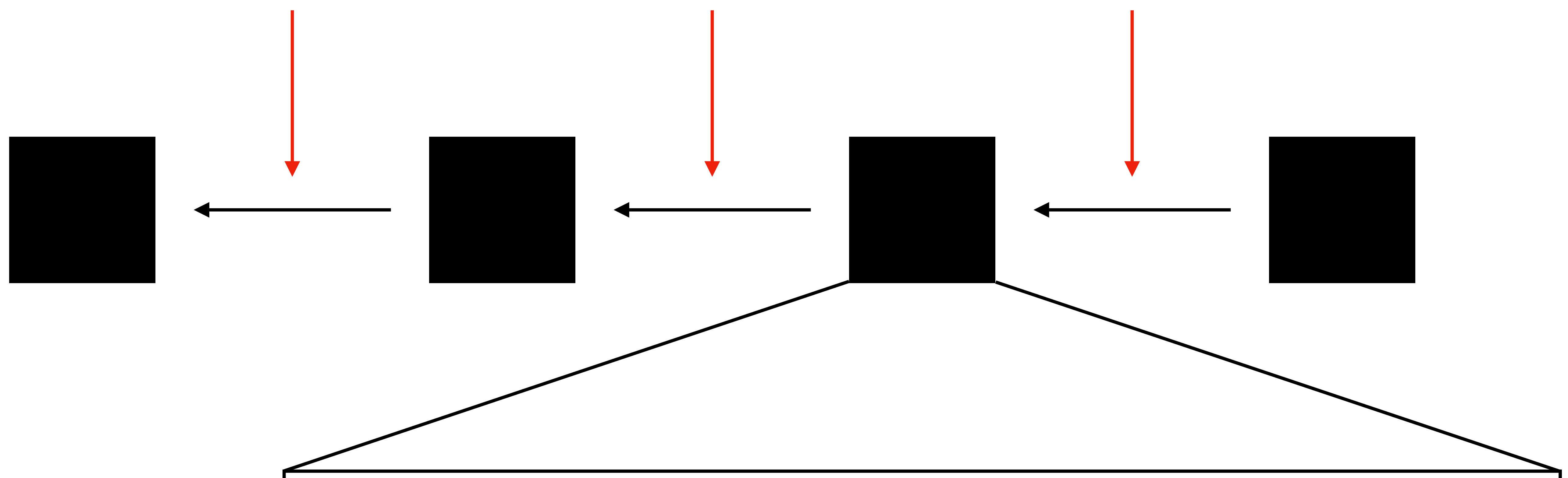
Cryptographic Sortition for Proof of Stake in Bazo

— by Roman Blum

Chained Blocks = Blockchain



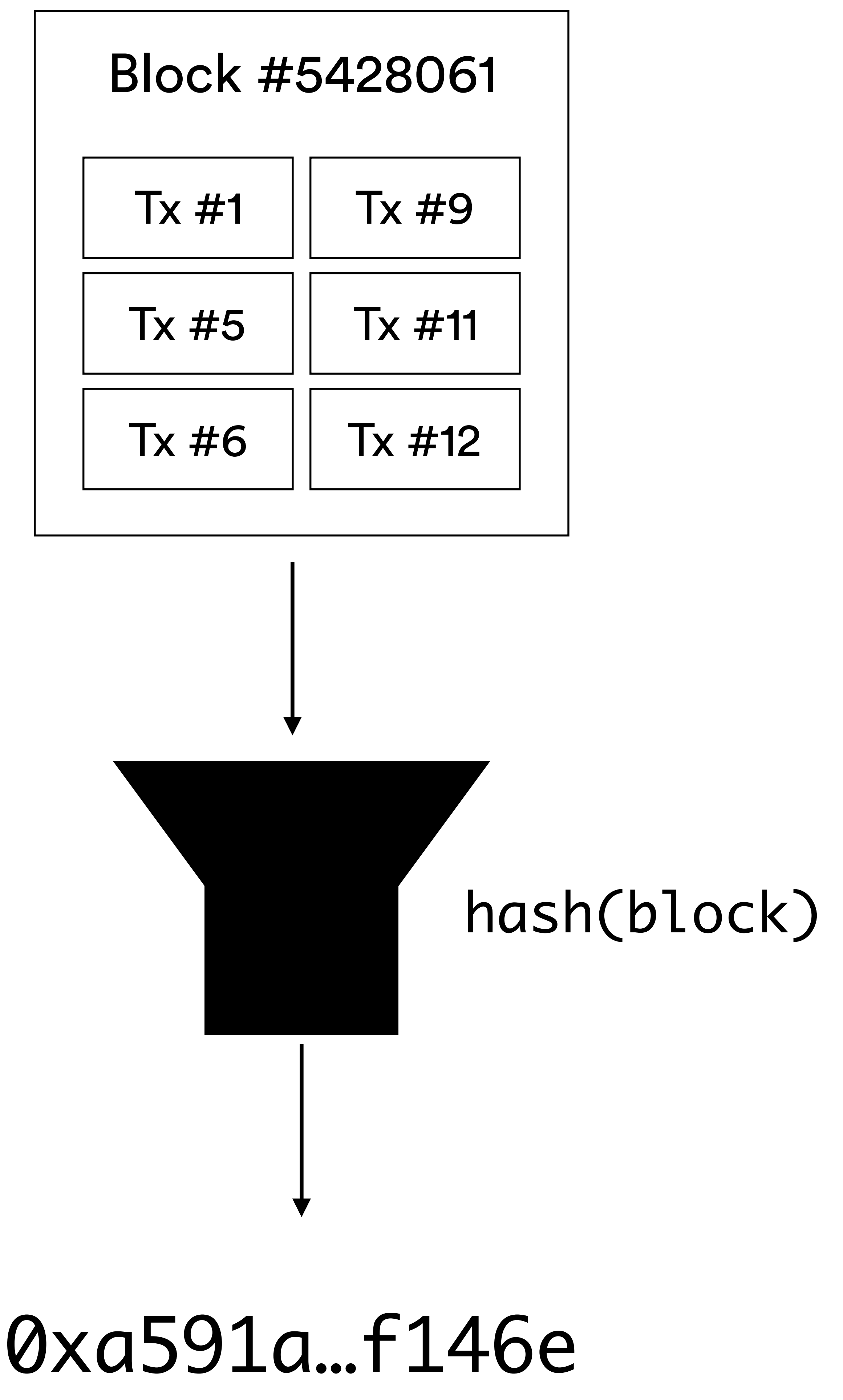
Points to previous block hash

Block #277’316	
Hash	2
Previous Block Hash	0000000000000002…569
Merkle Root	c91c…cf2e
Timestamp	2013-12-27 23:11:54
Difficulty Target	1,180,923,195.26
N	924591752

Proof of Work

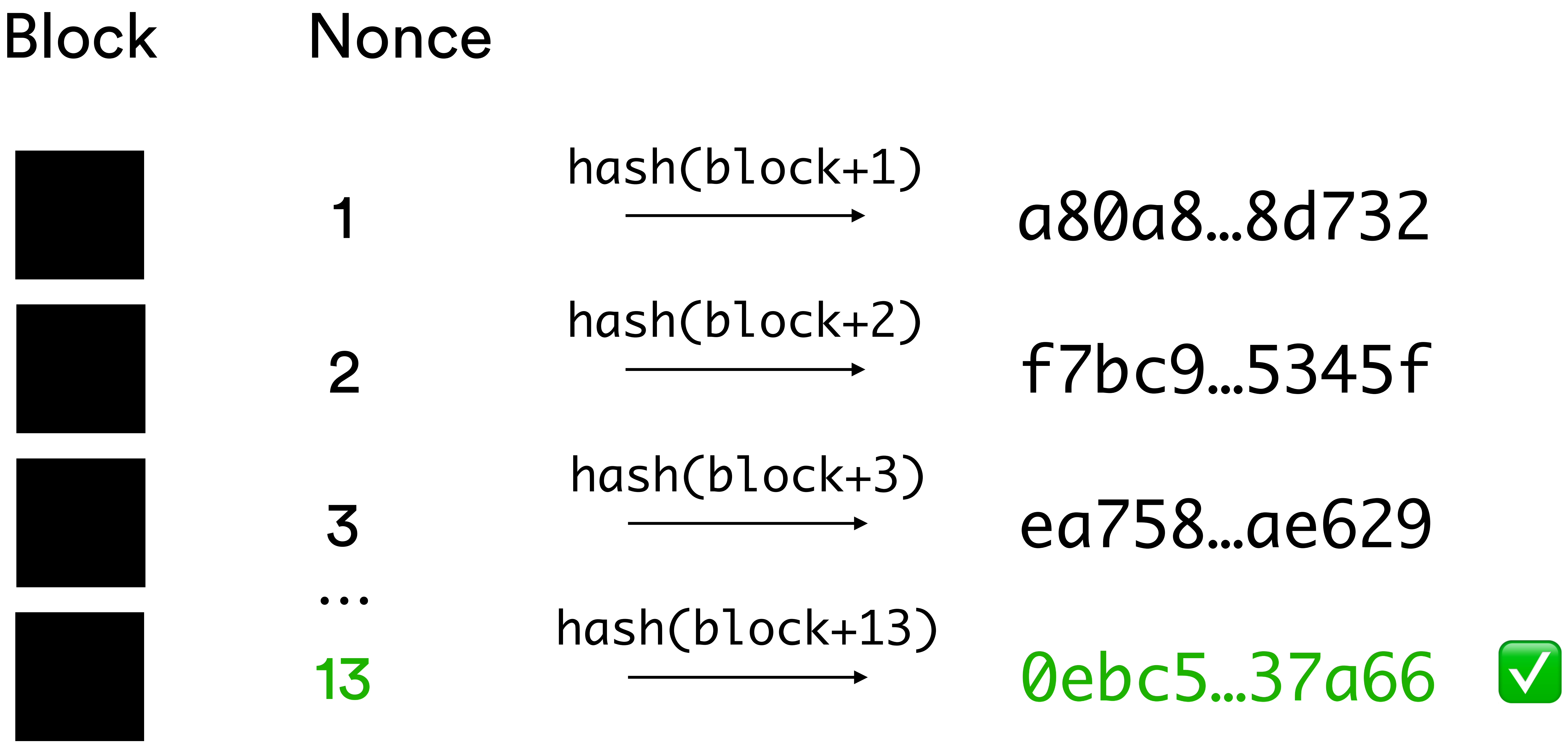
- Each node of the network has to solve a difficult mathematical problem to propose a block

- Since it takes significant computing power to solve this problem, it proves that the node has done sufficient work to produce the block



Proof of Work

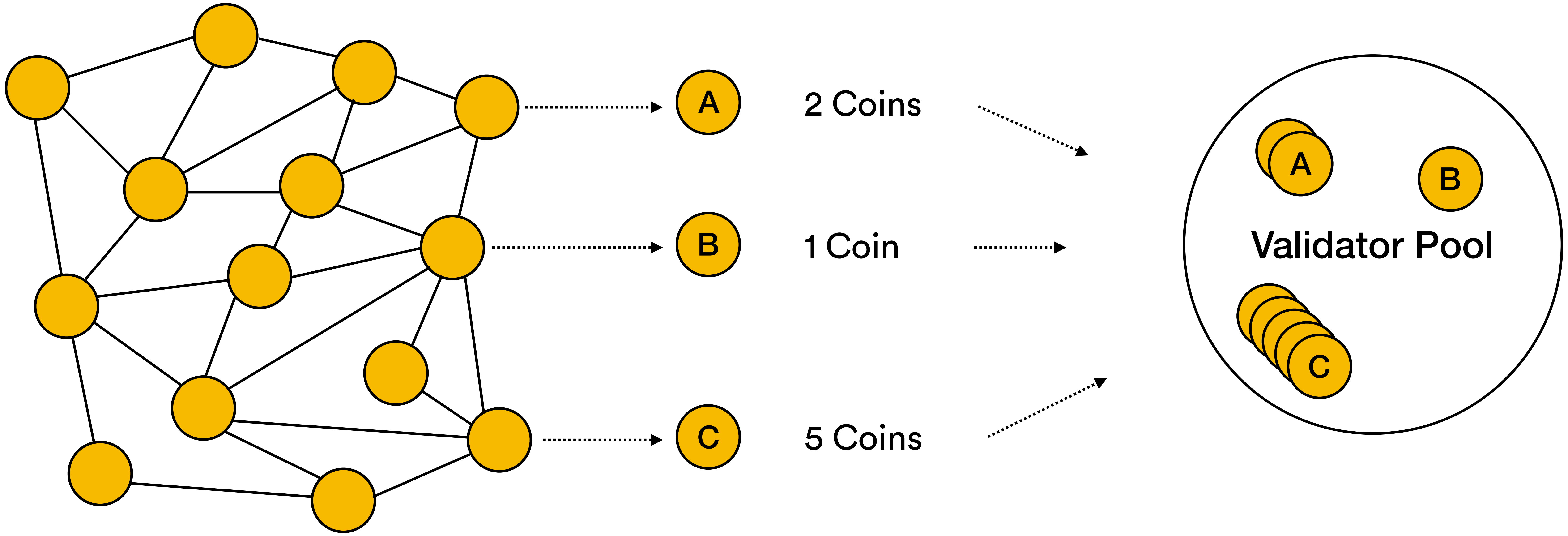
The nonce is used to **vary the output** of a cryptographic function.



Block	Nonce		
	1	hash(block+1) →	a80a8…8d732
	2	hash(block+2) →	f7bc9…5345f
	3	hash(block+3) →	ea758…ae629
	…		
	13	hash(block+13) →	0ebc5…37a66 ✅

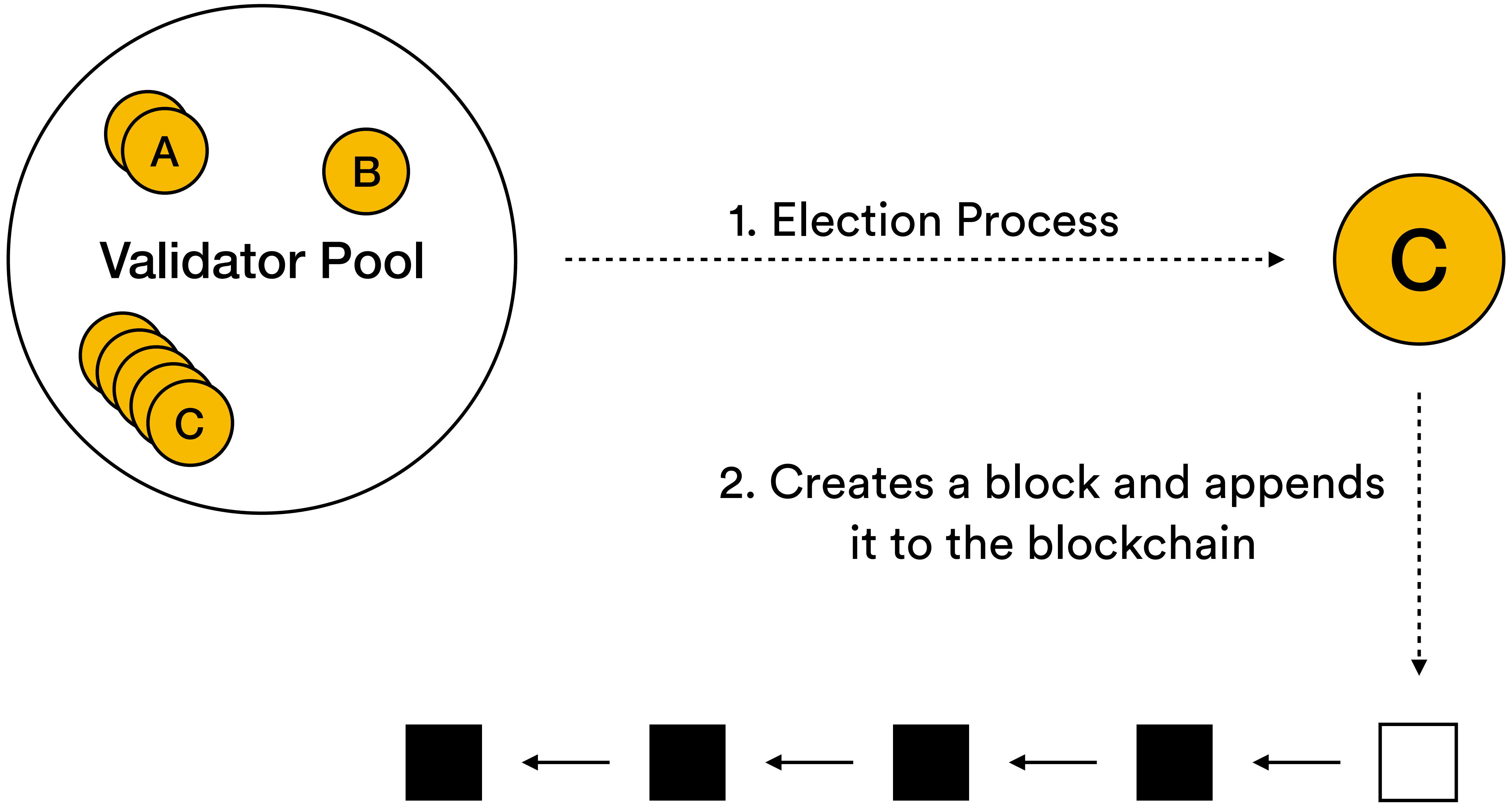
Proof of Stake

Nodes wishing to participate in the validation process put money on *stake*, i.e., joining a set of validators ("lottery").



Proof of Stake

The more coins a node invests, the higher its stake; and the higher the chance of winning the "lottery".



The Bazo Blockchain

- Blockchain developed by the University of Zurich and University of Applied Sciences Rapperswil

- Developed as PoW-based blockchain in 2017, moved to chain-based PoS in 2018

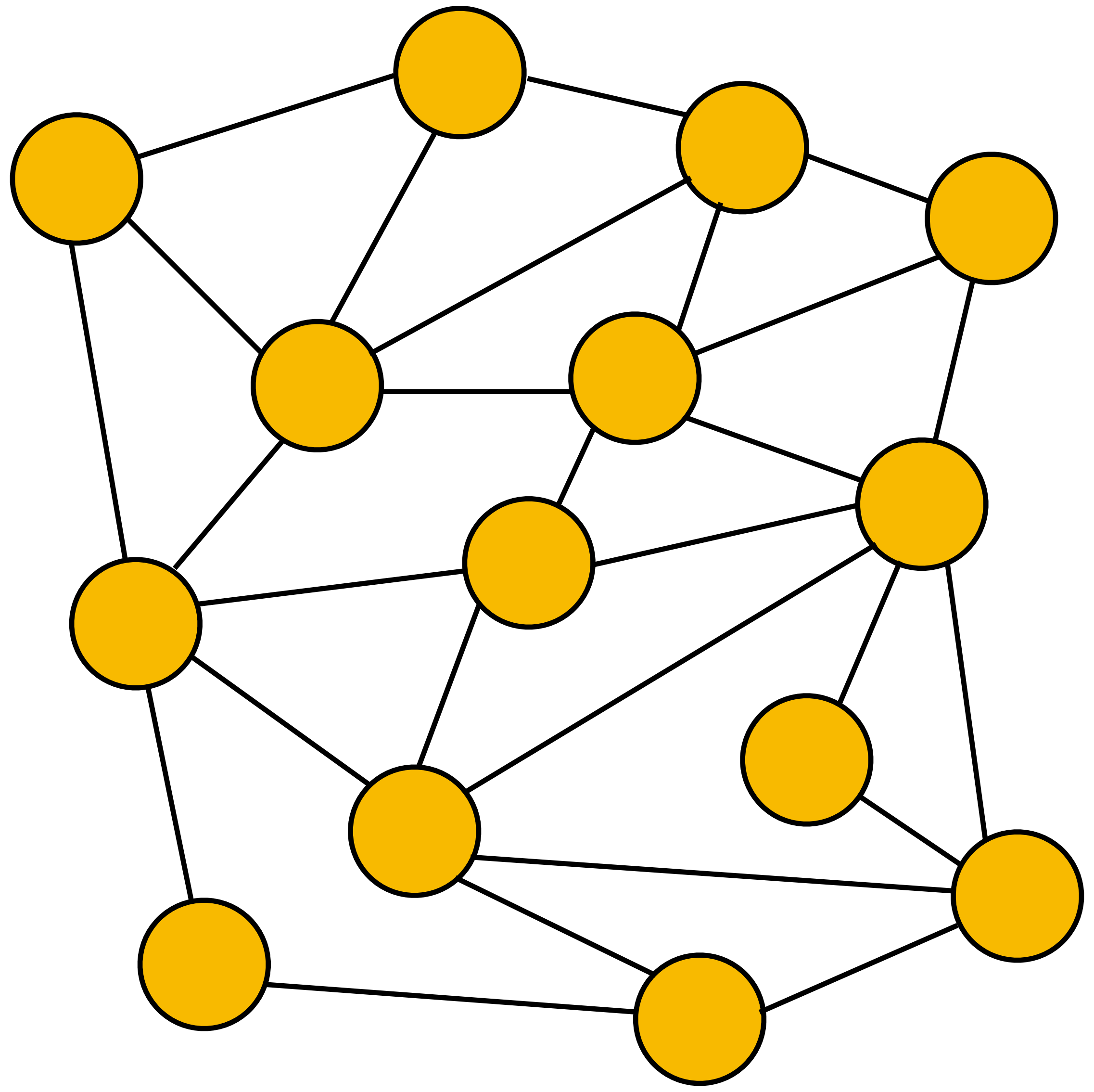
Proof of Stake in Bazo

Public
PubKey: 4dc4…b904
Hashed Seed: 3ae7…32cd

A

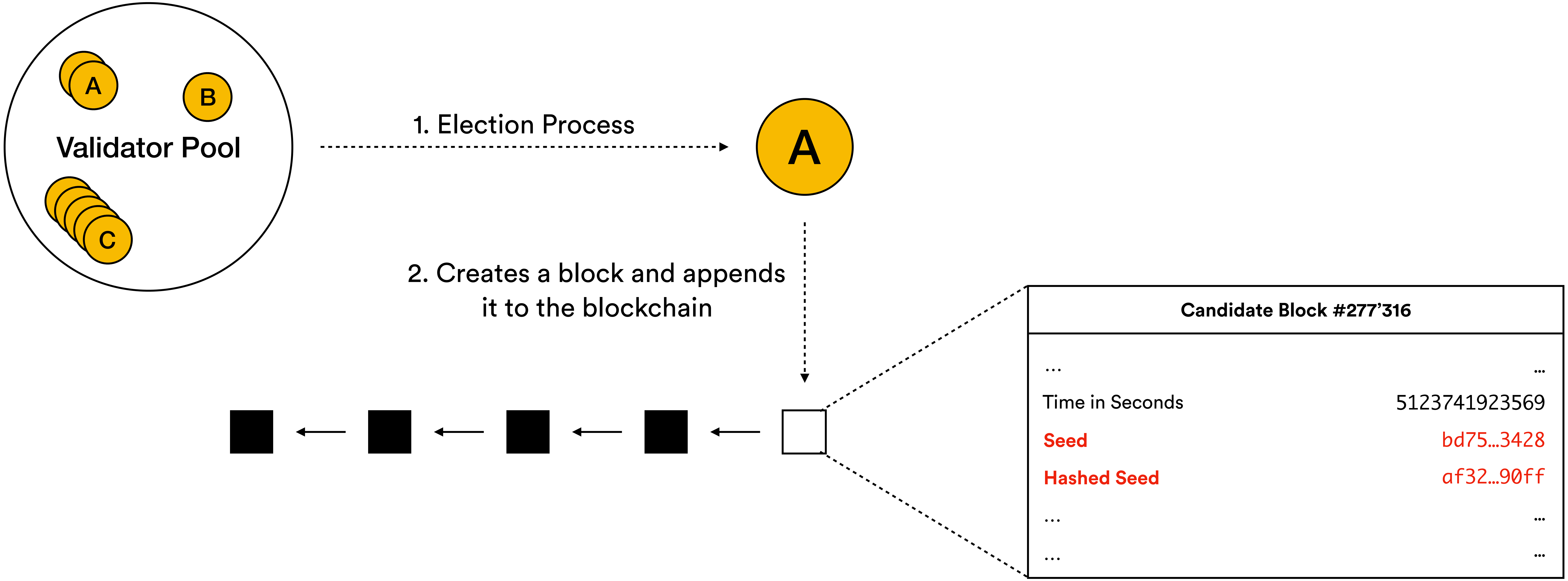
Private
PrivKey: 8063…aeac
Seed: bd75…3428

Publish Stake Transaction to the network



StakeTx #4’301	
Fee	2
Is Staking	True
Account	4dc4…b904
Timestamp	2018-04-27 23:11:54
Hashed Seed	3ae7…32cd
Signature	ffa1…43e1

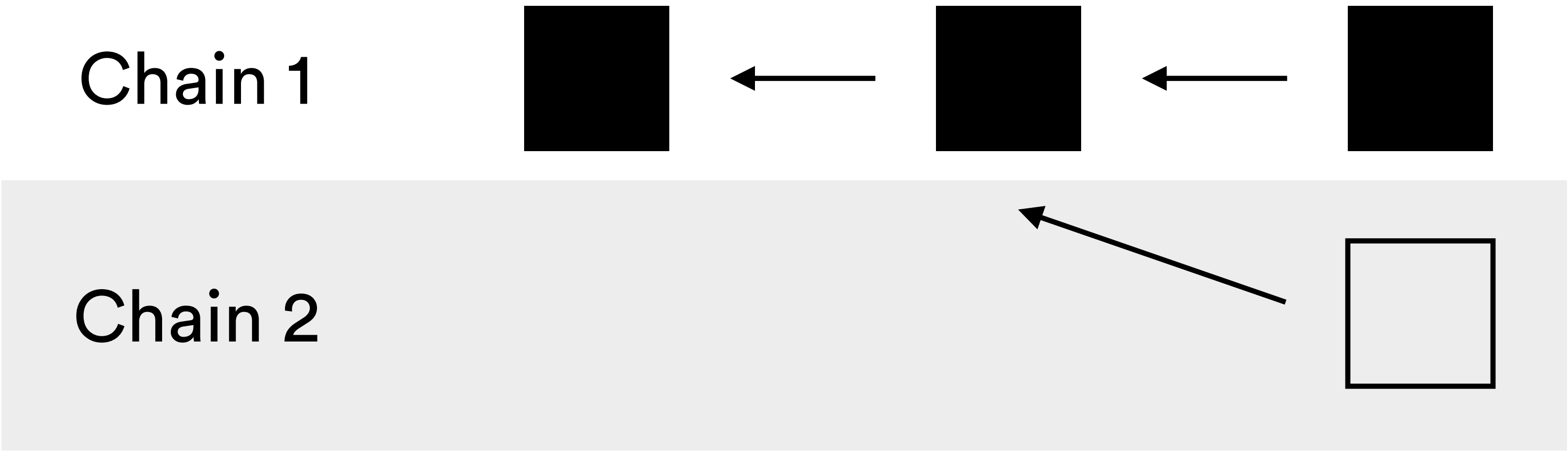
Proof of Stake in Bazo



Candidate Block #277'316	
...	...
Time in Seconds	5123741923569
Seed	bd75…3428
Hashed Seed	af32…90ff
...	...
...	...

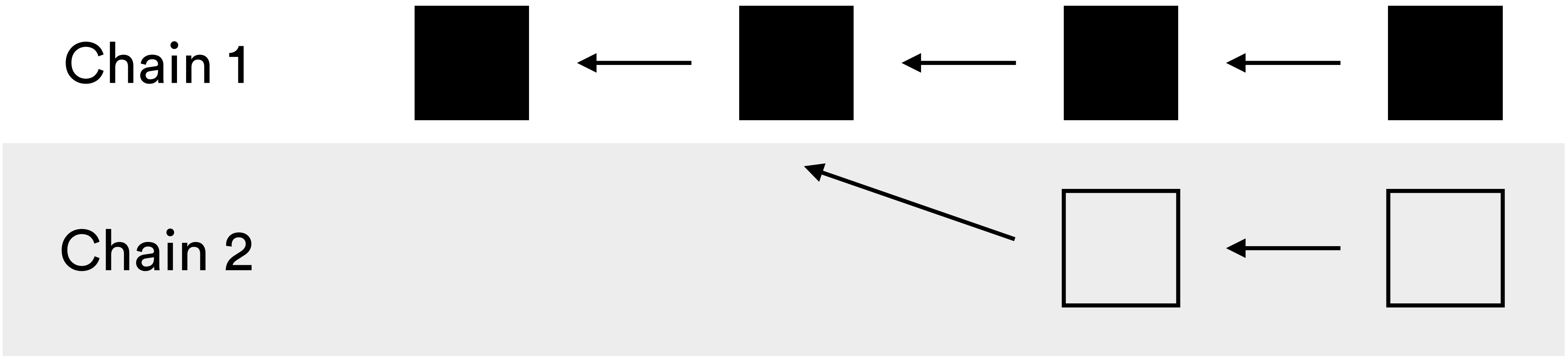
Problem: Seed Exposure

Assume that an accidental fork happens, i.e., two validators fulfill the PoS condition at the same time.



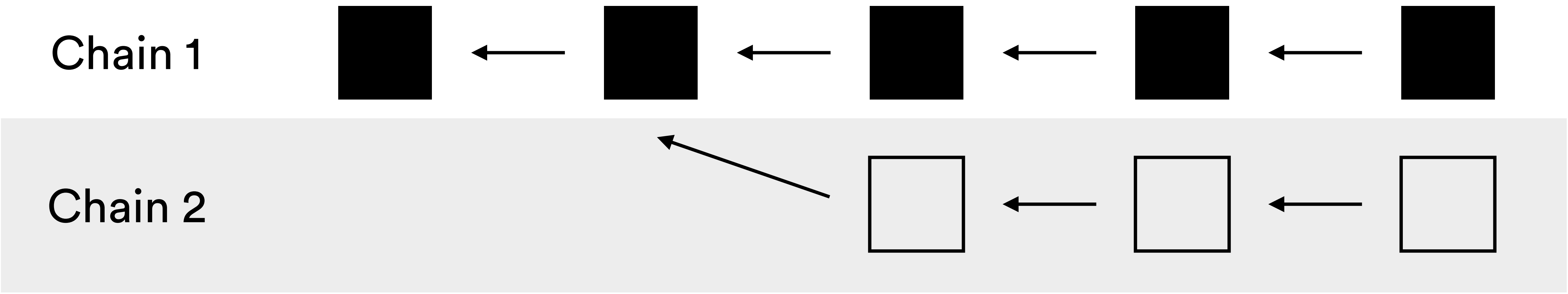
Problem: Seed Exposure

Both chains could potentially grow side-by-side for an indefinite amount of time



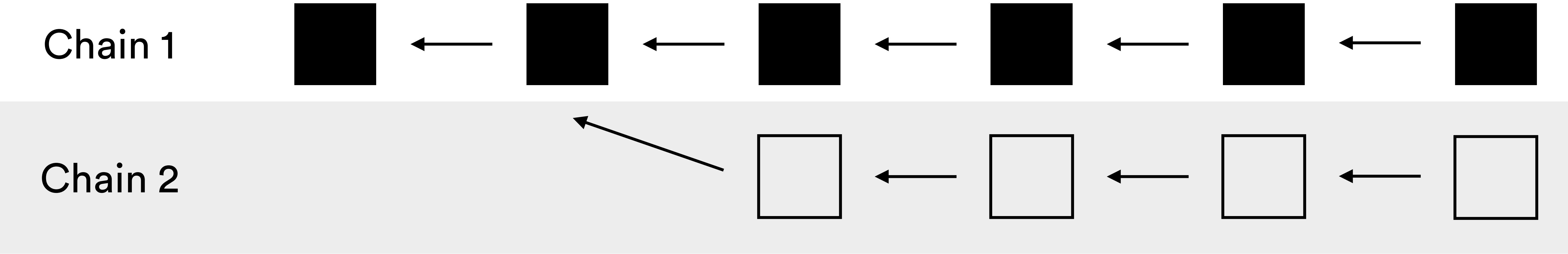
Problem: Seed Exposure

Both chains could potentially grow side-by-side for an indefinite amount of time



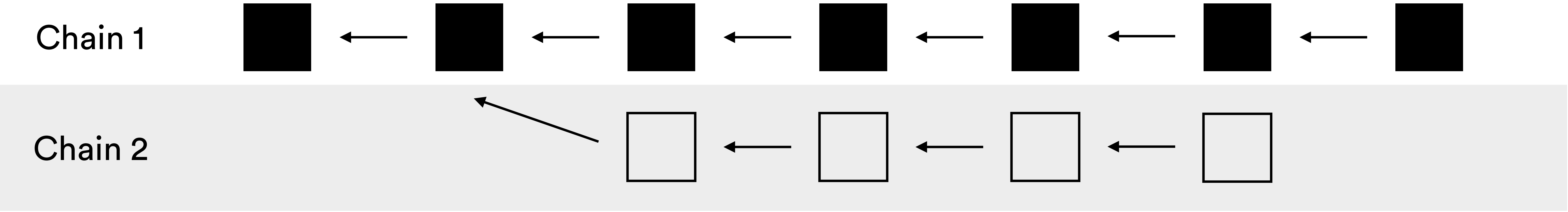
Problem: Seed Exposure

Validators who worked on the shorter chain have published their local seed



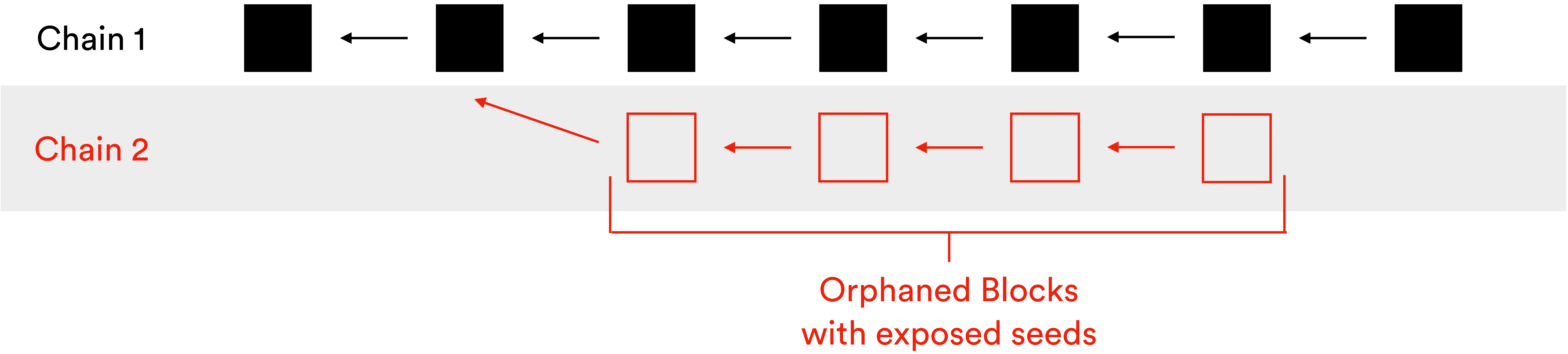
Problem: Seed Exposure

A fork is resolved when one chain becomes longer than the other.

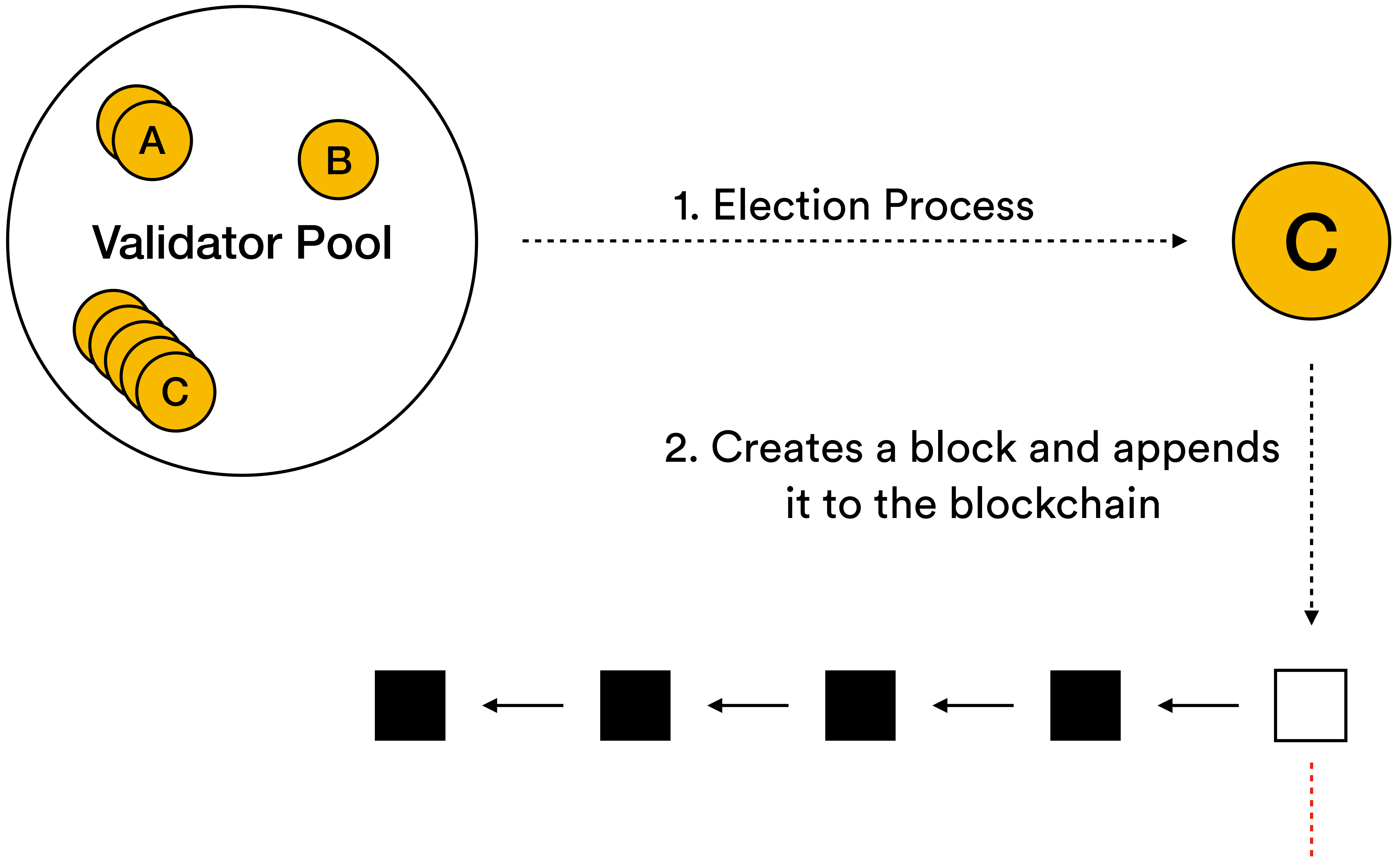


Problem: Seed Exposure

Validators who worked on the shorter chain have published their local seed



Design Approach



Block contains publicly verifiable information that is only valid for this block

Sortition Using VRFs vs. RSA

	VRFs	**RSA**
Additional public-private key-pair required?	No, public-private key-pair of wallet can be used	Yes, a second public-private key-pair must be maintained
Additional Size in StakeTx	0 Bytes	512 Bytes*
Size in Block	2 x 32 Bytes	512 Bytes*
Built-in Golang	No, 3rd party package required	Yes, "crypto/rsa" package

* assuming that a key size of 4096 bits is chosen

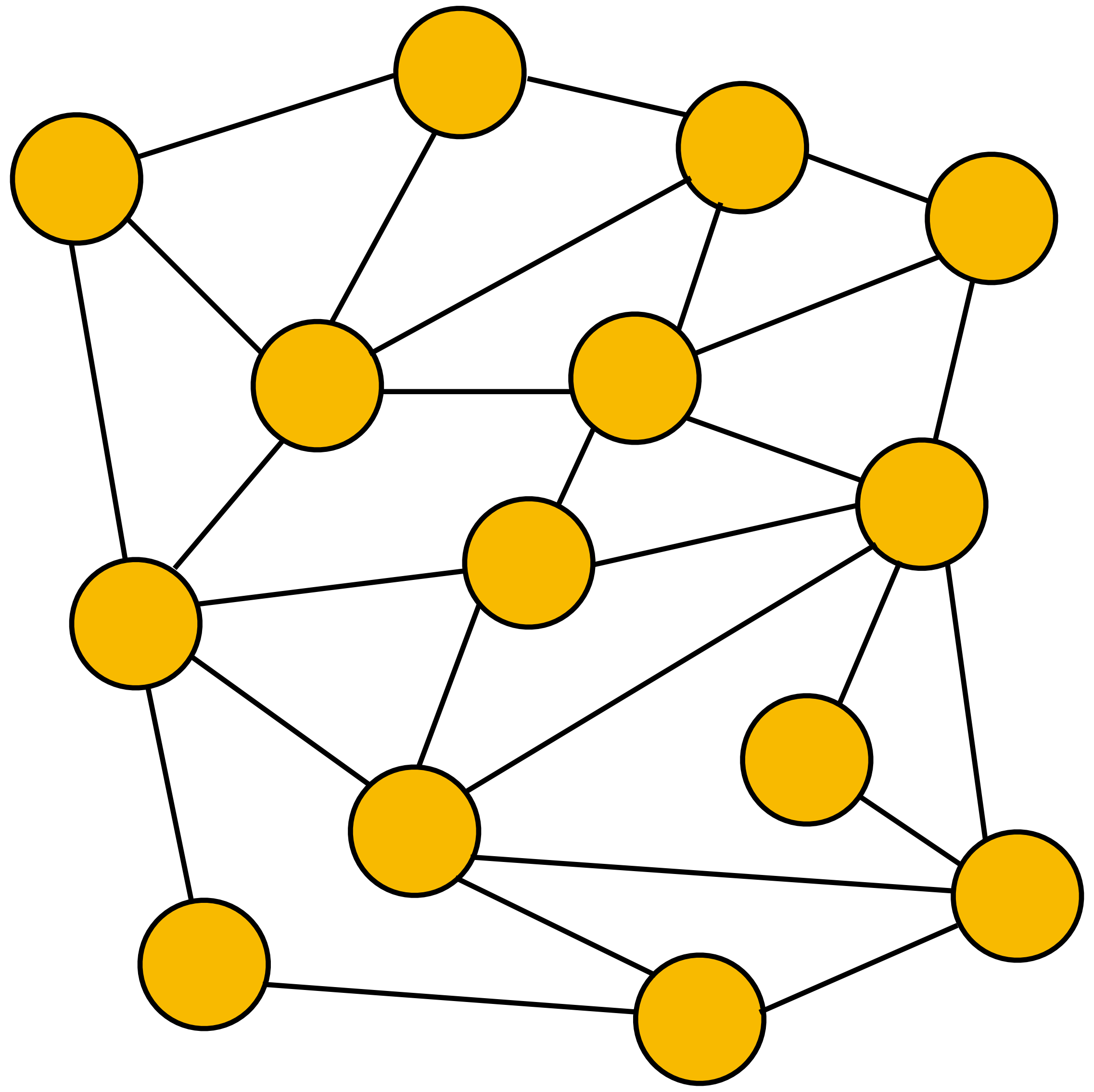
Solution Using RSA Sortition

Public
PubKey: 4dc4…b904
RSA PubKey: 3ae7…32cd

A

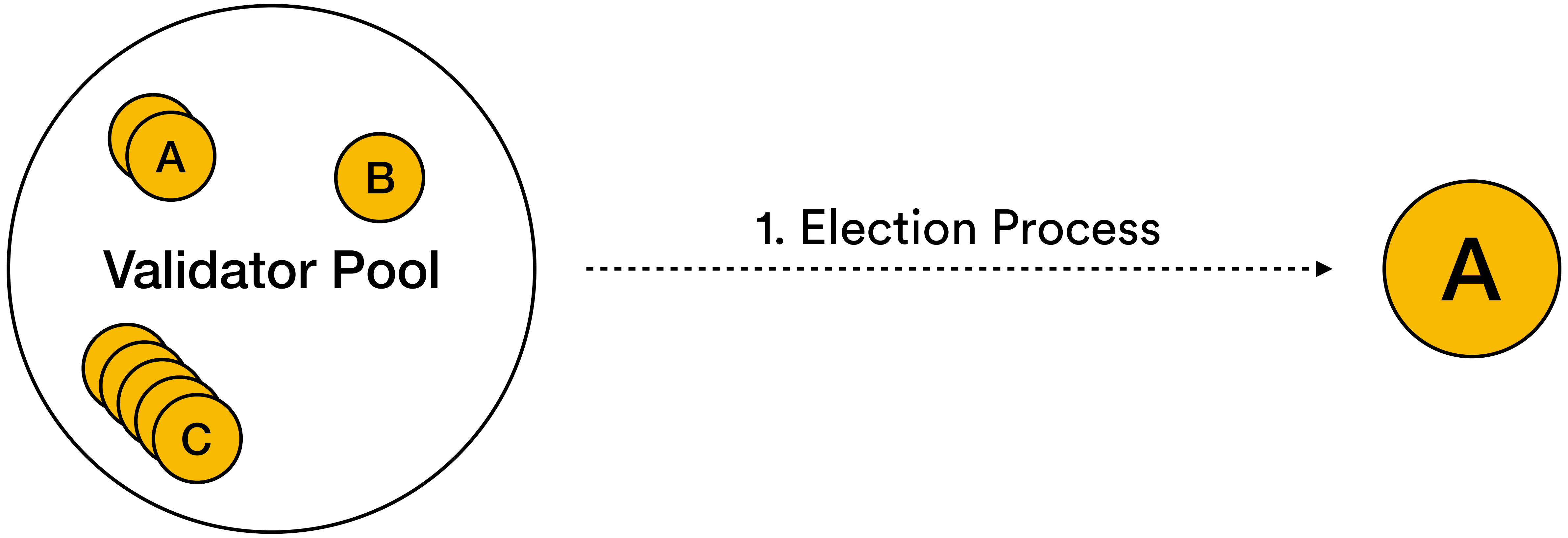
Private
PrivKey: 8063…aeac
RSA PrivKey: bd75…3428

Publish Stake Transaction to the network

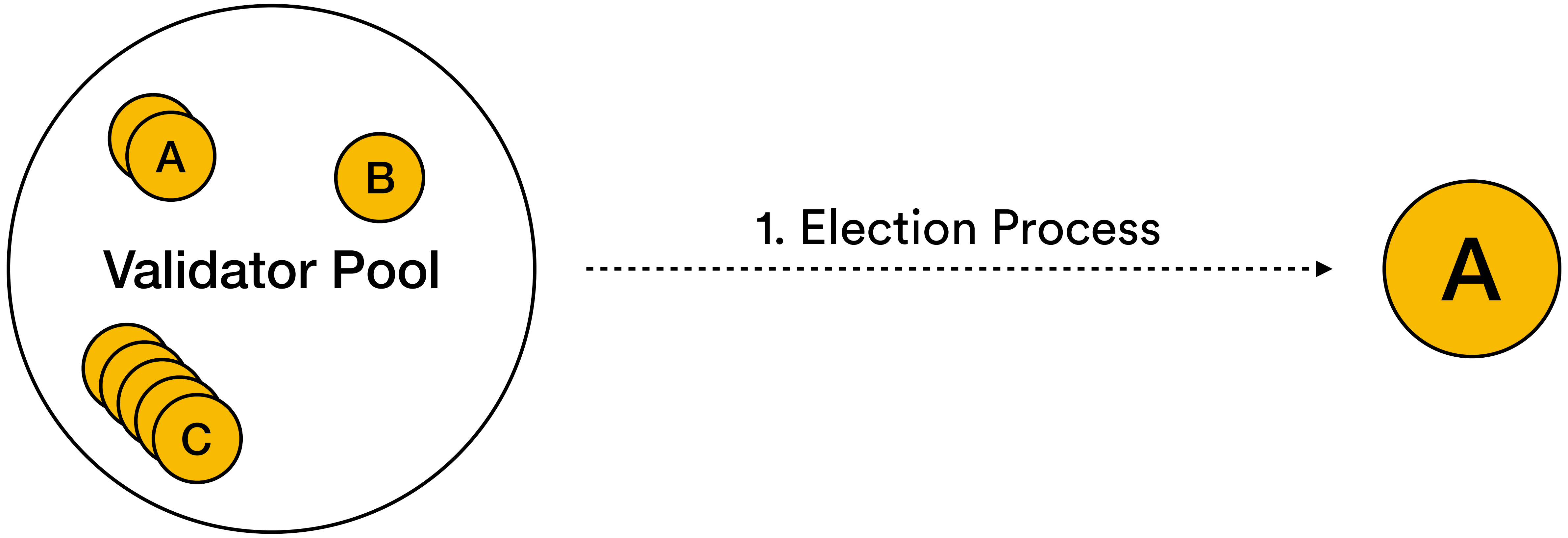


StakeTx #4’301	
Fee	2
Is Staking	True
Account	4dc4…b904
Timestamp	2018-04-27 23:11:54
Key Commitment	3ae7…32cd
Signature	ffa1…43e1

Solution Using RSA Sortition



Solution Using RSA Sortition



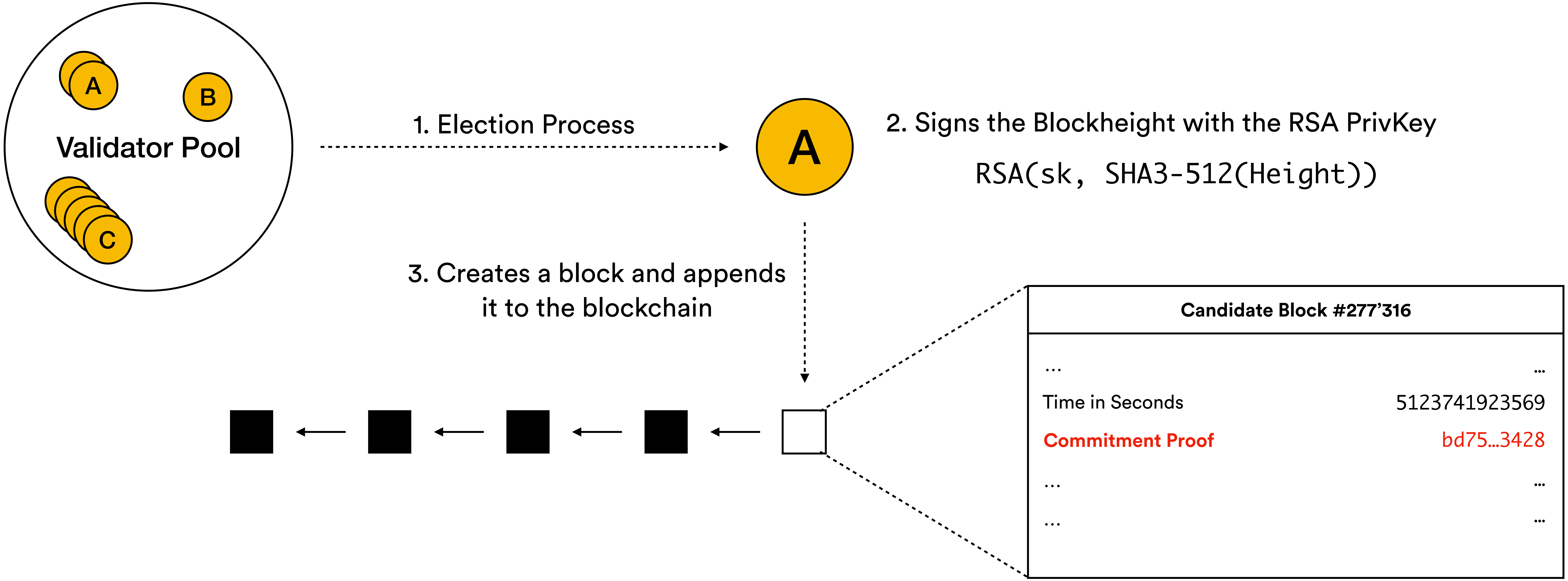
Validator Pool

1. Election Process

2. Signs the Blockheight with the RSA PrivKey

```
RSA(sk, SHA3-512(Height))
```

Solution Using RSA Sortition



1. Election Process

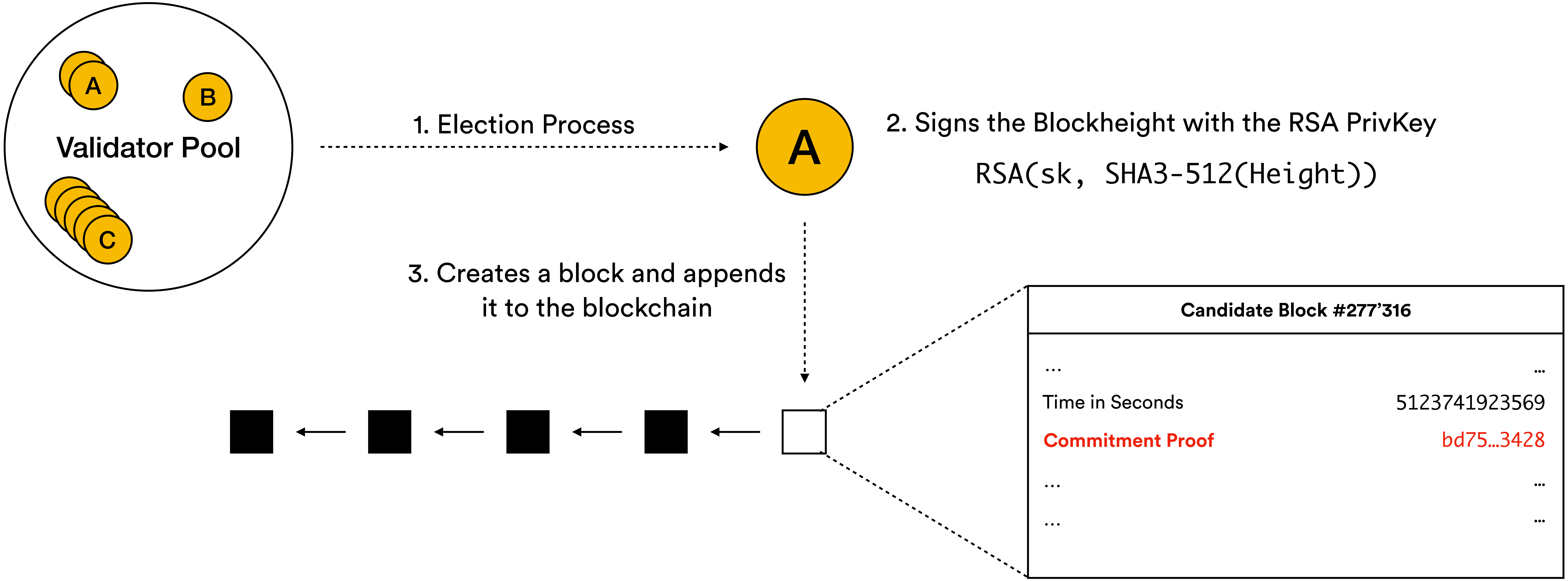
2. Signs the Blockheight with the RSA PrivKey

```
RSA(sk, SHA3-512(Height))
```

3. Creates a block and appends it to the blockchain

Candidate Block #277’316	
...	...
Time in Seconds	5123741923569
Commitment Proof	bd75...3428
...	...
...	...

Solution Using RSA Sortition



1. Election Process

2. Signs the Blockheight with the RSA PrivKey

```
RSA(sk, SHA3-512(Height))
```

3. Creates a block and appends it to the blockchain

Candidate Block #277’316	
…	…
Time in Seconds	5123741923569
Commitment Proof	bd75…3428
…	…
…	…

4. With the RSA PubKey of A, validators B and C can verify the commited proof by A

Questions?

Feel free to ask. 🙋‍♂️

Contact

Roman Blum
Mail: rblum@hsr.ch
Telegram: @rmnblm
Twitter: @rmnblm

Credits

- Proof of Stake for Bazo
  — *by S. Bachmann, 2018*
- Proof of Stake Infographic
  — *Cryptographics, https://bit.ly/2HJOQdt, 2018*