

TeleTrusT-Informationstag "Blockchain"

Frankfurt a.M., 13.07.2017

Blockchain: Proof of Stake

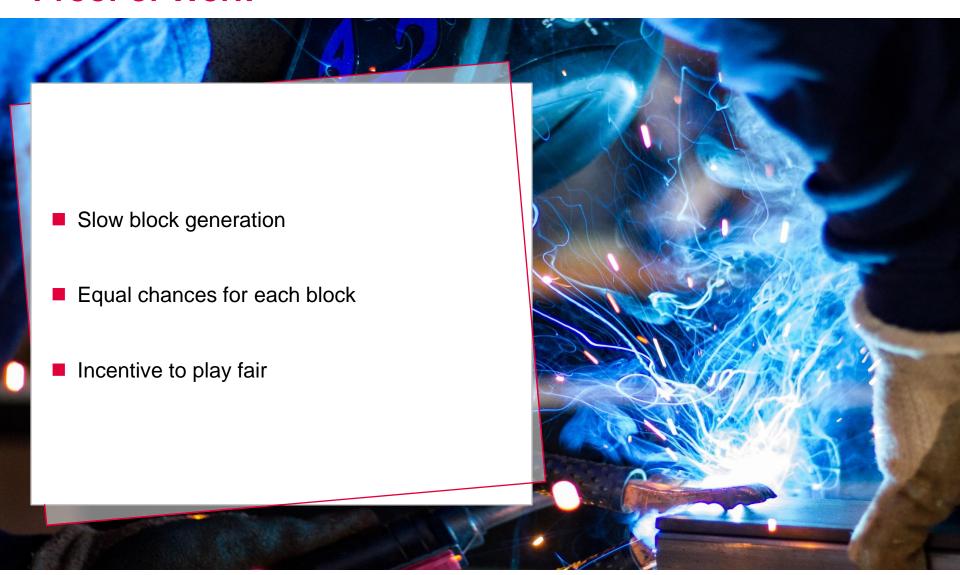
Jörn-Marc Schmidt, secunet Security Networks AG

secunet

Blockchain: Proof of Stake

Jörn-Marc Schmidt, 13.07.2017

Proof of Work



Proof of Stake

Seite 3

Slow Block Generation



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



Seite 4

Greedy Honest Nodes

- Not always online
- Problem: coin age
- Improve timestamps / selection of validators

Proof of Stake

Proofhash < coins * target</p>



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





Proof of Stake

Voting-Based

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



Proof of Stake

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

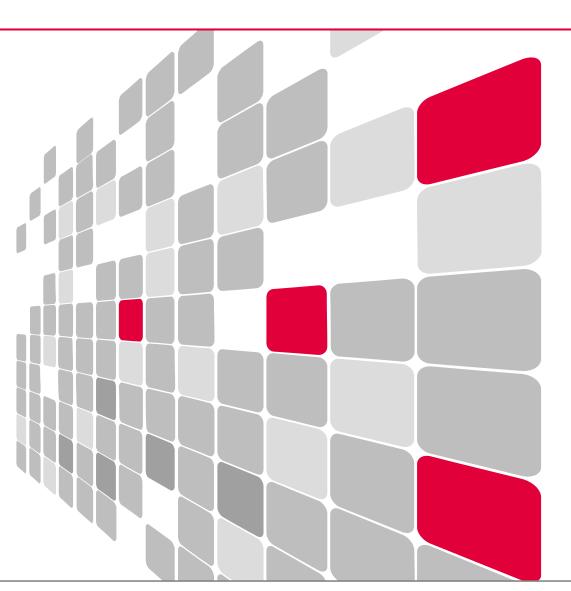
Proof of Stake



Seite 9

Conclusions

- Promising approach
- "Non-trivial"
- "Hybrid" checkpoints
- More to come
 - >> Casper
- **BUT: Simulations showed** successful attacks





secunet

Jörn-Marc Schmidt

secunet Security Networks AG
Mergenthaler Allee 77
65760 Eschborn

joern-marc.schmidt@secunet.com