

TeleTrust-Informationstag "Blockchain"

Frankfurt a.M., 13.07.2017

Blockchain: Proof of Stake

Jörn-Marc Schmidt, secunet Security Networks AG

Blockchain: Proof of Stake

Jörn-Marc Schmidt, 13.07.2017

A decorative graphic element consisting of several overlapping, wavy, red and pink shapes that sweep across the bottom of the slide, creating a modern, abstract background.

Proof of Work

- Slow block generation
- Equal chances for each block
- Incentive to play fair

Slow Block Generation



- Time-based generation
- Coin Age
 - » Reset when a block is found
 - » Age between 30 and 90 days
- $\text{Proofhash} < \text{coins} * \text{age} * \text{target}$
 - » Proofhash
 - » Transaction input
 - » Fixed data
 - » Current time
- Cannot be improved by increasing computation power

Greedy Honest Nodes

- Not always online
- Problem: coin age
- Improve timestamps / selection of validators
- $\text{Proofhash} < \text{coins} * \text{target}$



Building a Chain



- „Nothing at Stake“ Problem
- Why not voting for different chains?
- Preserve the value of their investment?
- Punish validators voting for both / the wrong chain?

Proof of Stake

- Use of validators
 - » Locking-up coins
- (Pseudo-)random selection
 - » More coins increase chances
- Blocks are forged, not mined
 - » No new coins are generated
- Expensive monopoly



Voting-Based

- Validators can propose blocks
- Voting on blocks
 - » By sending signed messages
 - » Weighted by deposited coins
- Finality conditions
- Slashing conditions
 - » Detect misbehavior

Benefits

- Increased efficiency
 - » No need to use so much electricity
 - » No need to create new coins

- Linear increase with the stake

- Increased flexibility
 - » Methods from game theory to prevent cartels
 - » Penalties become possible to prevent 51% attacks

Conclusions

- Promising approach
- „Non-trivial“
- „Hybrid“ checkpoints
- More to come
 - Casper
- BUT: Simulations showed successful attacks





Jörn-Marc Schmidt

secunet Security Networks AG

Mergenthaler Allee 77

65760 Eschborn

joern-marc.schmidt@secunet.com