Consensus Protocols II

Murat Osmanoglu

Consensus Protocols for Blockchain

- depending on the methods employed to select leaders to generate blocks, or to vote newly generated blocks, protocols analyzed here under two categories:

Consensus Protocols for Blockchain

- depending on the methods employed to select leaders to generate blocks, or to vote newly generated blocks, protocols analyzed here under two categories:

- lottery-based consensus protocol,
  - leaders randomly selected with a probability in proportion to some criteria such as its computing power, or its stake
  - newly created blocks appended to the chain without using BFT type voting mechanism
  - block finalization probabilistic

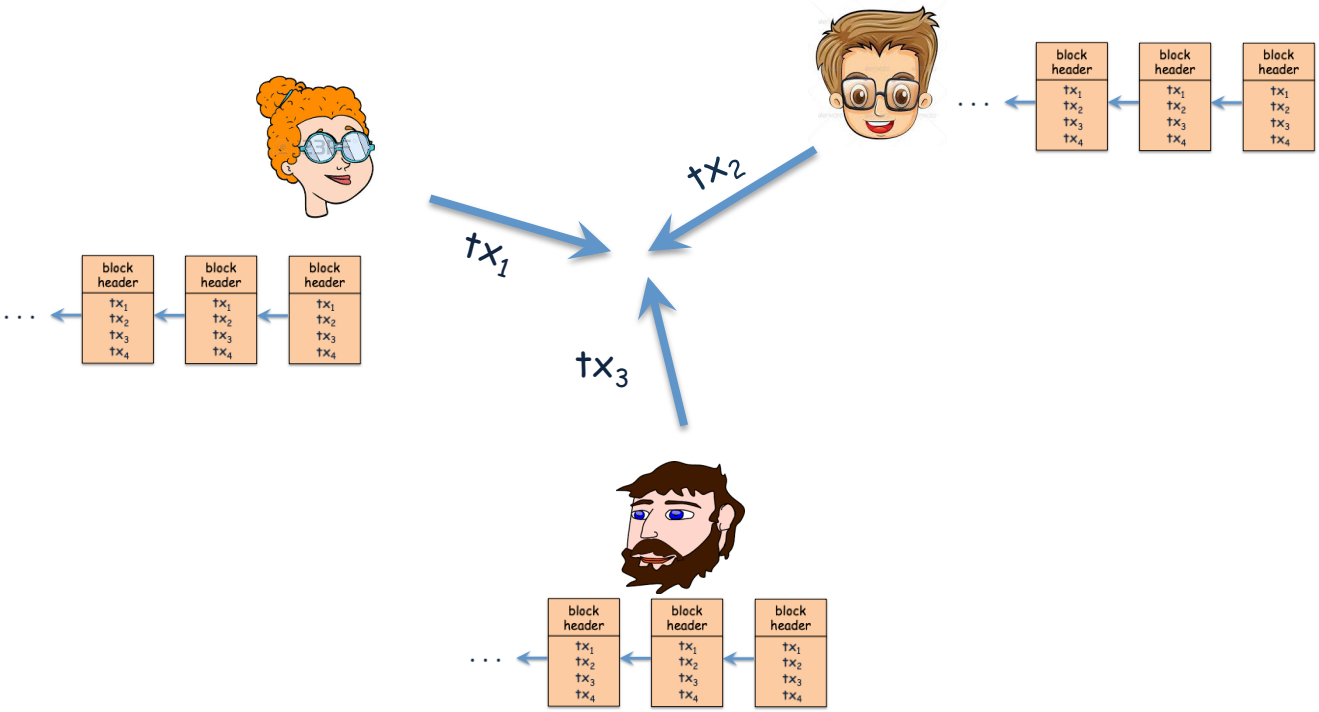
Consensus Protocols for Blockchain

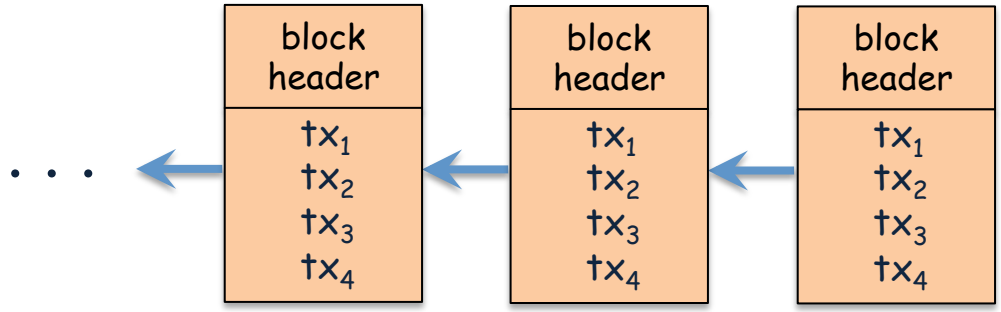
- depending on the methods employed to select leaders to generate blocks, or to vote newly generated blocks, protocols analyzed here under two categories:

- lottery-based consensus protocol,
  - leaders randomly selected with a probability in proportion to some criteria such as its computing power, or its stake
  - newly created blocks appended to the chain without using BFT type voting mechanism
  - block finalization probabilistic

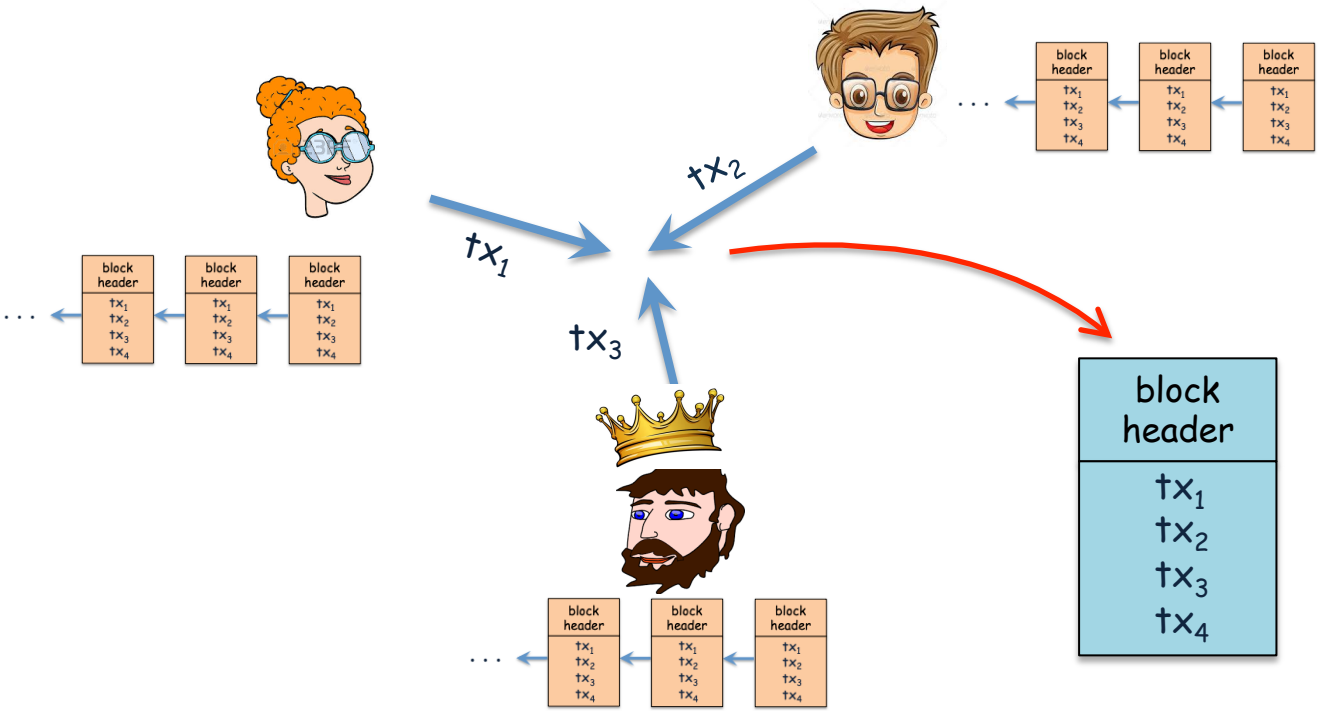
- voting-based consensus protocol,
  - leaders determined by utilizing simpler methods (round-rabin vs.)
  - newly created blocks appended to the chain through BFT type voting mechanism
  - block finalization deterministic

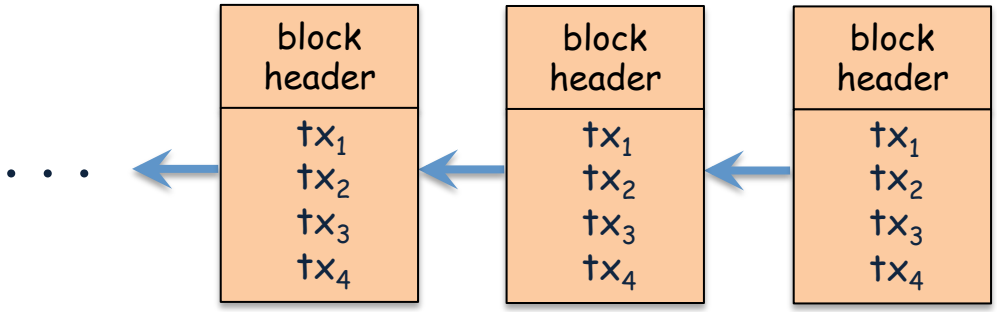
Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)



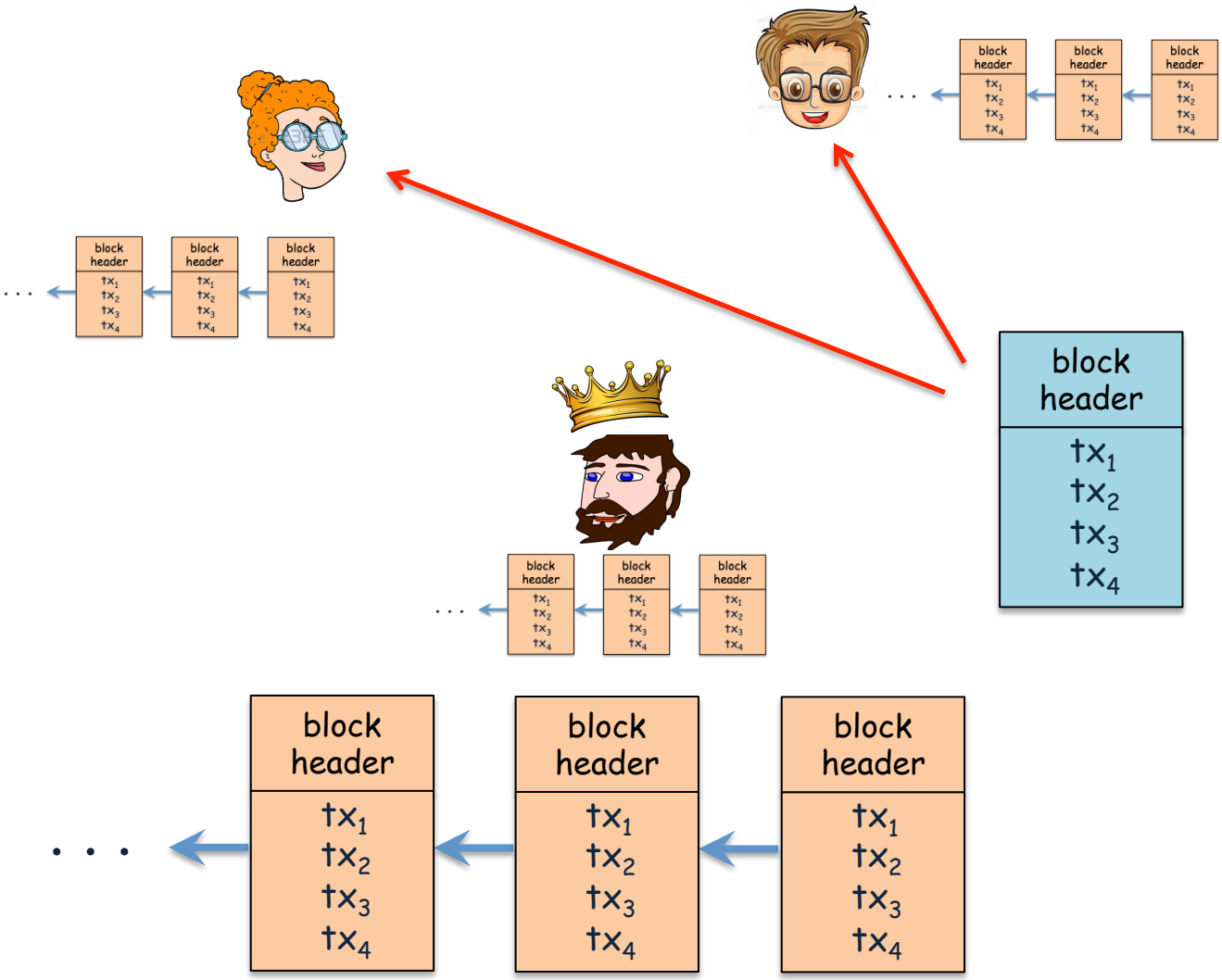


Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

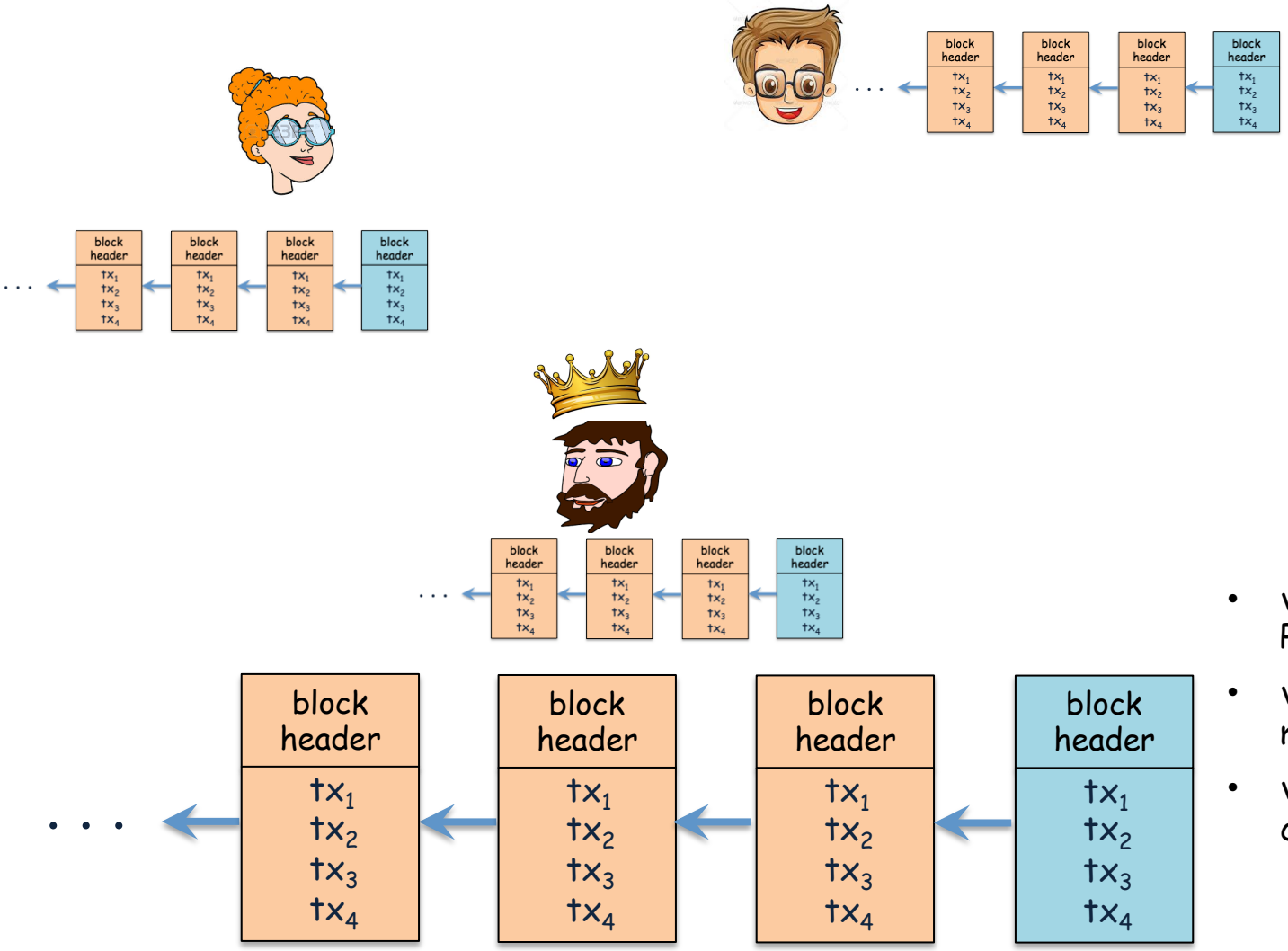




Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

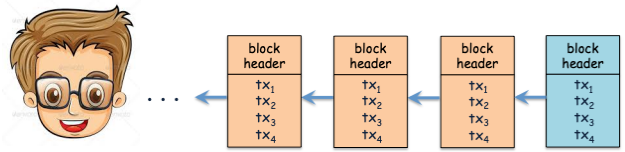


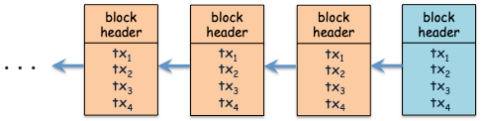
Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)



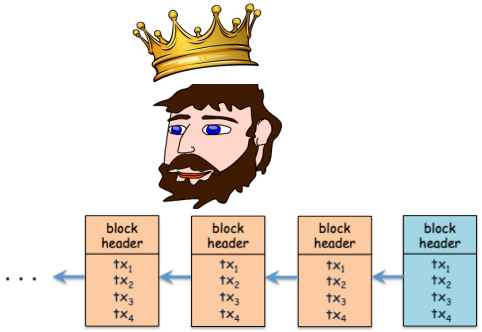
- validate the solution of PoW
- validate the signature of miner
- validate the transactions contained in the block

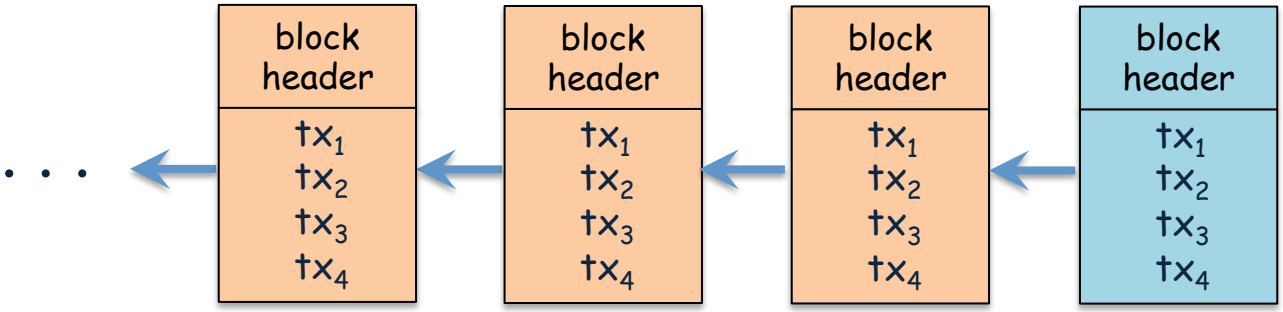
Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)





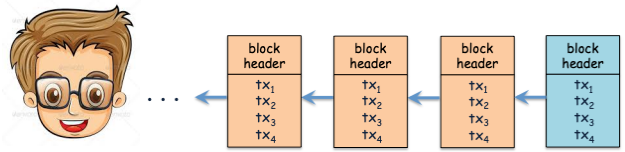
- after validating the new block, they append it to the chain without executing BFT style voting mechanism

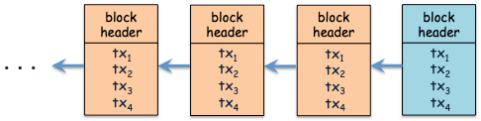




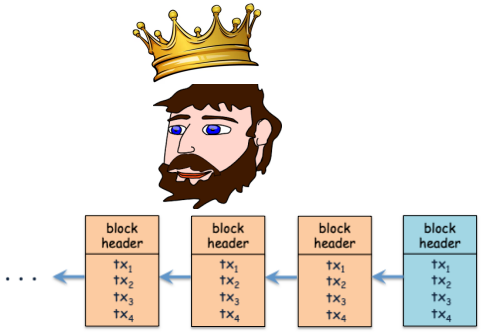
- validate the solution of PoW
- validate the signature of miner
- validate the transactions contained in the block

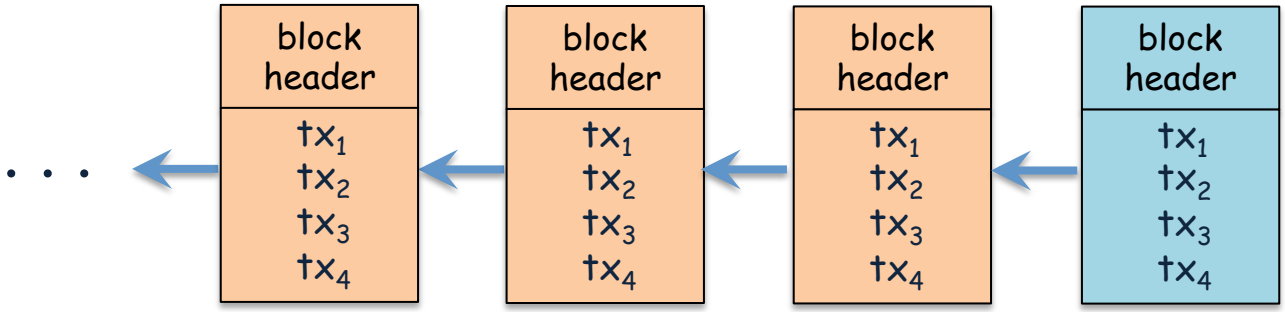
Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)





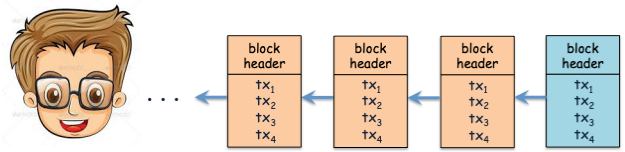
- after validating the new block, they append it to the chain without executing BFT style voting mechanism
- how the leader selected ?

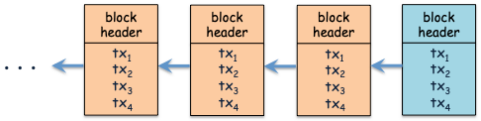




- validate the solution of PoW
- validate the signature of miner
- validate the transactions contained in the block

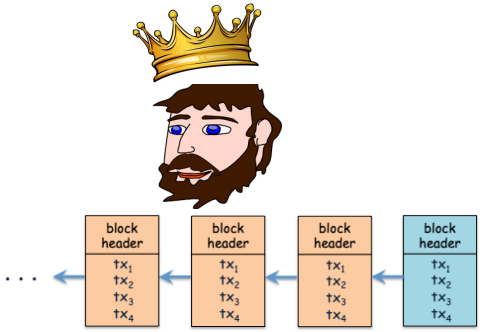
Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

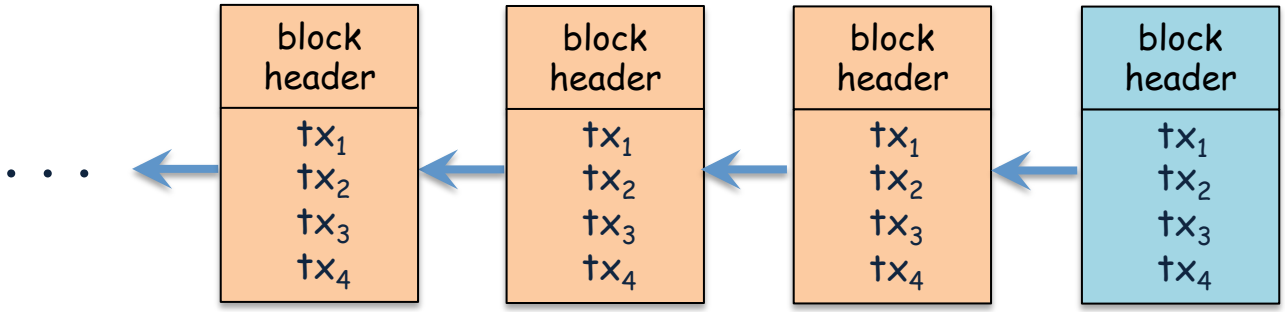




- after validating the new block, they append it to the chain without executing BFT style voting mechanism
- how the leader selected ?

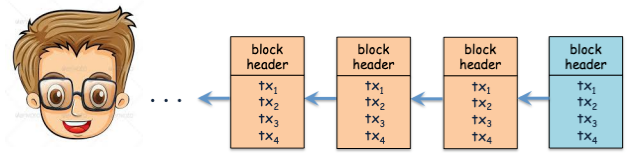
Proof-of-Work

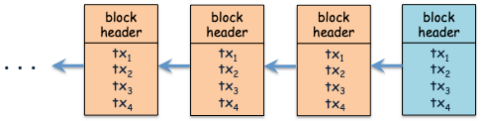


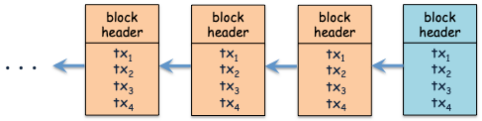


- validate the solution of PoW
- validate the signature of miner
- validate the transactions contained in the block

Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

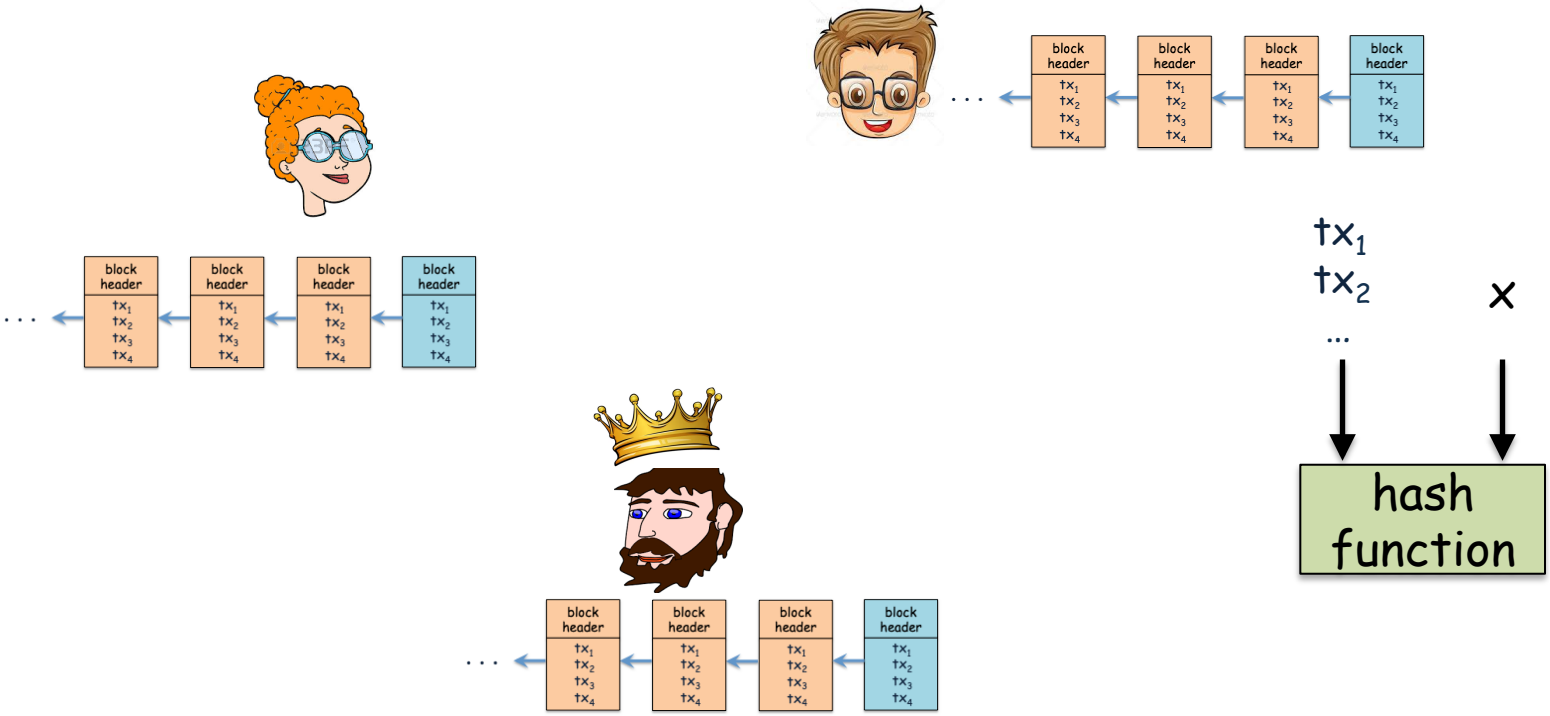




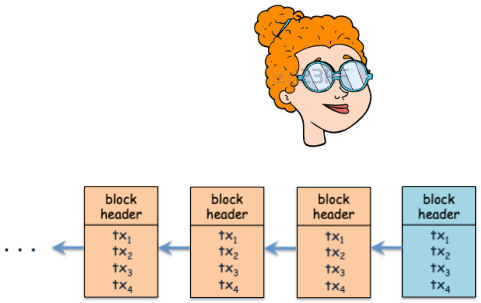


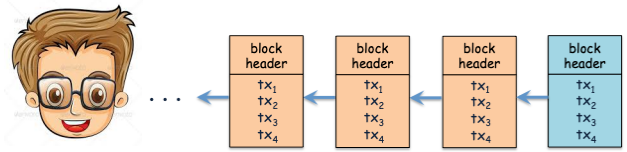
hash function

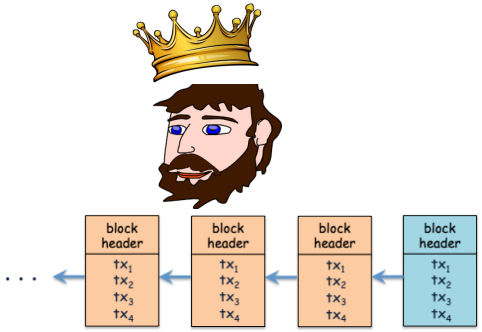
Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

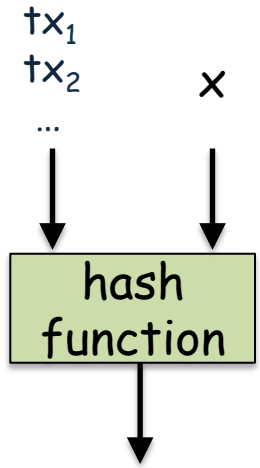


Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)



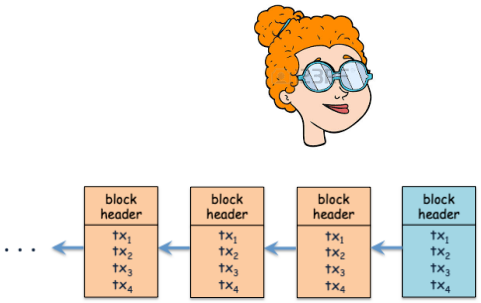


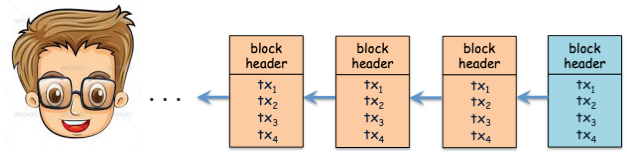


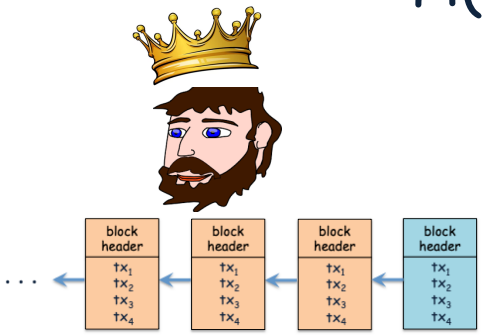


0000000000000000000001885d61a295ed
0f1daffc8a9a3e7866dcd87d34dd16e5

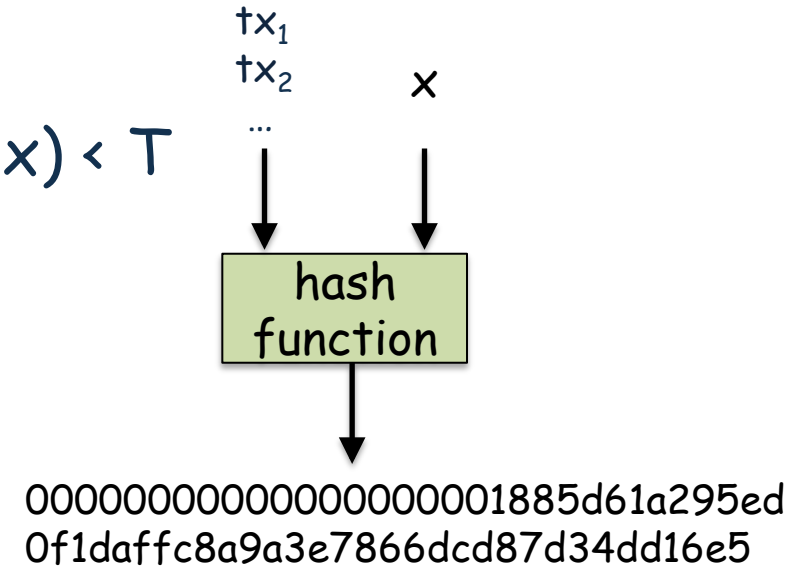
Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)



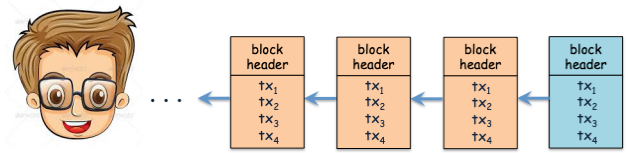


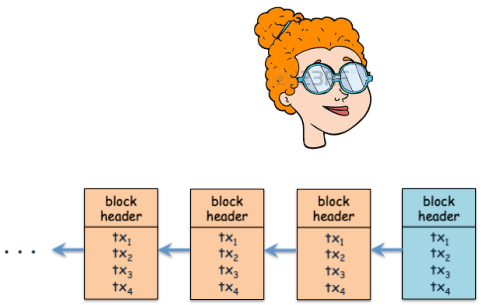


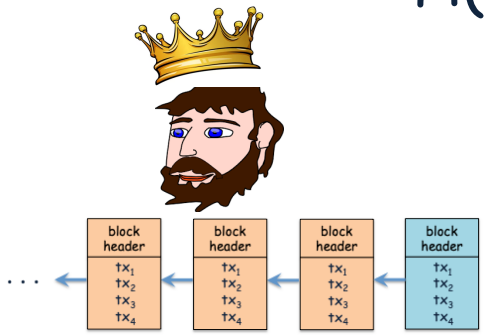
$$H(txs, x) < T$$



Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)







$$H(txs, x) < T$$

tx_1
tx_2
...

x

hash function

0000000000000000001885d61a295ed
0f1daffc8a9a3e7866dcd87d34dd16e5

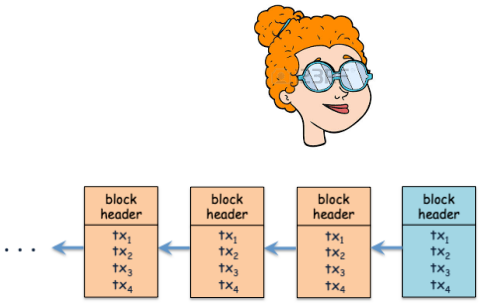
abc

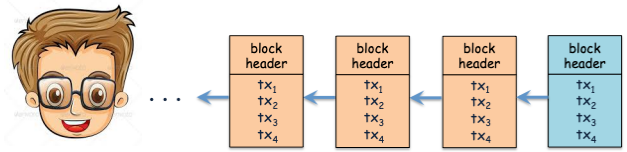
ba7816bf8f01cfea414140de5dae2223b
00361a396177a9cb410ff61f20015ad

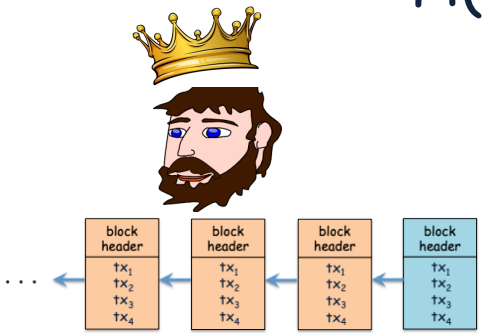
abC

0a2432a1e349d8fdb9bfca91bba9e9f28
36990fe937193d84deef26c6f3b8f76

Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)







$$H(txs, x) < T$$

tx_1
tx_2
...

x

hash function

0000000000000000001885d61a295ed
0f1daffc8a9a3e7866dcd87d34dd16e5

abc

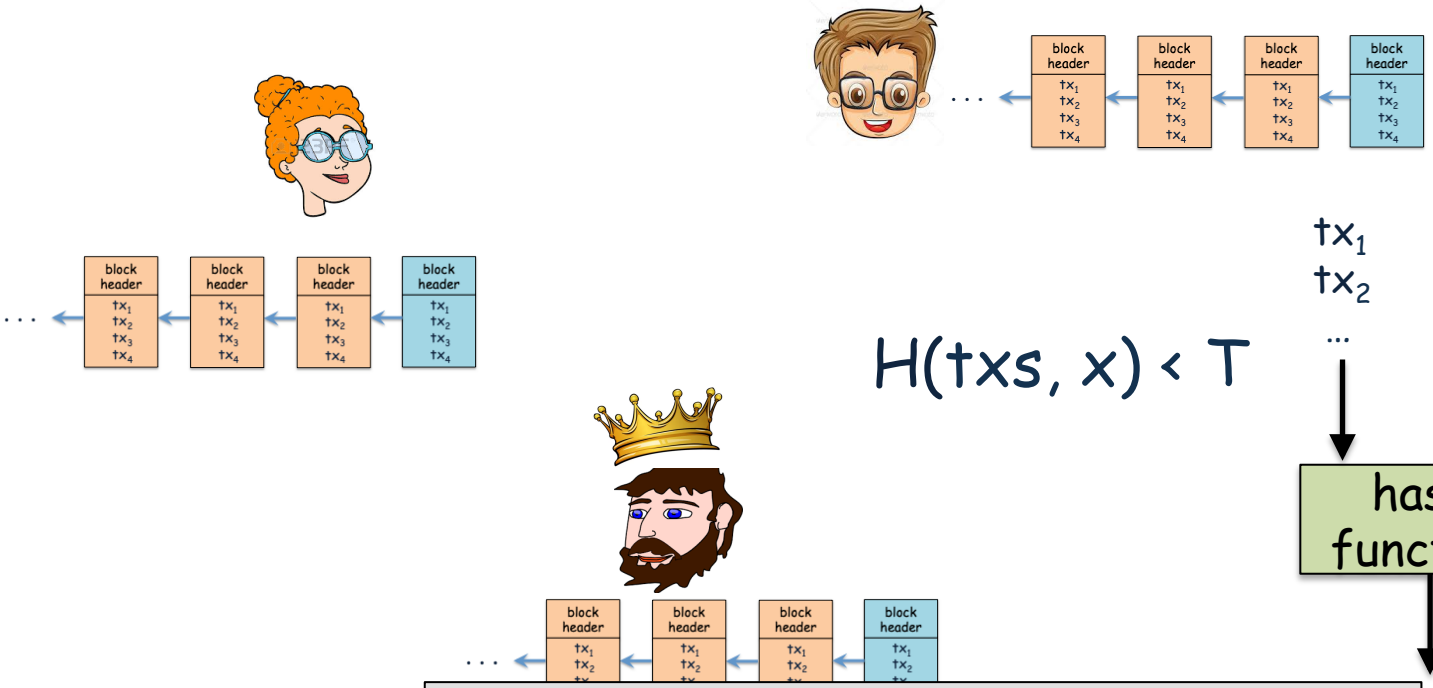
ba7816bf8f01cfea414140de5dae2223b
00361a396177a9cb410ff61f20015ad

the only way to find x is to try different nonce values till finding a solution

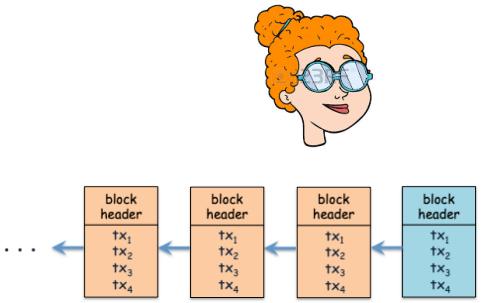
abC

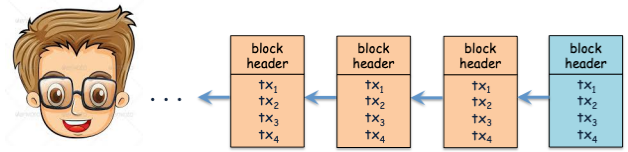
0a2432a1e349d8fdb9bfca91bba9e9f28
36990fe937193d84deef26c6f3b8f76

Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)



Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)





tx_1
tx_2
...

x

$H(txs, x) < T$

to keep the block time interval 10 m, the difficulty level T adjusted in every 2016 blocks (app. 2 weeks)

if i-th player's hash power is h_i, the probability that i-th player wins the game is $w_i/\Sigma w_j$

0000001885d61a295ed
7866dcd87d34dd16e5

abc

abC

the only way to find x is to try different nonce values till finding a solution

ba7816bf8f01cfea414140de5dae2223b
00361a396177a9cb410ff61f20015ad

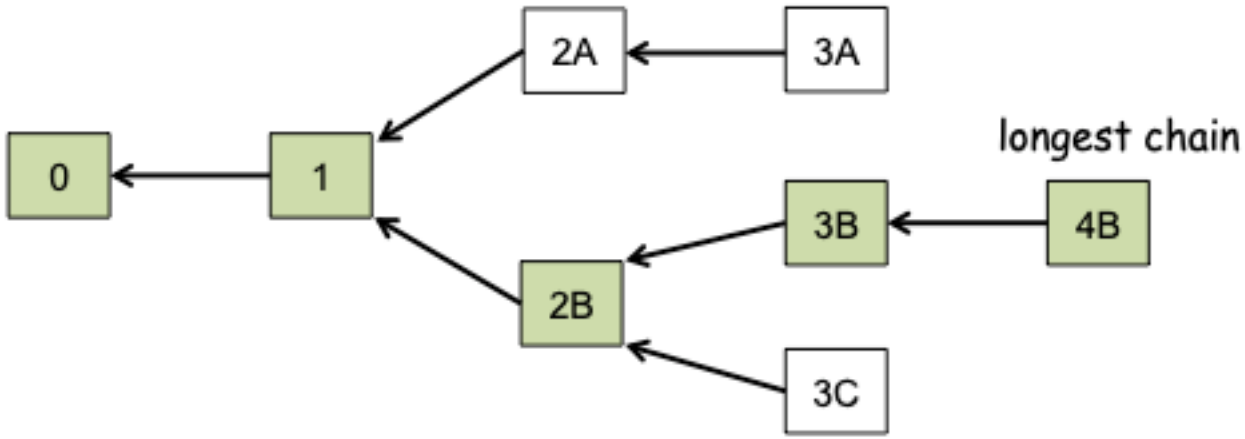
0a2432a1e349d8fdb9bfca91bba9e9f28
36990fe937193d84deef26c6f3b8f76

Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

- longest chain rule to resolve 'forking'
  (block finalization – reaching agreement on the acceptance of validated blocks - still probabilistic)

Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

- longest chain rule to resolve 'forking'
  (block finalization – reaching agreement on the acceptance of validated blocks - still probabilistic)



Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

- Garay and Kiayias [7] adapted 'safety' and 'liveness' to this setting as
  - persistence, once a tx recorded more than k blocks deep in the blockchain of one honest node, then it will be included in every honest node's chain with very high probability
  - liveness, all txs shared by honest nodes will eventually be placed more than k blocks deep in the blockchain of an honest node's chain

Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

- Garay and Kiayias [7] adapted 'safety' and 'liveness' to this setting as
  - persistence, once a tx recorded more than k blocks deep in the blockchain of one honest node, then it will be included in every honest node's chain with very high probability
  - liveness, all txs shared by honest nodes will eventually be placed more than k blocks deep in the blockchain of an honest node's chain

- they [7] that Nakamoto consensus protocol provides persistence and liveness,

  (i) if adversary controls minority of the total hashing power in the network,

  (ii) digital signature scheme unforgeable,

  (iii) network synchronizes much faster relative to PoW solution rate,

Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

- when an attacker gains the control of majority of hash power, it can use it
  - to rewrite the some part of the chain,
  - to damage the network by delaying or censoring some txs
  - to perform double-spending

Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

- when an attacker gains the control of majority of hash power, it can use it
  - to rewrite the some part of the chain,
  - to damage the network by delaying or censoring some txs
  - to perform double-spending

- Nakamoto [8] stated that the one acquiring the majority of total hash power will use it to improve its gaining instead of damaging the system

Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

- when an attacker gains the control of majority of hash power, it can use it
  - to rewrite the some part of the chain,
  - to damage the network by delaying or censoring some txs
  - to perform double-spending

- Nakamoto [8] stated that the one acquiring the majority of total hash power will use it to improve its gaining instead of damaging the system

- Bonneau [9] showed that an adversary can gain control the majority temporarily by renting others' hash power

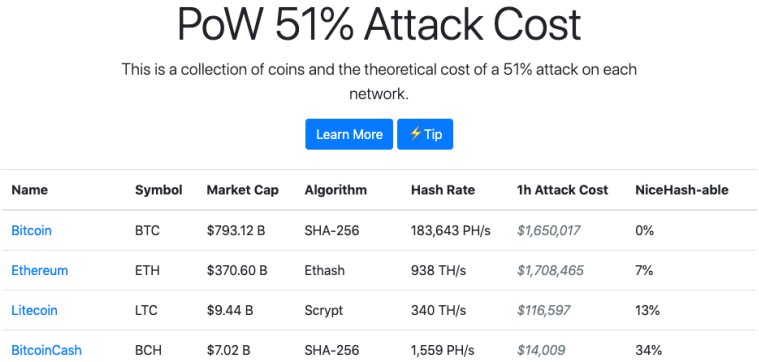
Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

- when an attacker gains the control of majority of hash power, it can use it
  - to rewrite the some part of the chain,
  - to damage the network by delaying or censoring some txs
  - to perform double-spending

- Nakamoto [8] stated that the one acquiring the majority of total hash power will use it to improve its gaining instead of damaging the system

- Bonneau [9] showed that an adversary can gain control the majority temporarily by renting others' hash power

nicehash.com



PoW 51% Attack Cost

This is a collection of coins and the theoretical cost of a 51% attack on each network.

Learn More ⚡Tip

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	$793.12 B	SHA-256	183,643 PH/s	*$1,650,017*	0%
Ethereum	ETH	$370.60 B	Ethash	938 TH/s	*$1,708,465*	7%
Litecoin	LTC	$9.44 B	Scrypt	340 TH/s	*$116,597*	13%
BitcoinCash	BCH	$7.02 B	SHA-256	1,559 PH/s	*$14,009*	34%

crypto51.app

Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

- blocks created in every 10 m, then 2000-3000 txs in average included in each block
- transactions per second (tps - throughput) for bitcoin 4-5 (maximum 7) (Visa can process more than 24k [10])
- two solutions to increase throughput: decrease the block time interval or increase the block size
  (both can cause 'forking')

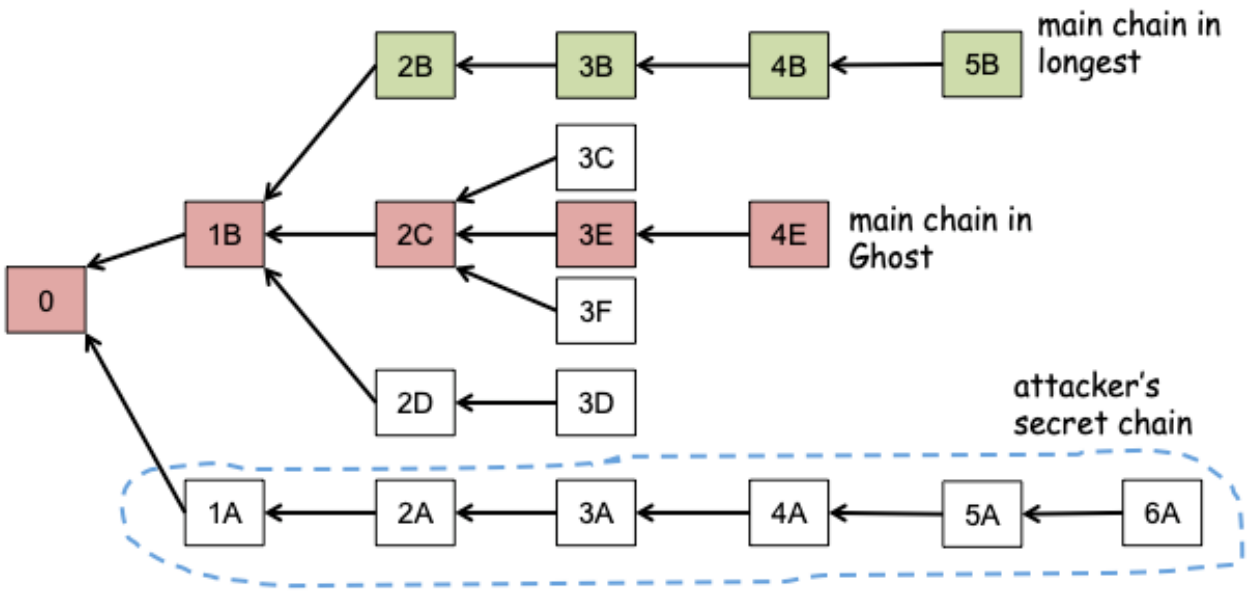
Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

- blocks created in every 10 m, then 2000-3000 txs in average included in each block
- transactions per second (tps - throughput) for bitcoin 4-5 (maximum 7) (Visa can process more than 24k [10])
- two solutions to increase throughput: decrease the block time interval or increase the block size
  (both can cause 'forking')

- Croman et al. [11] showed that when block size increased to 4MB (meaning 26-28 tps) 10% of the nodes would not be able to properly get the newly created blocks
  (it will reduce the network's effective hash power)
  - if the block size increased to 38MB (meaning 248-250 tps), it will become 50%

Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

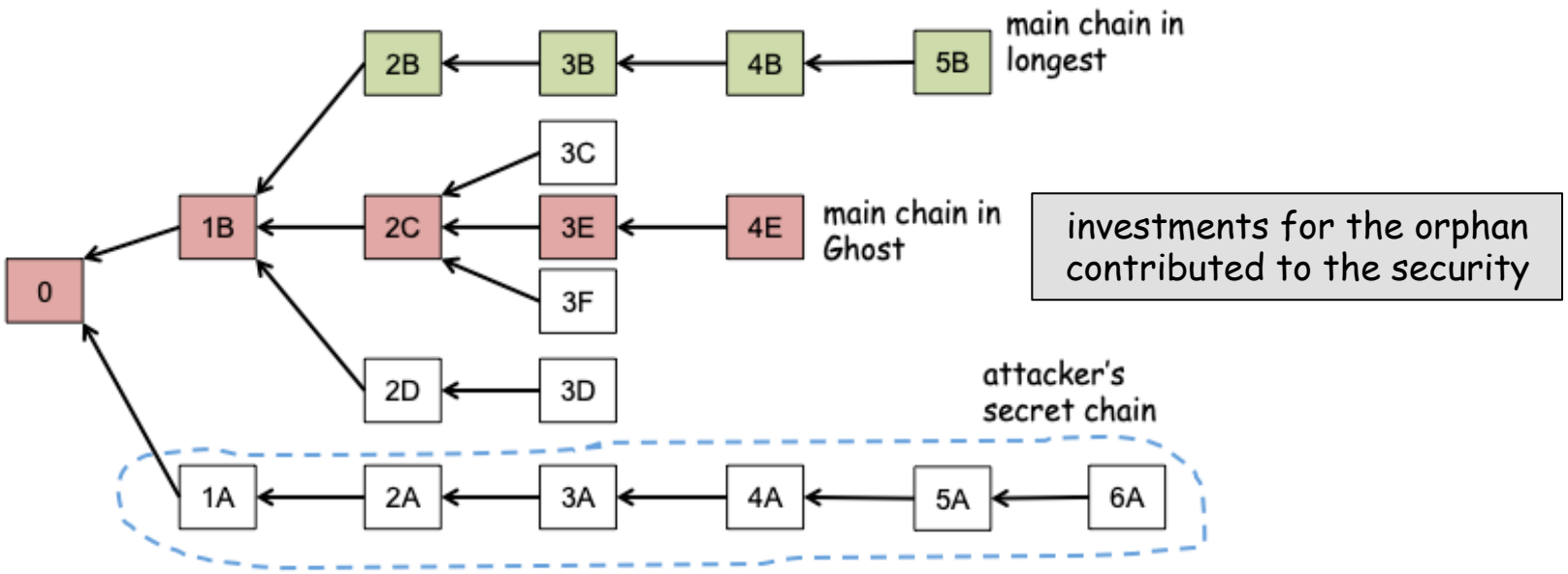
- blocks created in every 10 m, then 2000-3000 txs in average included in each block
- transactions per second (tps - throughput) for bitcoin 4-5 (maximum 7) (Visa can process more than 24k [10])
- Ghost protocol introduced by Sompolinsky and Zohar [12] in 2015



- Ghost maintains the security even if the network struggles extreme delays, and enables us to obtain larger block size and smaller block time interval

Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

- blocks created in every 10 m, then 2000-3000 txs in average included in each block
- transactions per second (tps - throughput) for bitcoin 4-5 (maximum 7) (Visa can process more than 24k [10])
- Ghost protocol introduced by Sompolinsky and Zohar [12] in 2015



- Ghost maintains the security even if the network struggles extreme delays, and enables us to obtain larger block size and smaller block time interval

Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

- a miner can earn $270k-290k when creating a valid block with bitcoin price $41k (checked in 4.3.22)
- this reward incentivizes too many people to make investments on mining

Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

- a miner can earn $270k-290k when creating a valid block with bitcoin price $41k (checked in 4.3.22)
- this reward incentivizes too many people to make investments on mining
- they buy special equipments like ASIC (≈$15k-20k) to have an advantage on mining competition

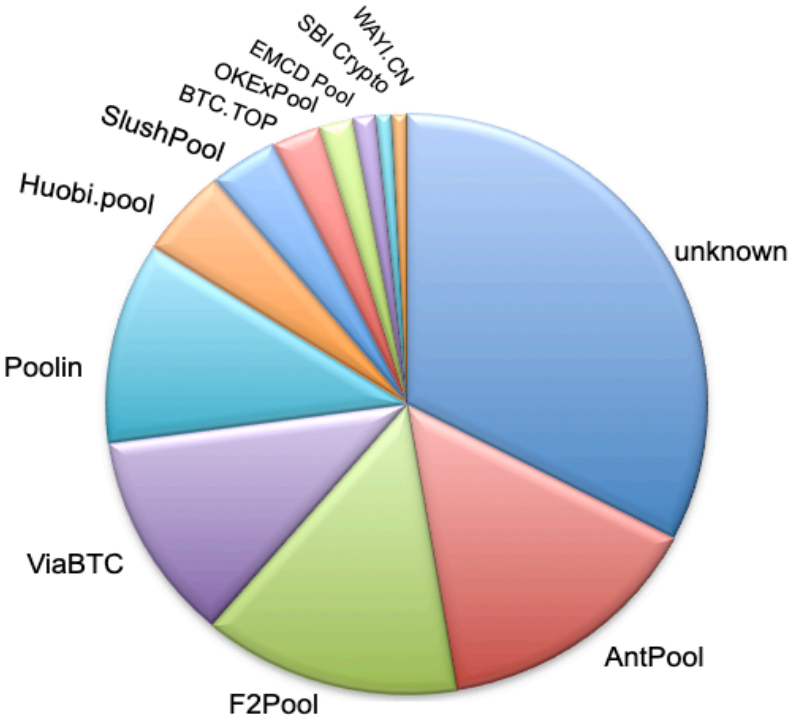
Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

- a miner can earn $270k-290k when creating a valid block with bitcoin price $41k (checked in 4.3.22)
- this reward incentivizes too many people to make investments on mining
- they buy special equipments like ASIC (≈$15k-20k) to have an advantage on mining competition

- makes it harder for small players to compete on mining
  (better to join a mining pool)

Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

- a miner can earn $270k-290k when creating a valid block with bitcoin price $41k (checked in 4.3.22)
- this reward incentivizes too many people to make investments on mining
- they buy special equipments like ASIC (≈$15k-20k) to have an advantage on mining competition



- makes it harder for small players to compete on mining
  (better to join a mining pool)

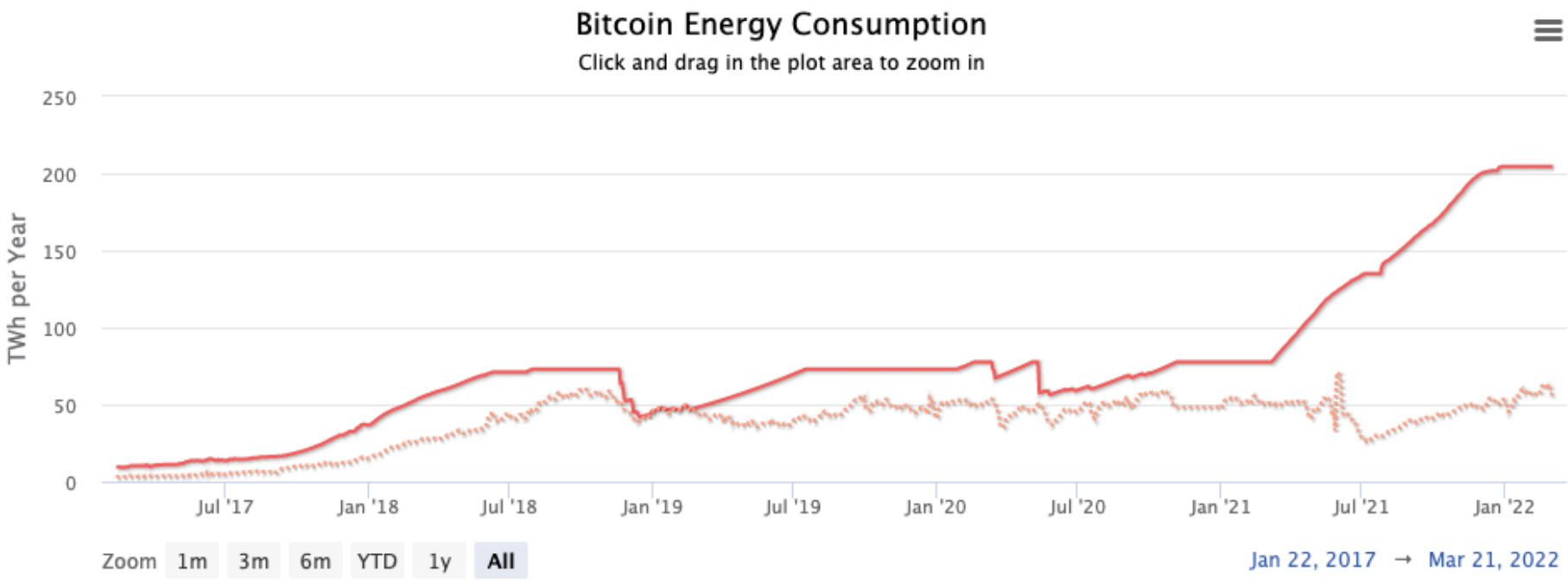
taken from
blockchain.com
in 13.06.21

Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

- Bitcoin network consumed too much electricity to generate the blocks (most of this effort wasted)

Blockchain Consensus Protocols-Nakamoto Consensus Protocol (Proof-of-Work Based)

- Bitcoin network consumed too much electricity to generate the blocks (most of this effort wasted)



taken from digiconomist.net in 13.06.21

- more than Argentina and Holland

Blockchain Consensus Protocols - Proof-of-Stake-Based

- the idea first introduced by QuantumMechanic in 2011:
  "instead of your "vote" on the accepted transaction history being weighted by the share of computing resources you bring to the network, it's weighted by the number of bitcoins you can prove you own, using your private keys"

Author | Topic: Proof of stake instead of proof of work (Read 32292 times)

QuantumMechanic
Member

Activity: 110
Merit: 19

Proof of stake instead of proof of work
July 11, 2011, 04:12:45 AM
Merited by ETFbitcoin (3), Vod (2), webtricks (2), d5000 (1), drays (1)

I've got an idea, and I'm wondering if it's been discussed/ripped apart here yet:

I'm wondering if as bitcoins become more widely distributed, whether a transition
"vote" on the accepted transaction history being weighted by the share of computi

For those that don't want to be actively verifying transactions, and so that not all p
transaction. In this way, voting power would accumulate with trusted delegates in
number of votes they've accumulated, thereby incentivising diversity of the delega

If the implementation could be done, it proved to maintain at least a similar level
compete a proof of work one due to much lower transaction fees, since its network
bandwith/storage overhead that would offset these savings by some amount which

Some other potential improvements this system could offer:

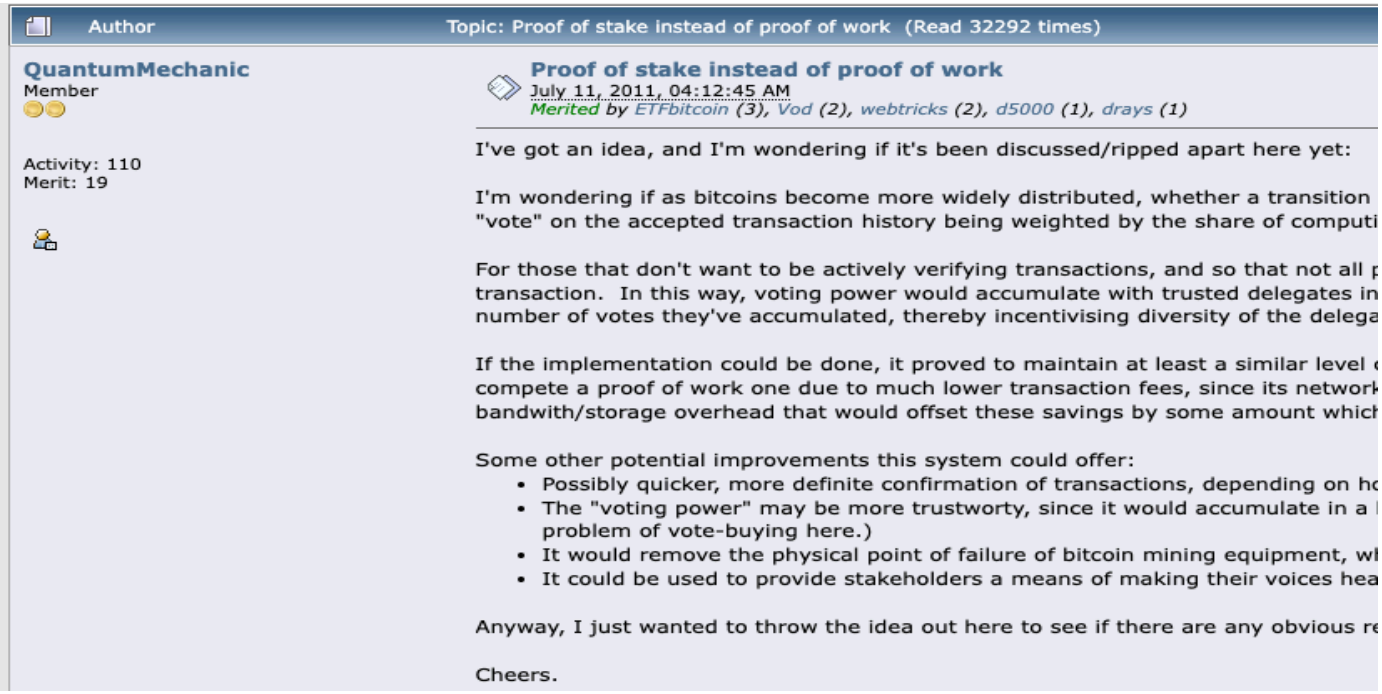
- Possibly quicker, more definite confirmation of transactions, depending on ho
- The "voting power" may be more trustworty, since it would accumulate in a
  problem of vote-buying here.)
- It would remove the physical point of failure of bitcoin mining equipment, wh
- It could be used to provide stakeholders a means of making their voices hea

Anyway, I just wanted to throw the idea out here to see if there are any obvious re

Cheers.

Blockchain Consensus Protocols - Proof-of-Stake-Based

- the idea first introduced by QuantumMechanic in 2011:
  "instead of your "vote" on the accepted transaction history being weighted by the share of computing resources you bring to the network, it's weighted by the number of bitcoins you can prove you own, using your private keys"



Author | Topic: Proof of stake instead of proof of work (Read 32292 times)

QuantumMechanic
Member

Activity: 110
Merit: 19

Proof of stake instead of proof of work
July 11, 2011, 04:12:45 AM
Merited by ETFbitcoin (3), Vod (2), webtricks (2), d5000 (1), drays (1)

I've got an idea, and I'm wondering if it's been discussed/ripped apart here yet:

I'm wondering if as bitcoins become more widely distributed, whether a transition
"vote" on the accepted transaction history being weighted by the share of computi

For those that don't want to be actively verifying transactions, and so that not all p
transaction. In this way, voting power would accumulate with trusted delegates in
number of votes they've accumulated, thereby incentivising diversity of the delega

If the implementation could be done, it proved to maintain at least a similar level
compete a proof of work one due to much lower transaction fees, since its network
bandwith/storage overhead that would offset these savings by some amount which

Some other potential improvements this system could offer:
- Possibly quicker, more definite confirmation of transactions, depending on ho
- The "voting power" may be more trustworty, since it would accumulate in a
  problem of vote-buying here.)
- It would remove the physical point of failure of bitcoin mining equipment, wl
- It could be used to provide stakeholders a means of making their voices hea

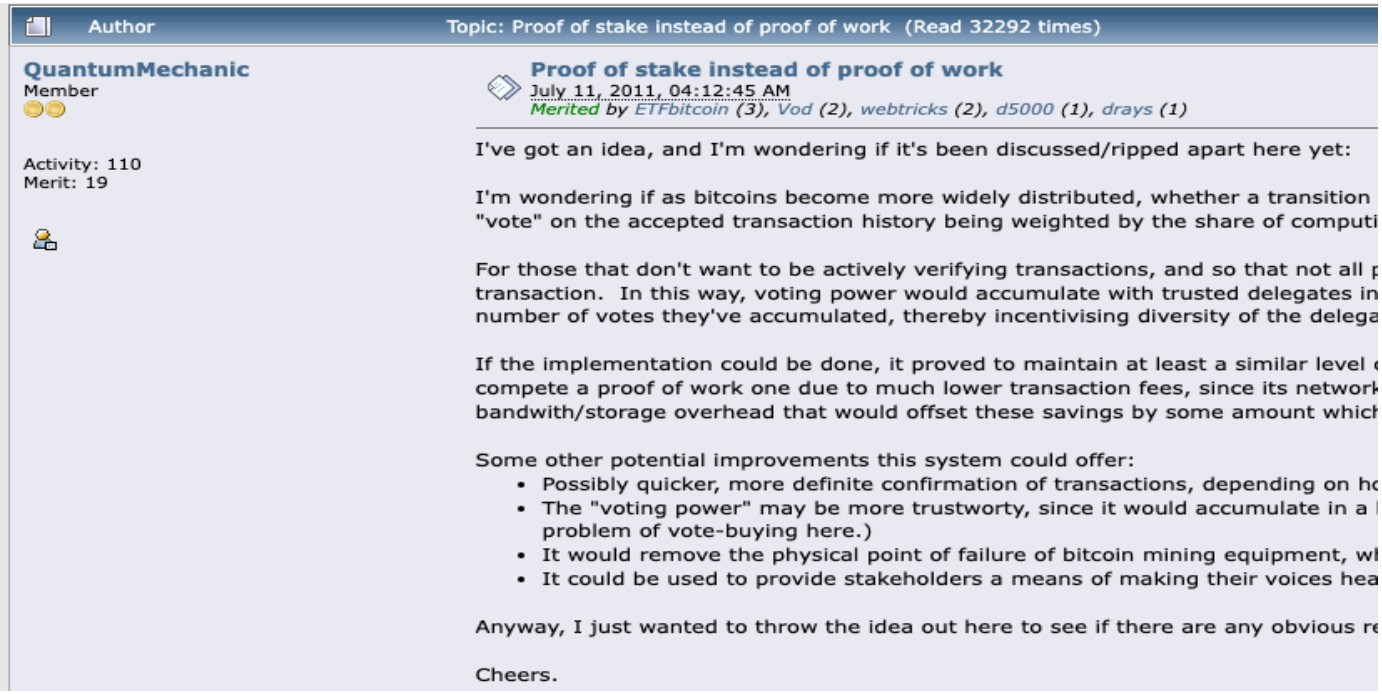
Anyway, I just wanted to throw the idea out here to see if there are any obvious re

Cheers.

- the parties who hold the stake in the system are well-suited to maintain the ledger since their stake will diminish in value when the security of the system collapses

Blockchain Consensus Protocols - Proof-of-Stake-Based

- the idea first introduced by QuantumMechanic in 2011:
  "instead of your "vote" on the accepted transaction history being weighted by the share of computing resources you bring to the network, it's weighted by the number of bitcoins you can prove you own, using your private keys"



Author | Topic: Proof of stake instead of proof of work (Read 32292 times)

QuantumMechanic
Member

Activity: 110
Merit: 19

Proof of stake instead of proof of work
July 11, 2011, 04:12:45 AM
Merited by ETFbitcoin (3), Vod (2), webtricks (2), d5000 (1), drays (1)

I've got an idea, and I'm wondering if it's been discussed/ripped apart here yet:

I'm wondering if as bitcoins become more widely distributed, whether a transition
"vote" on the accepted transaction history being weighted by the share of computi

For those that don't want to be actively verifying transactions, and so that not all p
transaction. In this way, voting power would accumulate with trusted delegates in
number of votes they've accumulated, thereby incentivising diversity of the delega

If the implementation could be done, it proved to maintain at least a similar level
compete a proof of work one due to much lower transaction fees, since its network
bandwith/storage overhead that would offset these savings by some amount which

Some other potential improvements this system could offer:
- Possibly quicker, more definite confirmation of transactions, depending on ho
- The "voting power" may be more trustworty, since it would accumulate in a
  problem of vote-buying here.)
- It would remove the physical point of failure of bitcoin mining equipment, wl
- It could be used to provide stakeholders a means of making their voices hea

Anyway, I just wanted to throw the idea out here to see if there are any obvious re

Cheers.

- the parties who hold the stake in the system are well-suited to maintain the ledger since their stake will diminish in value when the security of the system collapses
- a party who possesses p fraction of the total amount of coins in circulation will be the leader with the probability p

Chain of Activity

- introduced by Bentov et al. [13] in 2016
- a pure Proof of Stake protocol that aims to prevent the rational forks by which the only a single stakeholder identity can create the next block

Chain of Activity

- introduced by Bentov et al. [13] in 2016
- a pure Proof of Stake protocol that aims to prevent the rational forks by which the only a single stakeholder identity can create the next block
- there are two difficulties associated with pure Proof of Stake system:
  - fair initial distribution of the money supply to the parties
  - network fragility if the nodes are rational

Blockchain Consensus Protocols - Proof-of-Stake-Based

Chain of Activity

- time is divided into sequence of segments, called epoch
- each epoch is divided into L discrete unites, called slot
- each slot is associated with a single block that is generated by a single stakeholder
- the identity of this stakeholder is fixed and publicly known

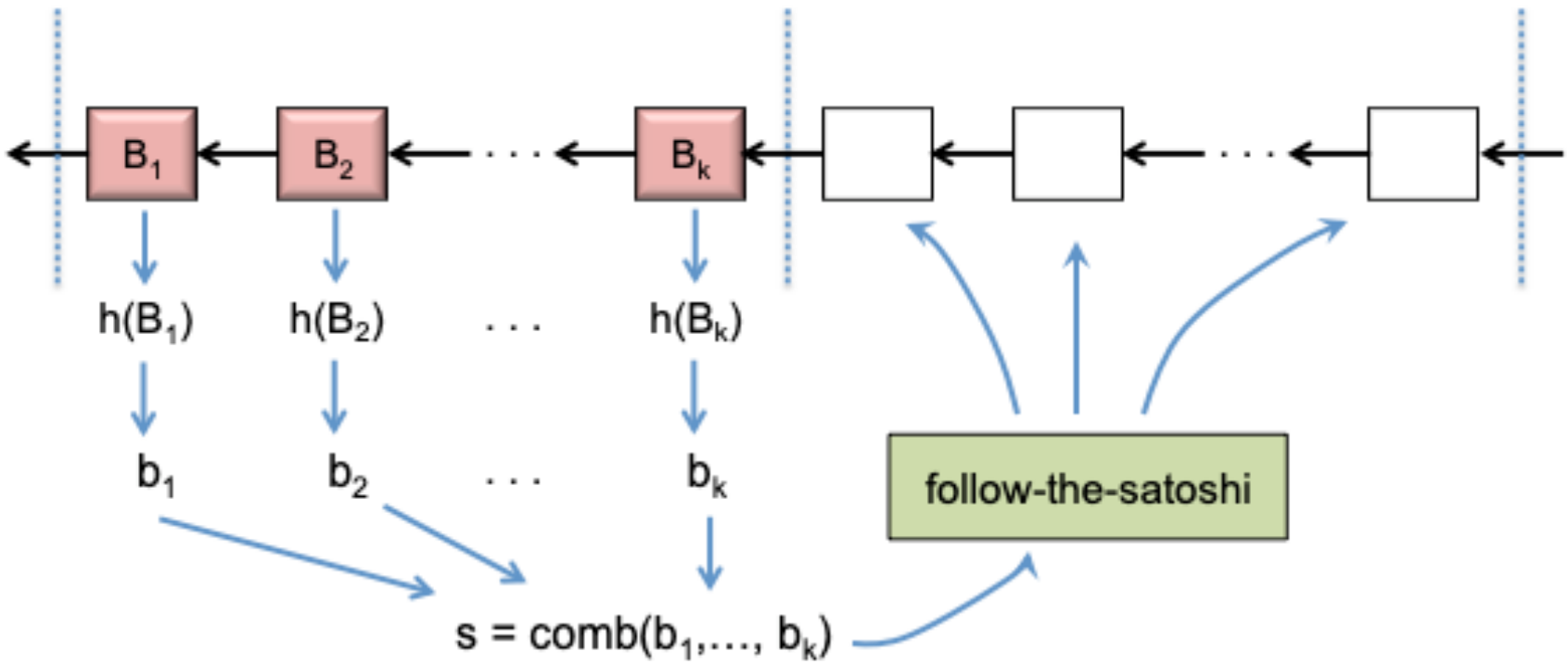
Blockchain Consensus Protocols - Proof-of-Stake-Based

Chain of Activity

- time is divided into sequence of segments, called epoch
- each epoch is divided into L discrete unites, called slot
- each slot is associated with a single block that is generated by a single stakeholder
- the identity of this stakeholder is fixed and publicly known
- the leaders of the current epoch will form a seed as SL = comb(b1,…,bL) where bi = Hash(Bi)
- the seed is then used to derive the identities of the next L stakeholders via 'follow-the-satoshi'

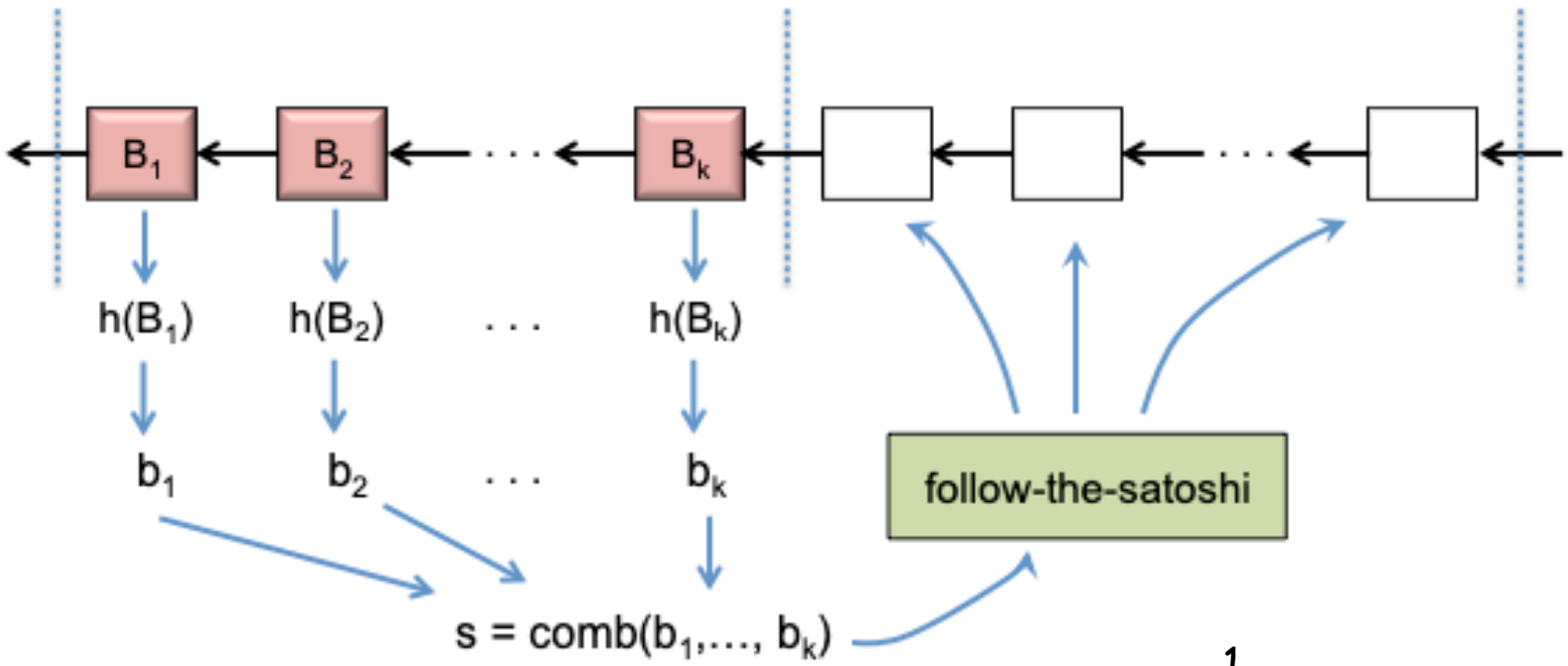
Blockchain Consensus Protocols - Proof-of-Stake-Based

Chain of Activity



Blockchain Consensus Protocols - Proof-of-Stake-Based

Chain of Activity

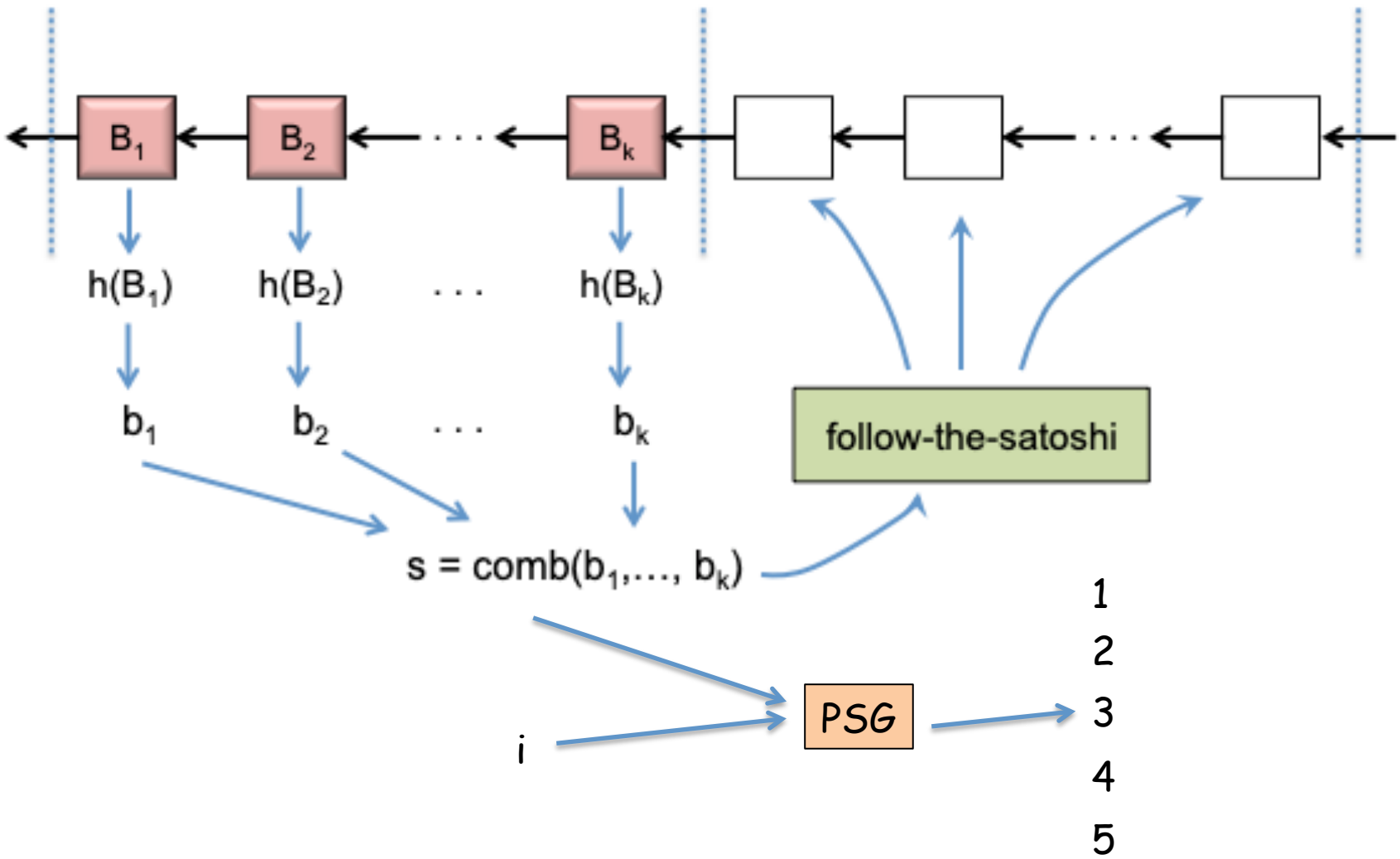


PSG

1
2
3
4
5

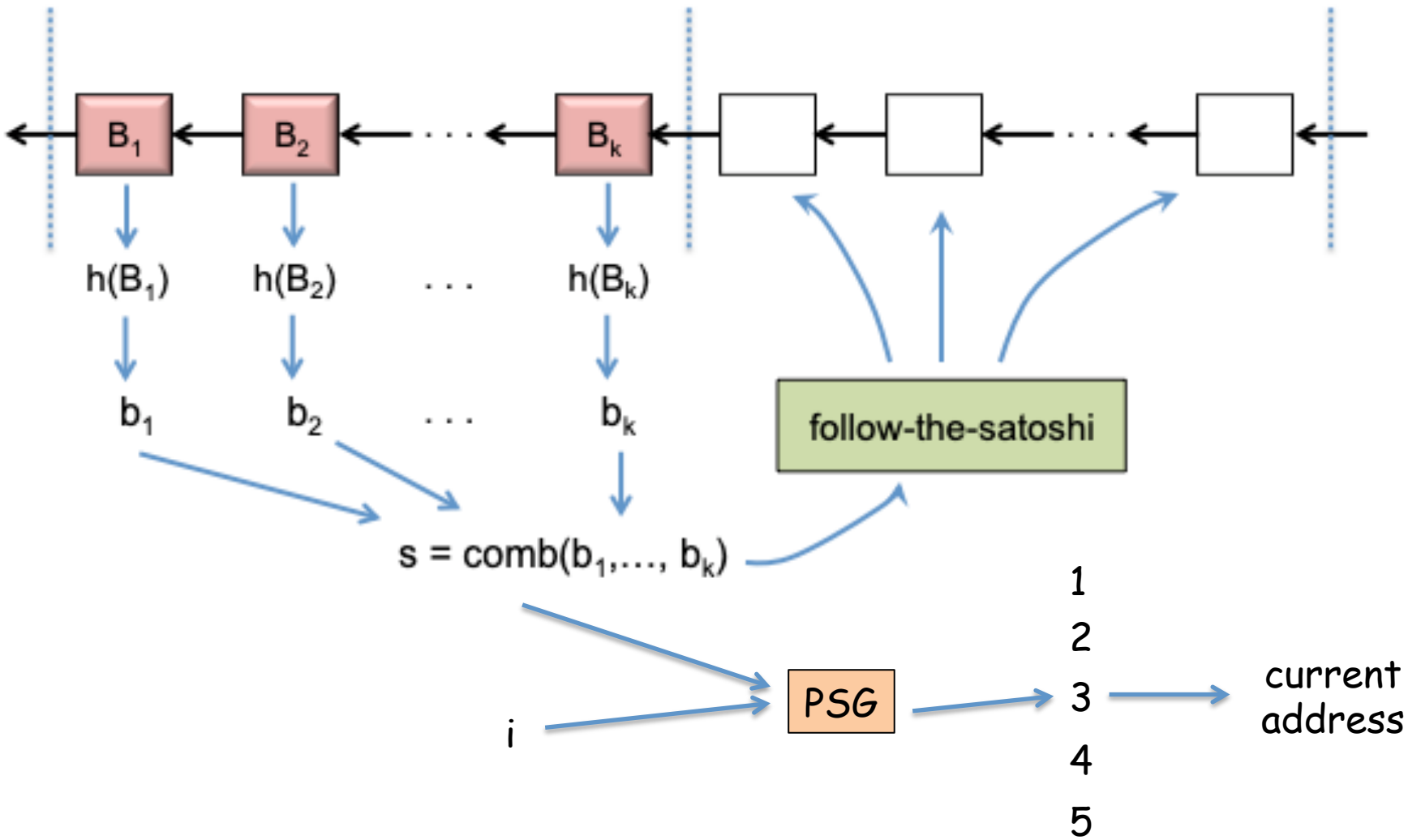
Blockchain Consensus Protocols - Proof-of-Stake-Based

Chain of Activity



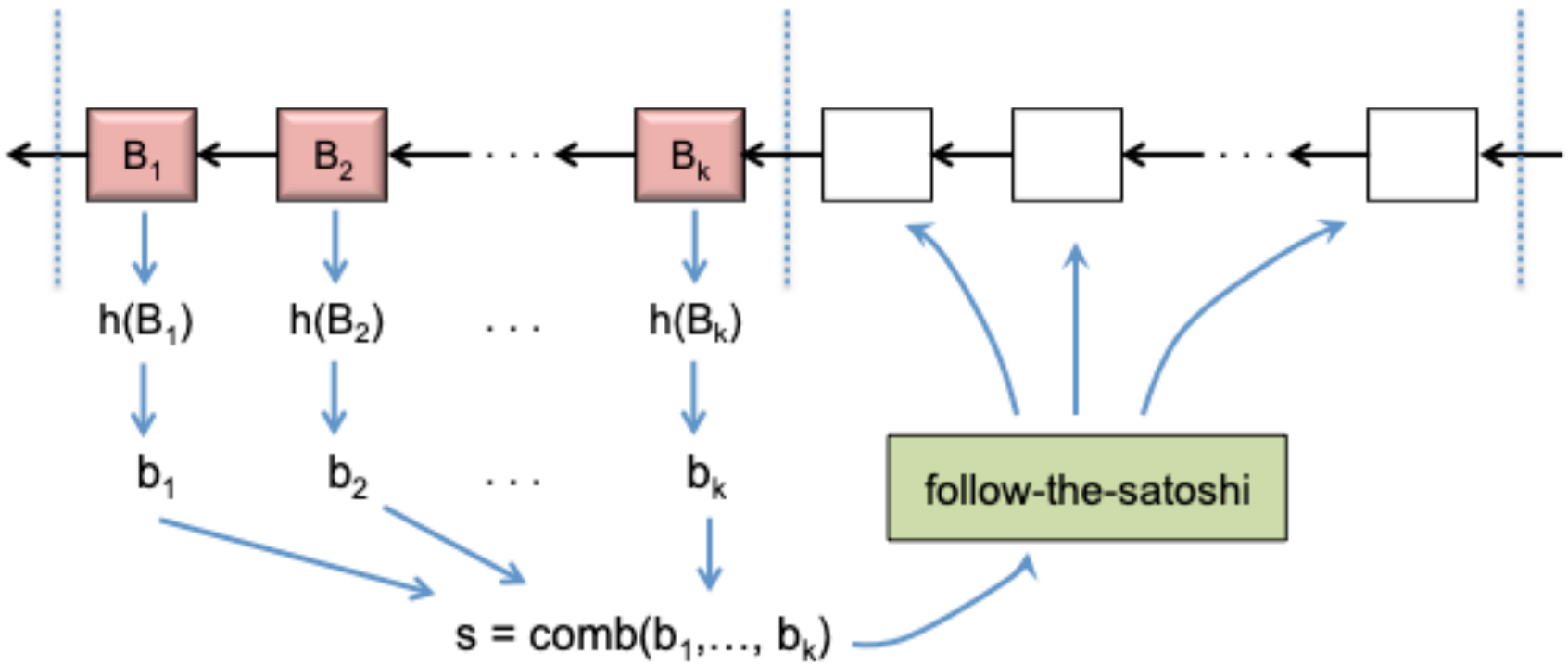
Blockchain Consensus Protocols - Proof-of-Stake-Based

Chain of Activity



Blockchain Consensus Protocols - Proof-of-Stake-Based

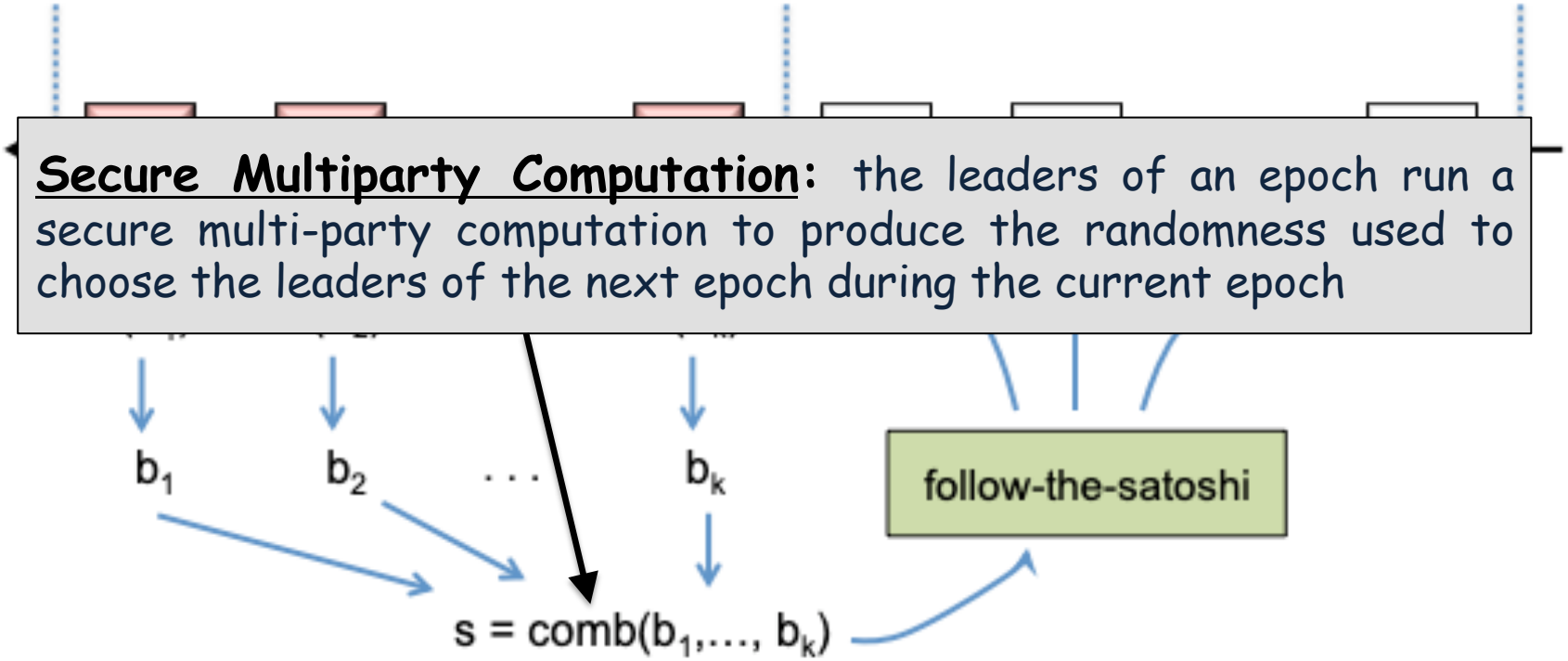
Ouroboros



- introduced by Aggelos et al. [14] as the first blockchain protocol based on PoS with rigorous security guarantees
- a fundamental problem for PoS is to simulate the leader election process.
- an adversary controlling a set of stakeholders may attempt to simulate the protocol execution trying different sequence of stakeholders participants so that it finds a protocol continuation that favors him

Blockchain Consensus Protocols - Proof-of-Stake-Based

Ouroboros



- introduced by Aggelos et al. [14] as the first blockchain protocol based on PoS with rigorous security guarantees
- a fundamental problem for PoS is to simulate the leader election process.
- an adversary controlling a set of stakeholders may attempt to simulate the protocol execution trying different sequence of stakeholders participants so that it finds a protocol continuation that favors him

Blockchain Consensus Protocols - Proof-of-Stake-Based

Delegated PoS

- nodes must be online to issue the blocks when they chosen as slot leaders
- being online will be unattractive for the nodes having small stake
- they need to be online to contribute the election of slot leaders for the next epoch

Delegated PoS

- nodes must be online to issue the blocks when they chosen as slot leaders
- being online will be unattractive for the nodes having small stake
- they need to be online to contribute the election of slot leaders for the next epoch
- Delegated PoS enables nodes to delegate their stake to others to represent them in the protocol
- thus, they can contribute their stake to the security of the system without being online

Blockchain Consensus Protocols – Proof-of-Stake-Based

Delegated PoS

- different than Cardano, in general, at the beginning of each epoch, top K delegates according to the votes they obtain determined and assigned to the time slots in the epoch
- Tron – 27, Lisk – 103, Bitshare – > 1% of total stake
- Cardano - 21600
- PoS-based consensus protocols incentivize nodes to create blocks by giving fees or producing some coin at inflation rate

Blockchain Consensus Protocols – Proof-of-Stake-Based

- Aggelos et al. [14] showed that Ourobors consensus protocol provides persistence and liveness,

  (i) if adversary controls minority of the total stake in the network,

  (ii) digital signature scheme unforgeable,

  (iii) network is synchronous

  (iv) nodes do not remain offline for long periods of time

Blockchain Consensus Protocols – Proof-of-Stake-Based

- Aggelos et al. [14] showed that Ourobors consensus protocol provides persistence and liveness,

  (i) if adversary controls minority of the total stake in the network,

  (ii) digital signature scheme unforgeable,

  (iii) network is synchronous

  (iv) nodes do not remain offline for long periods of time

- lack of formal security proof for most of the protocols (especially for DPoS-based)

Blockchain Consensus Protocols - Proof-of-Stake-Based

- Aggelos et al. [14] showed that Ourobors consensus protocol provides persistence and liveness,

  (i) if adversary controls minority of the total stake in the network,

  (ii) digital signature scheme unforgeable,

  (iii) network is synchronous

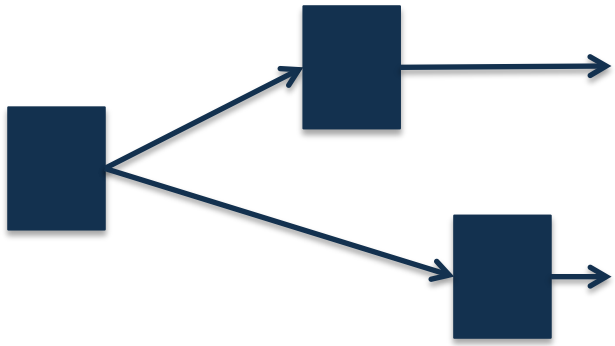
  (iv) nodes do not remain offline for long periods of time

- lack of formal security proof for most of the protocols (especially for DPoS-based)

- when an attacker gains the control of majority of total stake, it can use it
  - to rewrite the some part of the chain,
  - to damage the network by delaying or censoring some txs
  - to perform double-spending

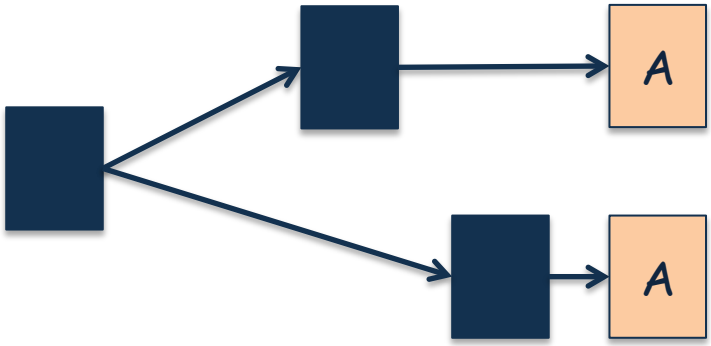
- similar to Nakamoto statement for PoW, the one acquiring the majority of total stake will use it to improve its gaining not to damage its investments

Blockchain Consensus Protocols - Proof-of-Stake-Based



- multiple blockchains can coexist since they don't run the protocol in a coordinated way

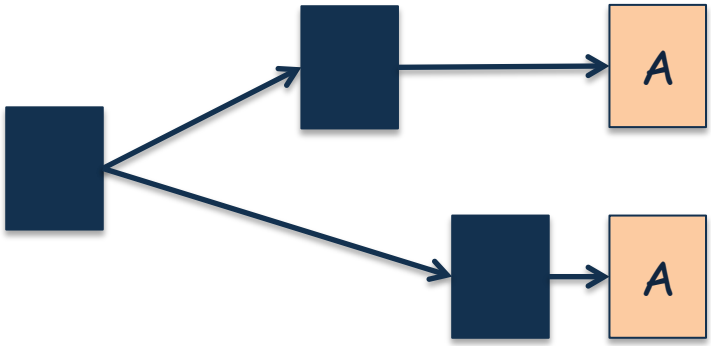
Blockchain Consensus Protocols - Proof-of-Stake-Based



- multiple blockchains can coexist since they don't run the protocol in a coordinated way

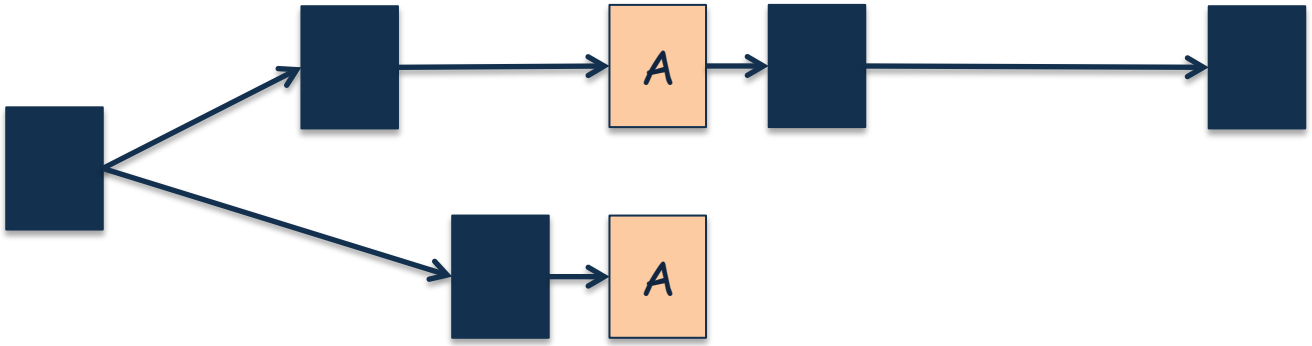
- the adv by being elected to issue the next block, capable of adding the new block to more than one chain (nothing-at-stake)

Blockchain Consensus Protocols - Proof-of-Stake-Based



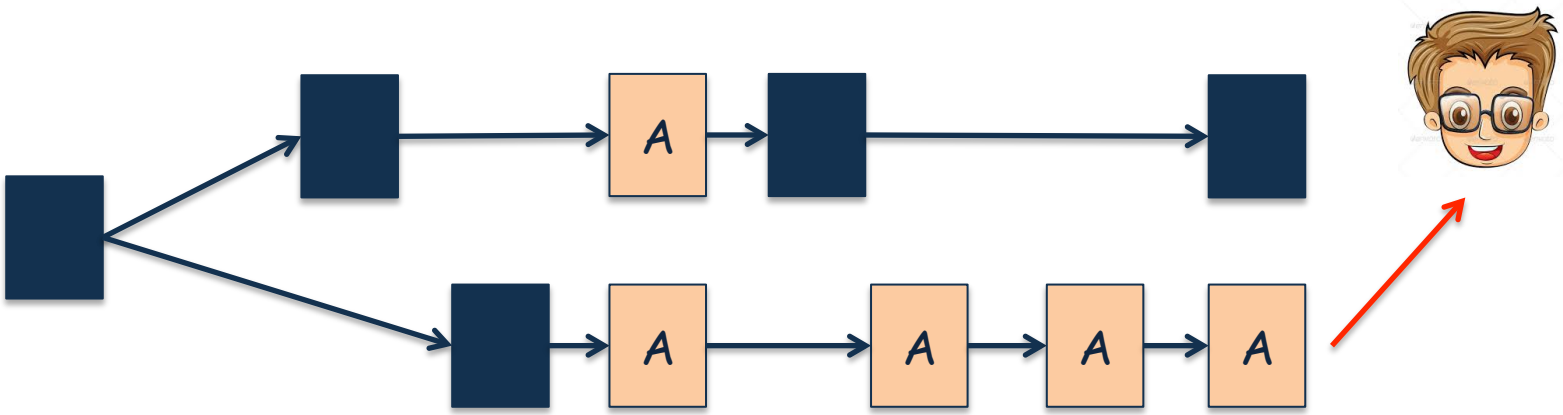
- multiple blockchains can coexist since they don't run the protocol in a coordinated way
- the adv by being elected to issue the next block, capable of adding the new block to more than one chain (nothing-at-stake)
- so the security argument for PoW cannot be applied here

Blockchain Consensus Protocols - Proof-of-Stake-Based



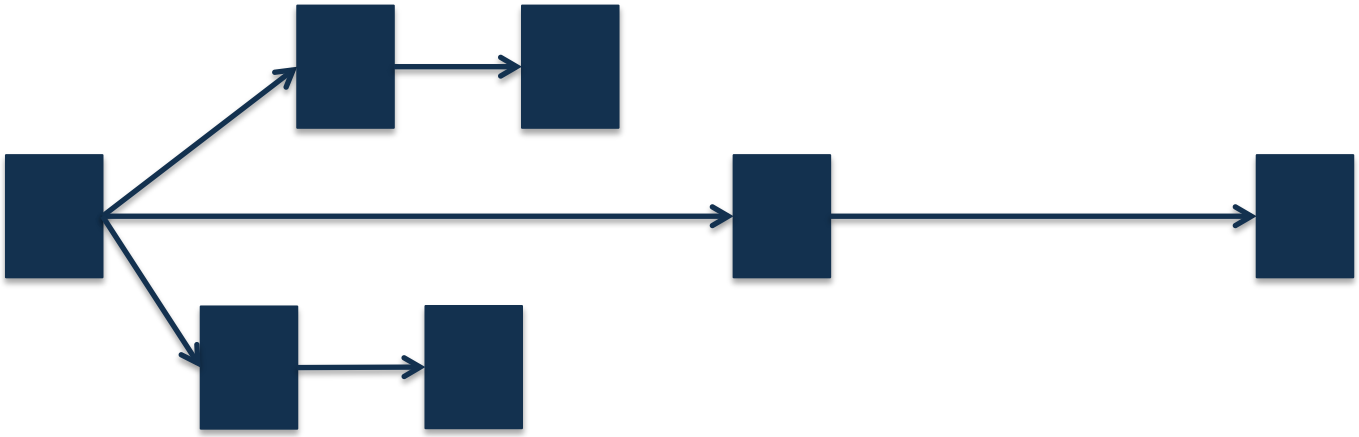
- multiple blockchains can coexist since they don't run the protocol in a coordinated way
- the adv by being elected to issue the next block, capable of adding the new block to more than one chain (nothing-at-stake)
- so the security argument for PoW cannot be applied here

Blockchain Consensus Protocols - Proof-of-Stake-Based



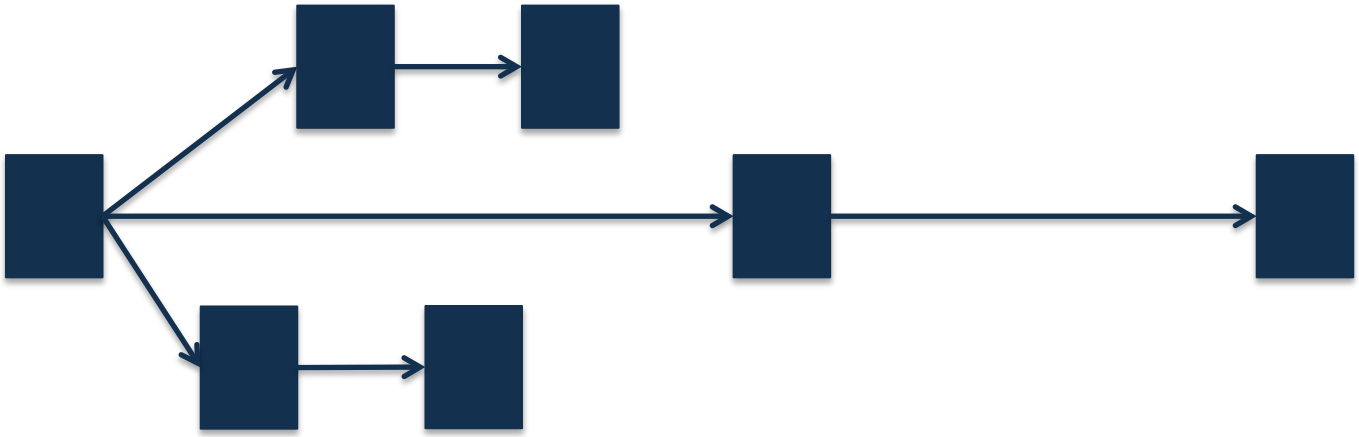
- multiple blockchains can coexist since they don't run the protocol in a coordinated way
- the adv by being elected to issue the next block, capable of adding the new block to more than one chain (nothing-at-stake)
- so the security argument for PoW cannot be applied here

Blockchain Consensus Protocols - Proof-of-Stake-Based



- multiple blockchains can coexist since they don't run the protocol in a coordinated way
- the adv by being elected to issue the next block, capable of adding the new block to more than one chain (nothing-at-stake)
- so the security argument for PoW cannot be applied here
- what we want the protocol execution has a single long chain, and any other disjoint chains are too short for the adv to be able to reach the longest one
- so, the honest part adopts the longest one easily

Blockchain Consensus Protocols - Proof-of-Stake-Based



- multiple blockchains can coexist since they don't run the protocol in a coordinated way
- the adv by being elected to issue the next block, capable of adding the new block to more than one chain (nothing-at-stake)
- so the security argument for PoW cannot be applied here
- what we want the protocol execution has a single long chain, and any other disjoint chains are too short for the adv to be able to reach the longest one
- so, the honest part adopts the longest one easily
- Ouroboros proved that this happens almost all the time.

Blockchain Consensus Protocols - Proof-of-Stake-Based

- rich gets richer !

Blockchain Consensus Protocols - Proof-of-Stake-Based

- rich gets richer !
- initial coin distribution ? (73 people for Nxt)

Blockchain Consensus Protocols - Proof-of-Stake-Based

- rich gets richer !
- initial coin distribution ? (73 people for Nxt)
- for committee-based PoS, the leaders who issue the blocks determined and shared before each epoch
  - they become targets for some attacks
  - Kerber et al. [15] proposed a protocol that hides the indentities of the slot leaders of the next epoch

Lottery-Based Protocols

protocol	leader selection	incentivization	fault tolerance	throughput	disadvantage
Bitcoin	PoW	fresh coin + fee	minority of total hash power	7 tps	electricity consumption
Ghost	PoW	fresh coin + fee	minority of total hash power	15 tps	electricity consumption
CoA	PoS	fee	minority of total stake	?	ICD
Ouroboros	PoS	fee	minority of total stake	257 tps	ICD
Tron	DPoS	fee + inflation rate	minority of total stake	2000 tps	ICD