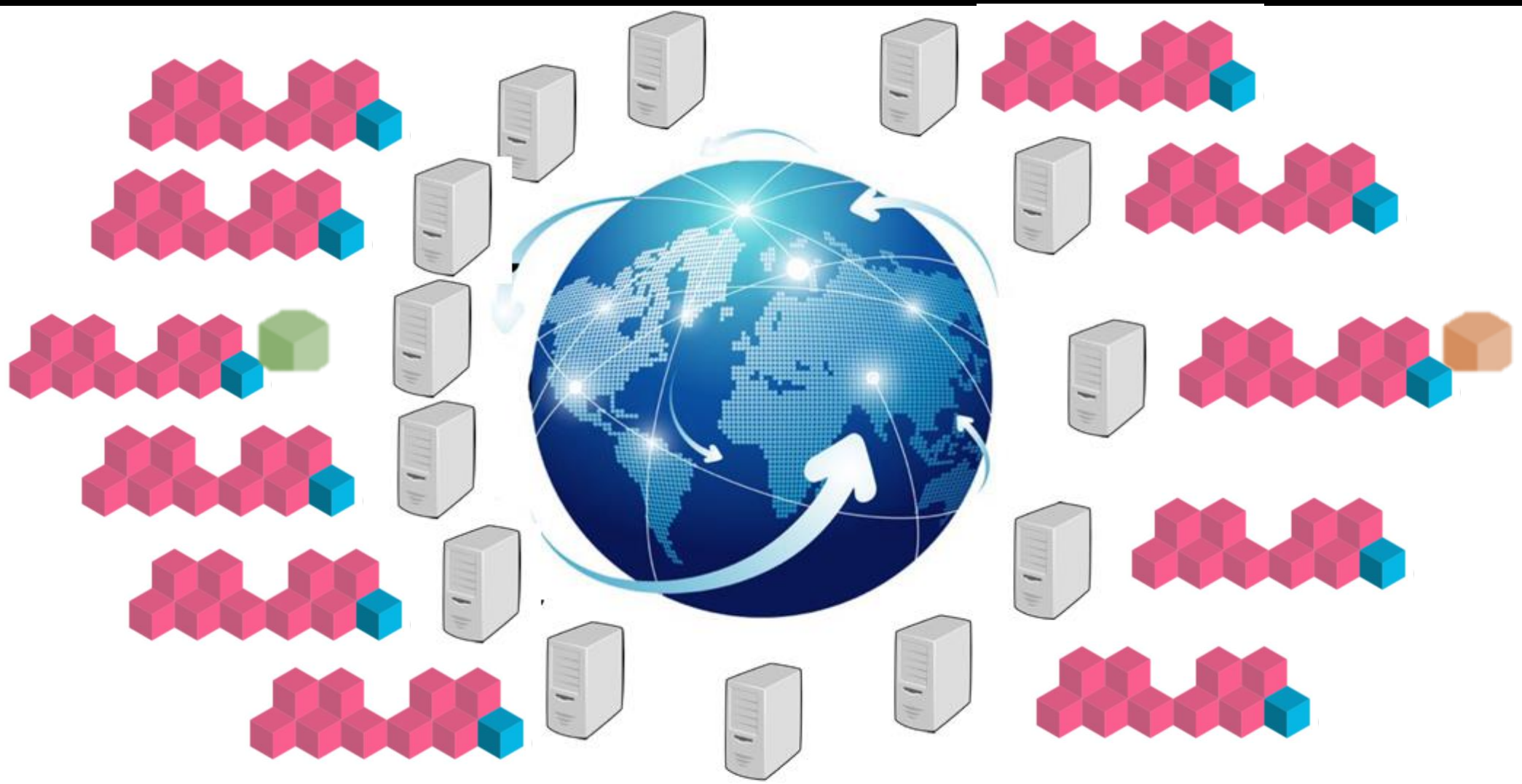
Active Etherium Nodes

Proof of Work is Expensive

Description	Value	Monthly change	Trend
Mining Revenue			
Average Bitcoin Price	$7,995	-11.52%	↓
Average Price Volatility	72.81%	-16.89%	↓
Mining Revenue from Fees	$8,039,216	-17.17%	↓
Mining Revenue from Blocks Mined	$516,713,328	-15.87%	↓
Total Mining Revenue	$524,752,544	-15.89%	↓
Mining Costs			
Total Costs of Mining	$251,568,949	5.92%	↑
Percentage of Total Revenue	47.94%	25.93%	↑
Total KWh Consumed	5,031,378,986	5.92%	↑
Network Statistics			
Total Transactions Processed	5,635,041	-1.67%	↓
Average KWh Consumed per TX	893	7.72%	↑
Average Fee per Transaction	$1.43	-15.38%	↓
Energy cost per TX (at 5 cents per KWh)	$44.65	7.72%	↑
Average Network Hashrate (GH/s)	30,627,726,466	11.48%	↑
Average Network Effciency (J/GH)	0.23	-1.81%	↓
Bounds			
Economic Maximum KWh Consumed	10,495,050,888	-15.89%	↓
Technical Minimum KWh Consumed	2,204,811,124	7.87%	↑


Next generation blockchains
Proof of Stake consensus

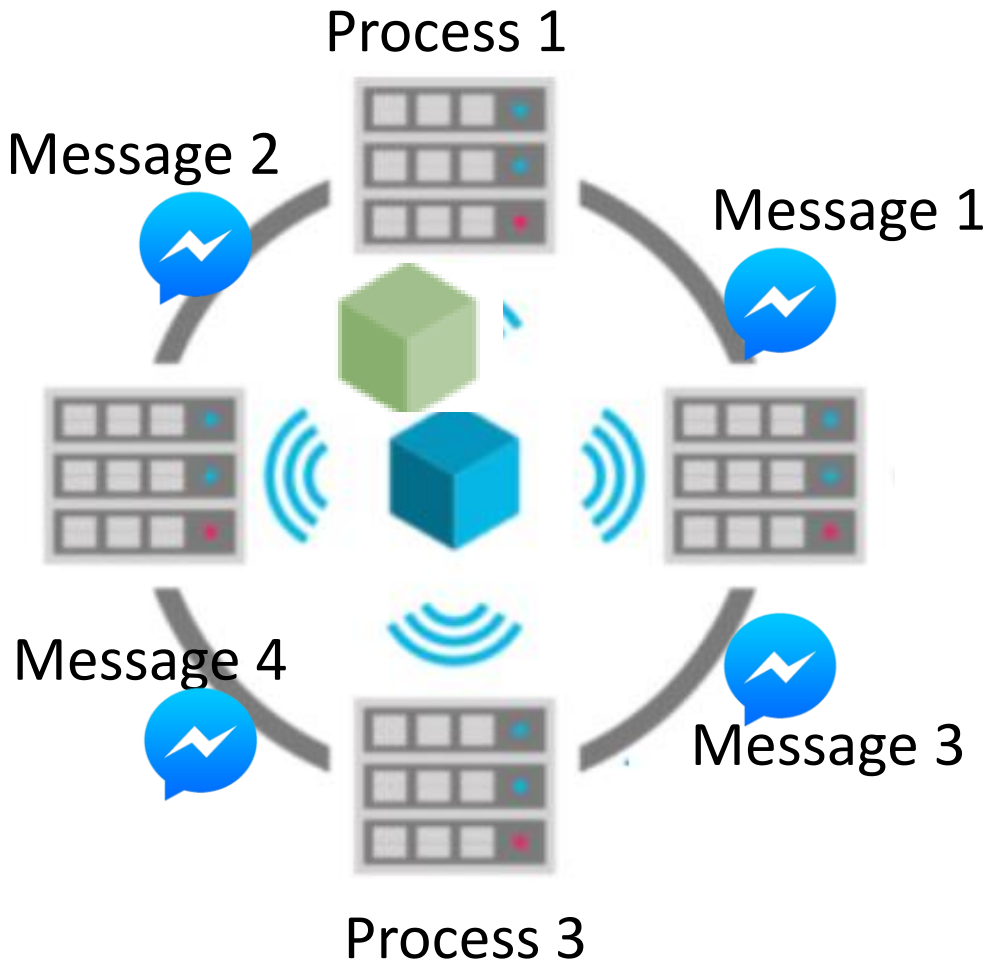
Consensus Problem – Every node must agree on same blocks?



Consensus in distributed network – which Block should we choose?

Byzantine Fault Tolerant Algorithms

- Termination – every correct process eventually decides
- Integrity – every correct process decides at least once
- Agreement – if one correct process decides v1 and another correct process decides v2 then v1=v2
- Validity – if one process decides v1 then at least one process proposed v1

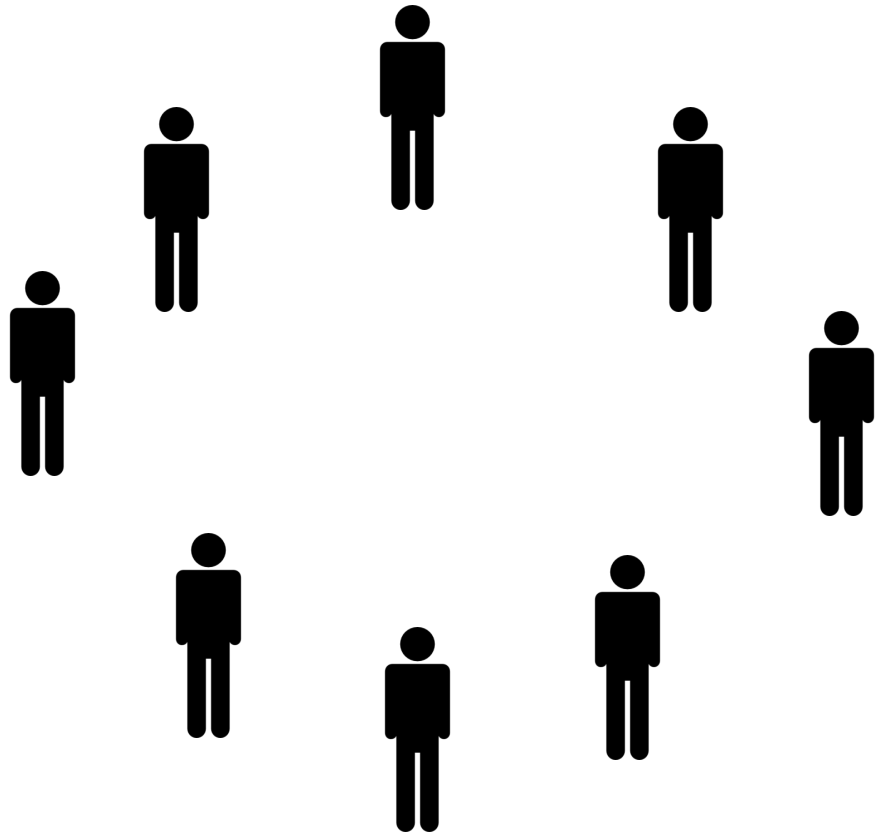


Algorithms are called Byzantine Fault Tolerant

Permissioned Blockchains eg HyperLedger, Algorand

General approach

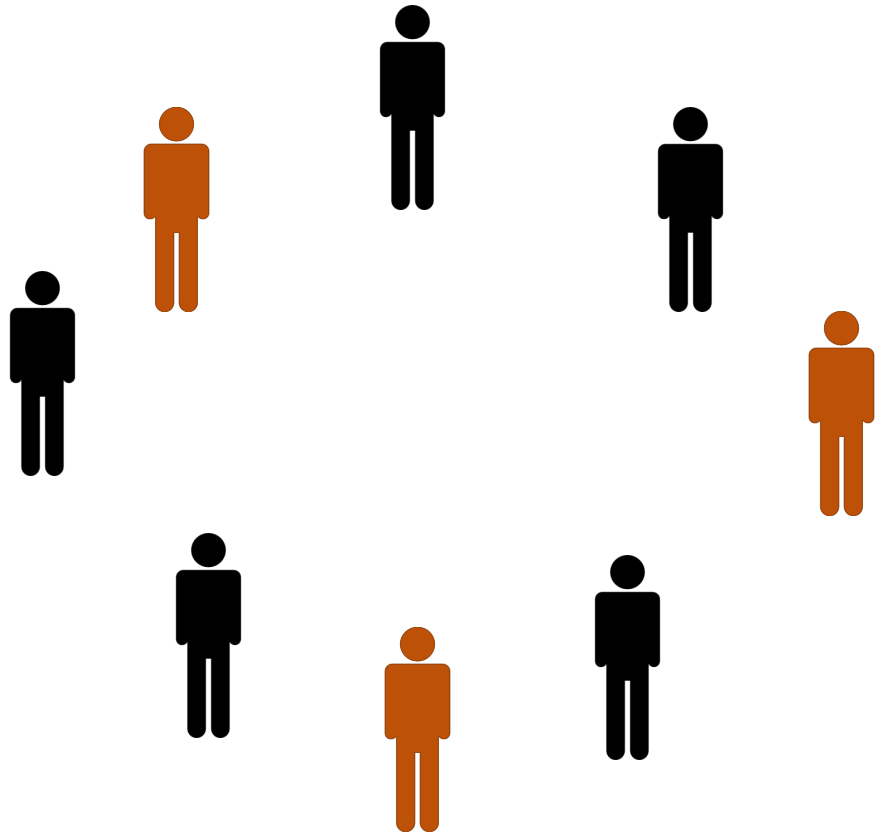
- Choose a number of leaders at random



Permissioned Blockchains – eg HyperLedger

General approach

- Choose a number of leaders at random

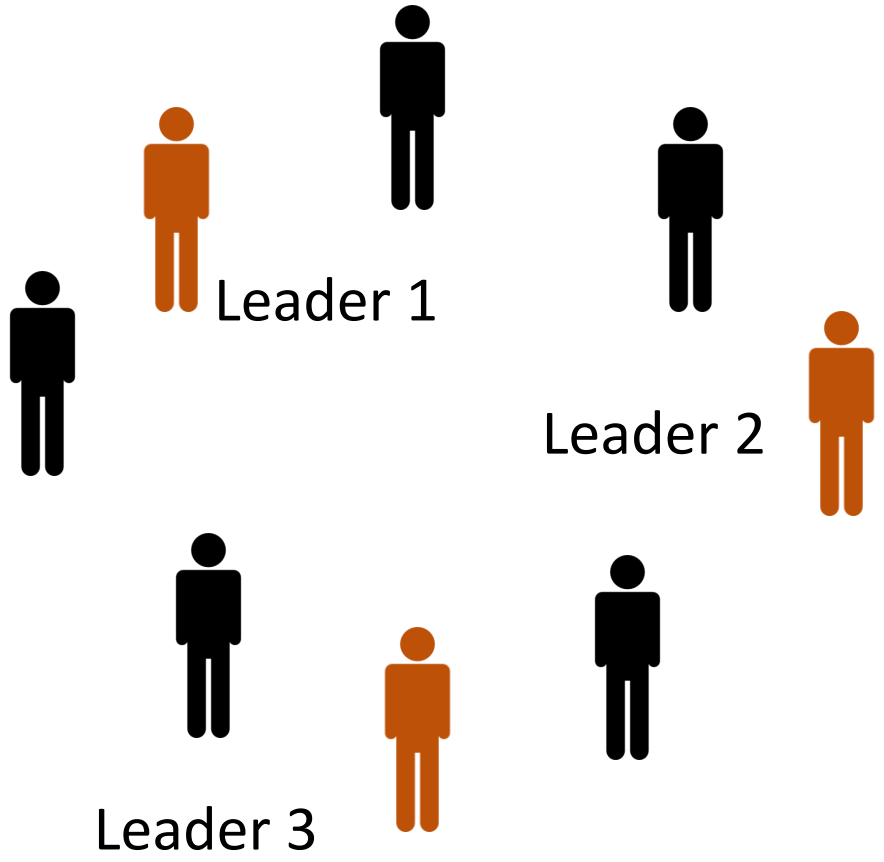


Permissioned Blockchains

General approach

- Order the chosen Leaders

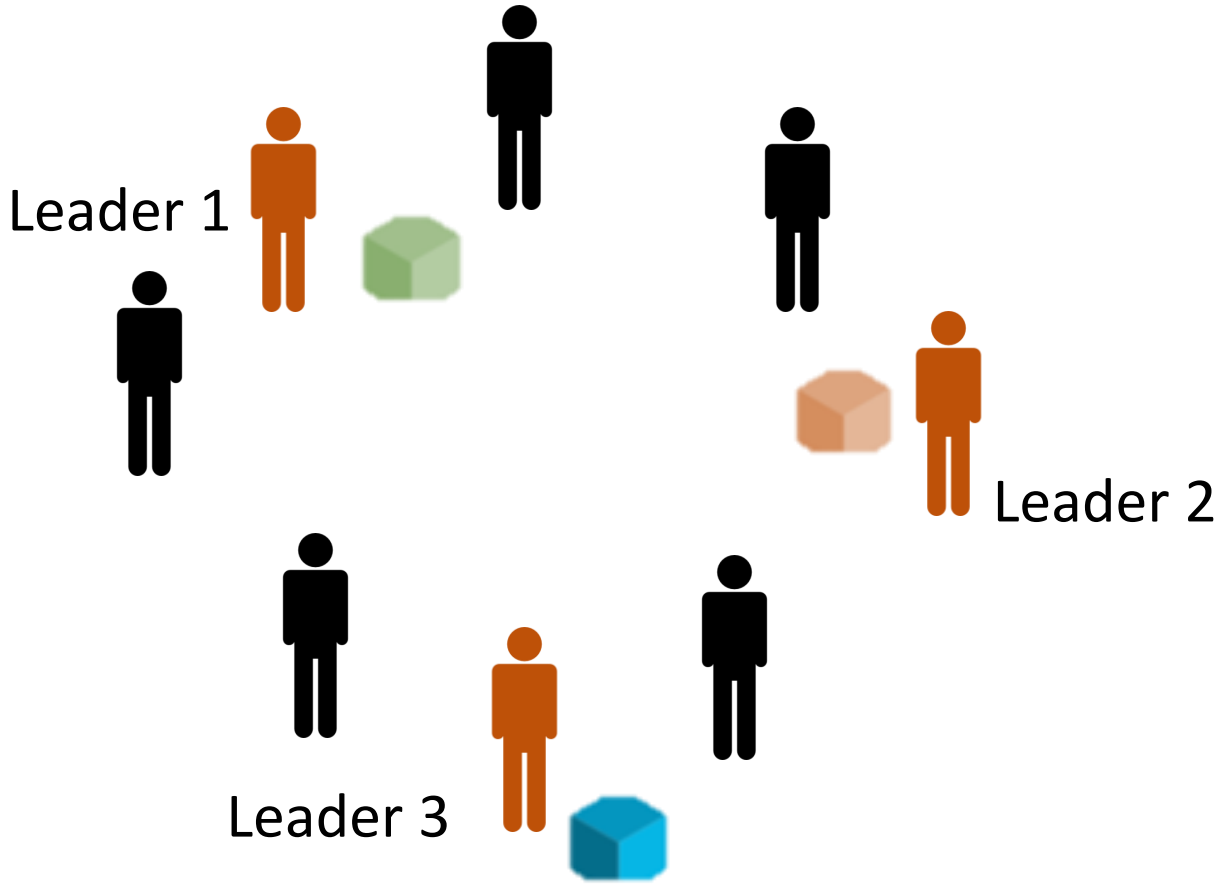
This is called SOLTITION



Permissioned Blockchains - HyperLedger

General approach

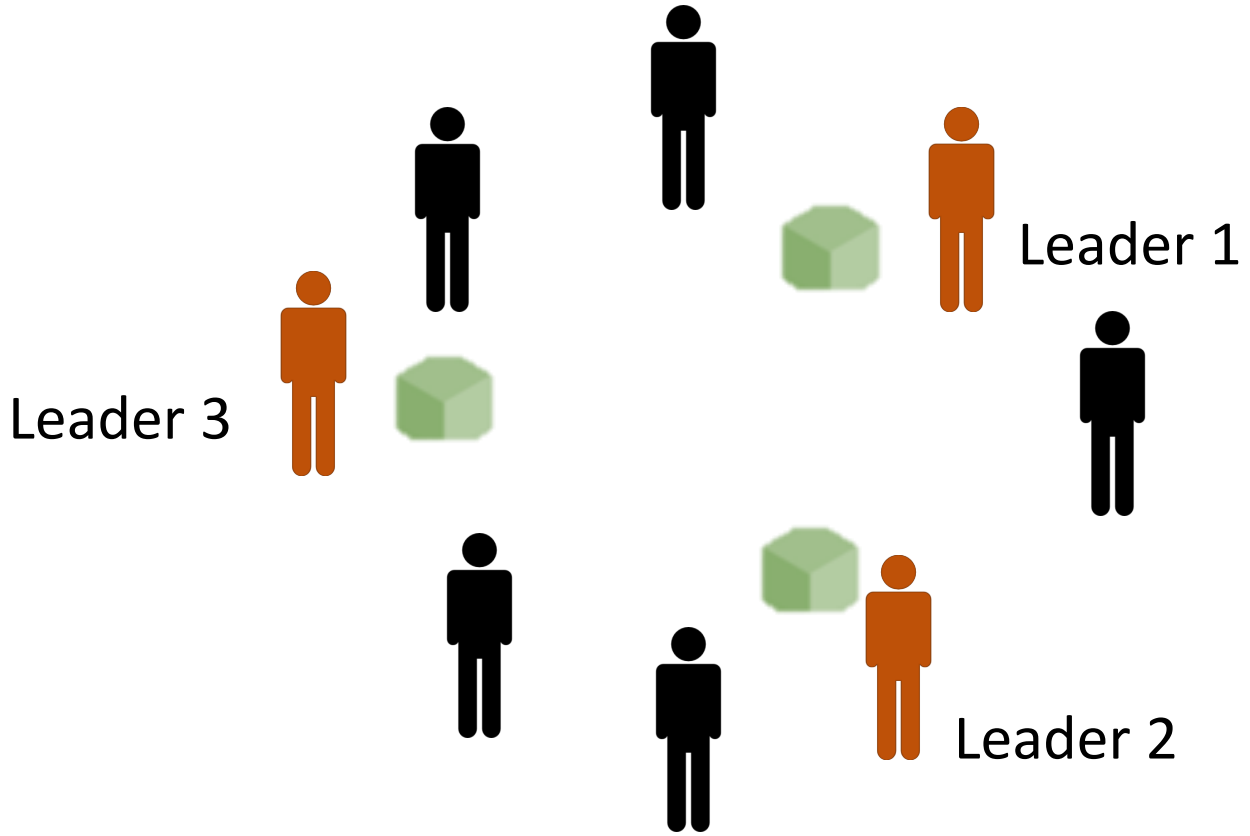
- Leaders broadcast their Block + proof of their leader status
- Rule: All nodes follow Leader 1 in next round (so long as block is valid)



Permissioned Blockchains – Algorand Consensus MIT

Round 2

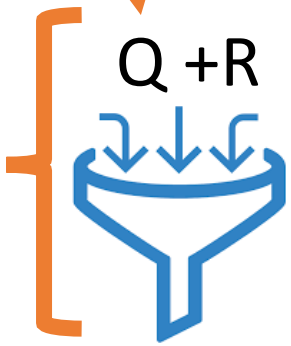
- New leaders chosen
- Based on messages they received from last round they follow Leader 1 and choose green block



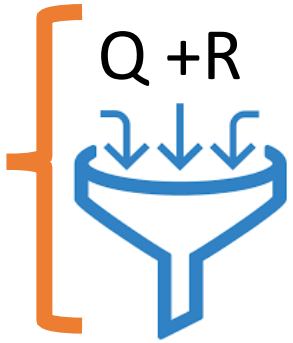
Round 1 so R = 1 both Alice and Bob can calculate Hash of (Q+R)

Q is Hash of Last Block added

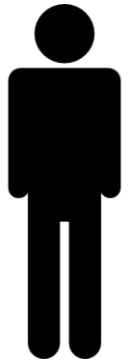
Alice



H(Q+R)

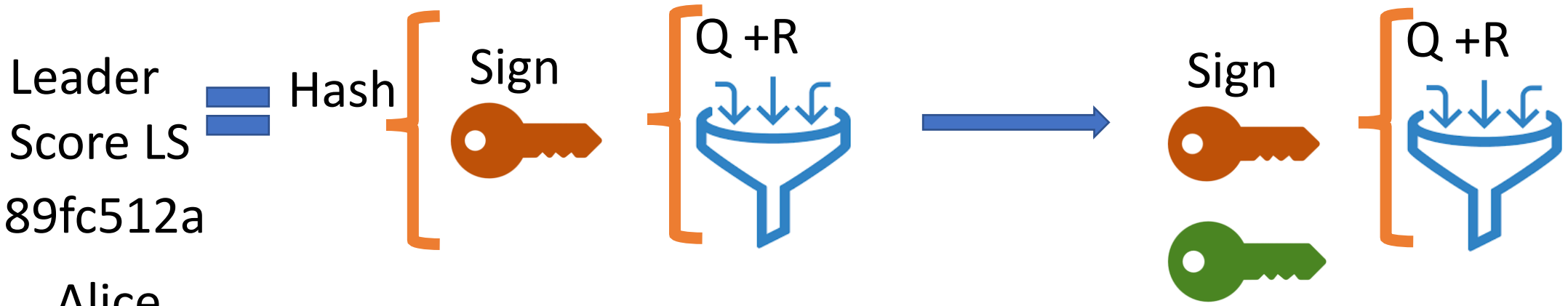


H(Q+R)



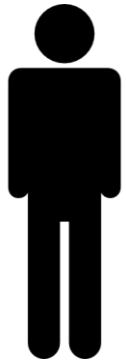
Bob

Alice sends Bob Sign(H(Q+R))



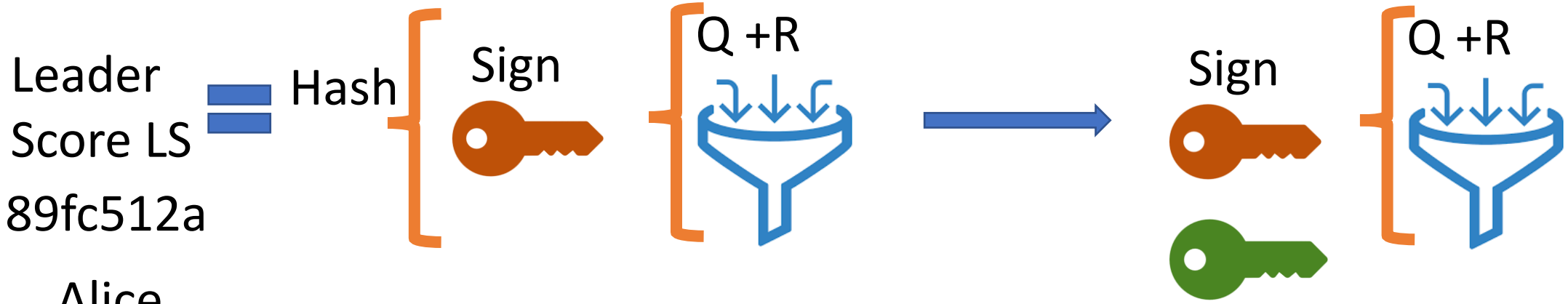
Alice

1. Bob can take the Hash of Alice's Proof and gets Alice's Leader Score = 89fc512a
2. Bob can Decrypt Alice's Proof and gets the same Q+R that he has. So he knows Alice's Leader score is valid. He still has zero knowledge of her private key.



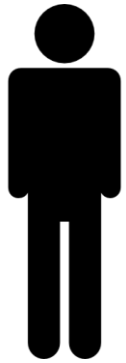
Bob

Prof Silvio Micali MIT – Zero Knowledge Proof



Alice

1. Bob can take the Hash of Alice's Proof and gets Alice's Leader Score = 89fc512a
2. Bob can Decrypt Alice's Proof and gets the same Q+R that he has. So he knows Alice's Leader score is valid. He still has zero knowledge of her private key.



Bob

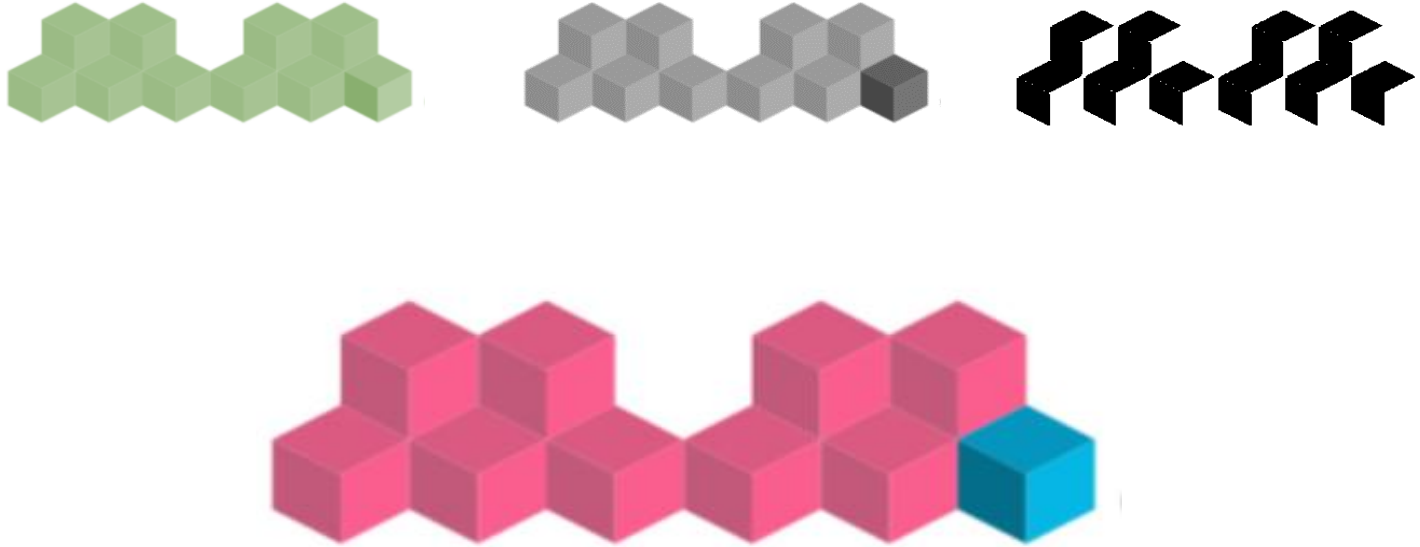
TABLE I: Evaluation of blockchain consensus protocols. Notation for binary values: ✓ has property, ✗ does not have property. Notation for non-binary values: ● has property, ◒ partially has property, ○ does not have property. Notation for meta-information: – the property does not apply to the given category, ? the value could not be extracted, ! the value is missing. The rows correspond to selected systems in each protocol category; a full list of the corresponding citations is provided in Appendix A. A list of terms is included in Appendix B. In the *Msg.* column (message complexity), n refers to the number of participants, and c is the size of the committee.

	Systems	code avail.	Committee Formation (Resources)	Strong consistency	Single Committee				Multiple Committee			Safety			Performances			
					Committee Configuration	Inter-Committee Consensus			Intra-Committee Configuration	Intra-committee Consensus		Transaction Censorship Resistance	DoS Resistance	Adversary Model	Throughput	Scalable	Latency	Exp. Setup
						Incentives (Join,Participate)	Leader	Msg.		Mediated	Incentives							
hybrid	**ByzCoin [84]**	✓	PoW	✓	Rolling (single)	✓✗	Internal	$O(n)$	-	-	-	✓	◒	33%	1000 tx/s [1]	✗	10–20s [1]	Real
	Solidus [16]	✗	PoW	✓	Rolling (single)	✓✓	External	$O(n^2)$	-	-	-	✗	◒	33%	-	-	-	-
	Algorand [70]	✗	Lottery	✓	Full swap	✗✗	Internal	$O(n^2)$	-	-	-	✗	●	33%	90 tx/h [2]	✗	40s [2]	Real
	Hyperledger [134]	✓	Permissioned	✓	Static	-	Flexible	Flexible	-	-	-	✓	●	33%	110k tx/s [3]	✗	<1s [3]	Real
	RSCoin [51]	✓	Permissioned	✓	Static	-	Internal	$O(n)$	✗	Client	✗	✓	●	33%	2k tx/s [4]	✓	<1s [4]	Real
	Elastico [95]	✗	PoW	✓	Full swap	✓✗	Internal	$O(n^2)$	Dynamic (Random)	!	!	✗	●	33%	16 blocks in 110s [5]	✓	110s for 16 blocks [5]	Real
	Omniledger [85]	✗	PoW/PoX	✓	Rolling (subset)	✓✗	Internal	$O(n)$	Dynamic (Random)	Client	✗	✓	●	33%	≈10k tx/s [6]	✓	≈1s [6]	Real
	Chainspace [18]	✓	Flexible	✓	Flexible	✗✗	Internal	$O(n^2)$	✗	✗	✗	✓	◒	33%	350 tx/s [7]	✓	<1s [7]	Real
proof-of-X	**Ouroboros [83]**	✗	Lottery	✗	Full swap	✓✓	Internal	$O(nc)$	–	–	–	✗	◒	50%	257.6 tx/s [9]	✗	20s	Simulation
	Praos [52]	✗	Stake	✗	Rolling (subset)	✓✓	Internal	O(1)	–	–	–	✗	●	50%	–	–	–	–
	Snow-white [50]	✗	Stake	✗	Full swap	✓✓	Internal	O(1)	–	–	–	✗	◒	50%	100-150 tx/s [9]	✓	?	Simulation
	PermaCoin [102]	✓	PoW/PoR[11]	✗	Rolling (single)	✗✓	Internal	$O(1)$	–	–	–	✓	●	50%	–	✗	–	–
	SpaceMint [77]	✓	PoS	✗	Rolling (single)	✗✓	Internal	$O(1)$	–	–	–	✓	●	50%	?	✗	600s	Simulation
	Intel PoET [79]	✓	TH[12]	✗	Rolling (single)	✗✓	Internal	$O(1)$	–	–	–	✓	●	TH[12]	1000 tx/s [10]	✓	–	Real
	REM [139]	✗	TH[12]	✗	Rolling (single)	✗✓	Internal	$O(1)$	–	–	–	✓	●	TH[12]	!	✓	–	Real
proof-of-work	**Bitcoin [105]**	✓	PoW	✗	Rolling (single)	✗✓	Internal	$O(1)$	–	–	–	✓	●	50%	7 tx/s	✗	600s	Real
	Bitcoin-NG [61]	✗	PoW	✗	Rolling (single)	✗✓	Internal	$O(1)$	–	–	–	✓	◒	50%	7 tx/s	✗	<1s	Simulation
	GHOST [126]	✗	PoW	✗	Rolling (single)	✗✓	Internal	$O(1)$	–	–	–	✓	●	50%	–	✗	–	–
	DECOR+HOP [92]	✗	PoW	✗	Rolling (single)	✗✓	Internal	$O(1)$	–	–	–	✓	●	50%	30 tx/s [8]	✗	60s	Simulation
	Spectre [125]	✗	PoW	✗	Rolling (single)	✗✓	Internal	$O(1)$	–	–	–	✓	●	50%	–	✗	–	–

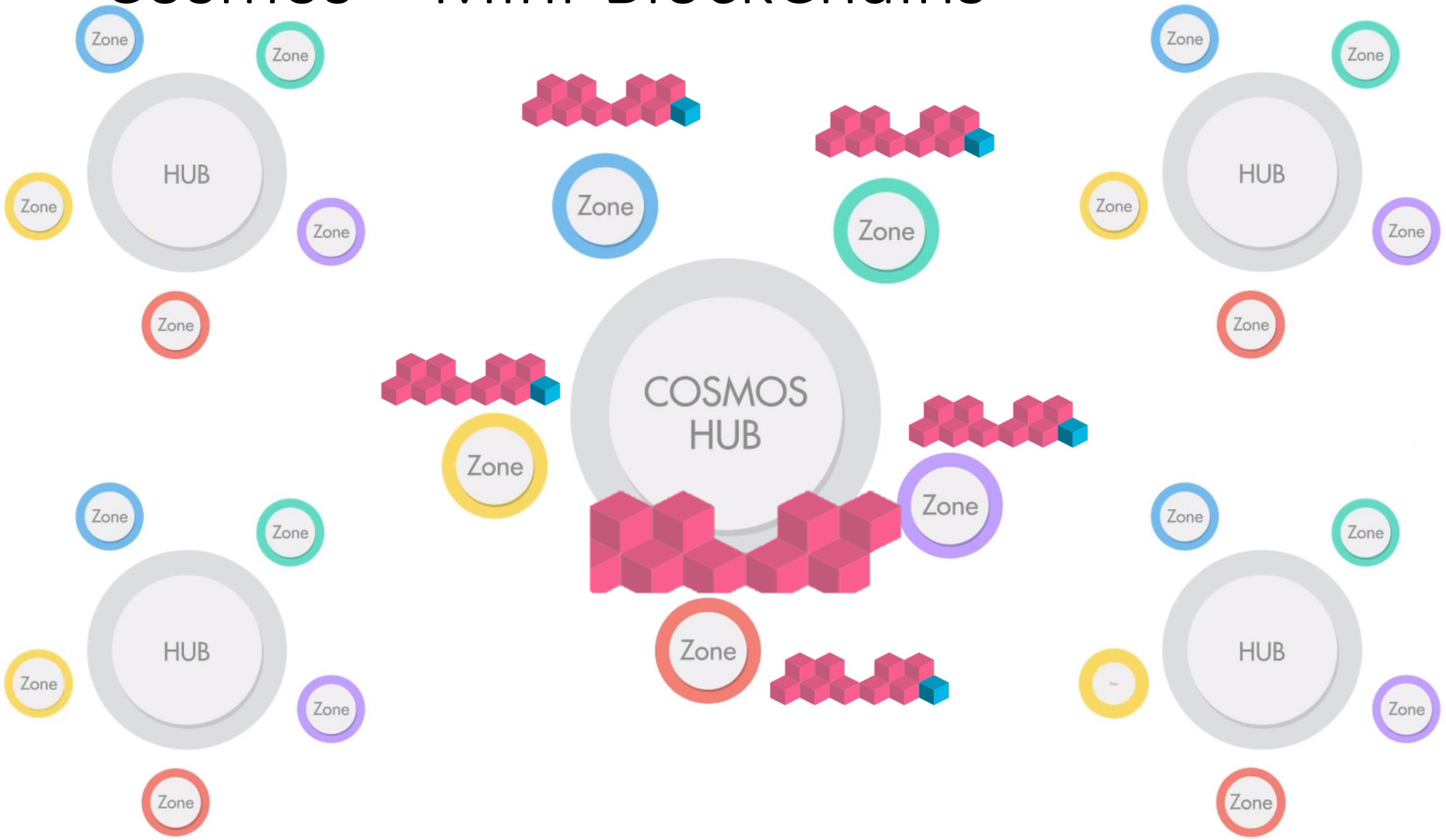
Next generation blockchains
Side chains, sharding

Side chains (sharding)

- Side chains run independently from Main Chain. They commit only Merkle Root of many transactions



Cosmos – Mini-BlockChains



BitCoin Attacks

Date	Event
2007	Satoshi began working on the Bitcoin concept
18.8.2008	Bitcoin is registered
3.1.2009	The Genesis Block is mined
12.1.2009	First Bitcoin transaction
5.10.2009	An exchange rate is established
6.2.2010	A currency exchange is born
17.7.2010	MtGox is established
15.8.2010	**A vulnerability in the system** is discovered and exploited, resulting in the generation of 184 billion Bitcoins
18.9.2010	First collective mining starts
29.9.2010	Another **exploit discovered**
28.10.2010	First ever short sale
9.12.2010	First call option contract sold
2011	**Silk Road** opens for business
28.1.2011	25% of total Bitcoins generated
9.2.2011	Bitcoin reaches parity with USD (1:1)
12.4.2011	First put option sold

BitCoin Attacks

Date	Event
12.6.2011	The Great Bubble of 2011
13.7.2011	25,000 BTC **theft** reported
19.7.2011	**Major breach** at MtGox
26.7.2011	Bitomat (Poland) **loses 17,000 Bitcoins**
5.8.2011	MyBitcoin **loses 150,000 Bitcoins**
6.9.2011	Creation of physical Bitcoins
13.2.2012	Second largest Bitcoin exchange **shuts down**
1.3.2012	Linode hacked **46,000 BTC stolen**
9.5.2012	**FBI report** on Bitcoin leaked
11.5.2012	Bitcoinica **hacked** (18,000 BTC)
3.9.2012	Bitfloor **hacked** (24,000 BTC)
24.9.2012	Bitcoin Savings and Trust investigated for running **Ponzi scheme**
8.3.2013	BitInstant **hacked** (12,000 $)
11.3.2013	**Glitch** causes halt in transactions
28.3.2013	Market cap reaches $ 1 billion
1.4.2013	Bitcoin surpasses $100
20.4.2013	Bitcoin Central is **hacked**
1.5.2013	Gaming company caught **secretly mining** Bitcoins from customer computers

BitCoin Attacks

Date	Event
2.5.2013	First Bitcoin ATM (San Diego)
14.5.2013	MtGox **funds seized** by Homeland
18.5.2013	Online casino that accepts Bitcoin is founded
23.5.2013	Bitcoin central gets **hacked**
1.6.2013	Winklevoss Bitcoin Trust filed
6.8.2013	Bitcoin ruled currency by Texas judge
12.8.2013	22 Bitcoin companies **subpoenaed**
20.8.2013	Bitcoin ruled private money in Germany
2.10.2013	**FBI shuts down Silk Road** (3.6 milllion USD seized)
2.10.2013	BitcoinTalk.org **hacked**
31.10.2013	BitMarket.eu **closes** the doors
13.11.2013	Senate hearing of potential Bitcoin **risks and threats**
19.11.2013	Bitcoin goes above $ 1000
2.12.2013	96,000 Bitcoins are **stolen** from Sheep Marketplace
5.12.2013	China **bans** Bitcoin transactions
26.1.2014	BitInstant CEO charged with **money laundering**
12.09.2014	**First bitcoin swap approved**