TeleTrusT
Pioneers in IT security.

TeleTrusT-Informationstag "Blockchain"

Berlin 27.06.2018

Neue Basis-Technologien und Konsensalgorithmen

Philipp Lang, Blockchain Team esatus AG

Agenda

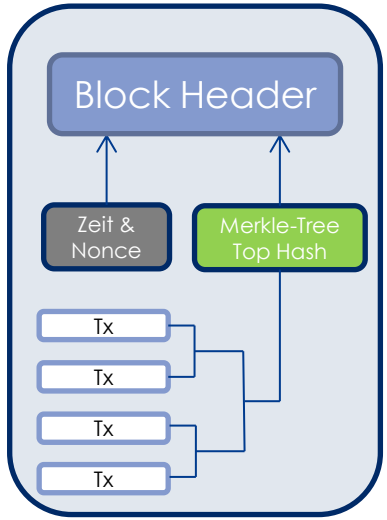
esatus® AG
Enforcing Information Security

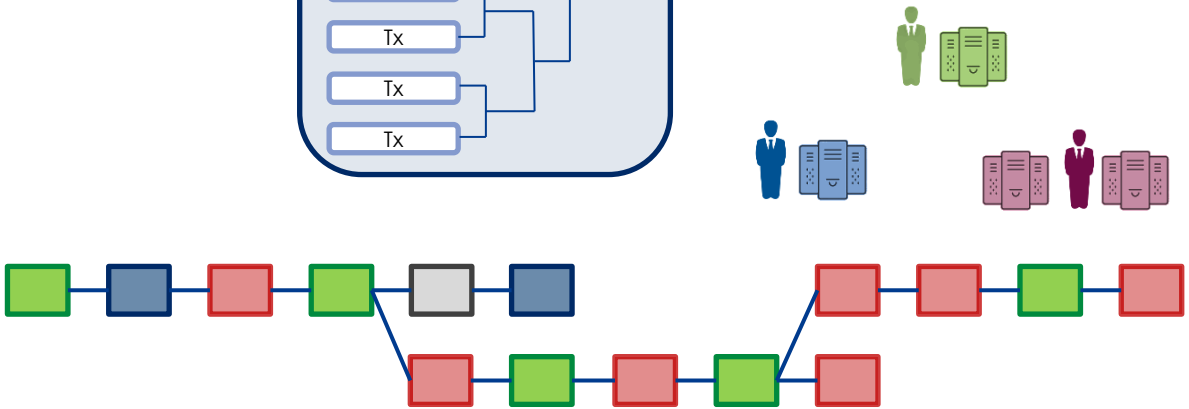
1. Proof of X
2. Directed Acyclic Graph (DAG)
3. BFT-Algorithmen
4. Forschung

Proof of Work (PoW)

esatus® AG
Enforcing Information Security

- Anwendungen
  - BTC/BCH
  - LTC
  - ETH/ETC
- Stärken
  - Vertrauenslose Umgebungen
  - Etabliertes Verfahren
  - Funktioniert (aktuell)
- Schwächen
  - Hohe Kosten
  - Skalierung
  - Majority Attacken

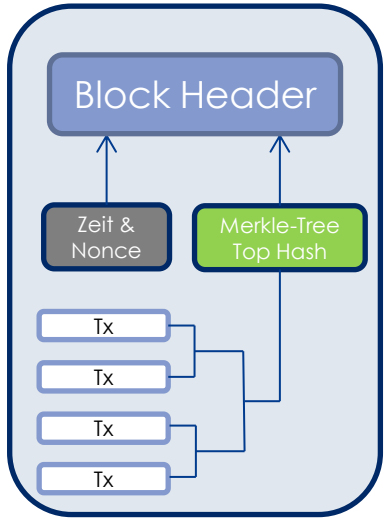


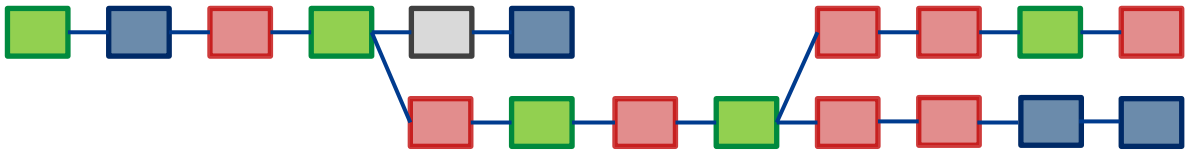


Proof of Stake (PoS)

esatus® AG
Enforcing Information Security

- Anwendungen
  - ADA
  - STRAT
  - Dash
  - Neo
- Stärken
  - Energie effizienter
  - Vertrauenslose Umgebungen
  - Bereits in Anwendung
- Schwächen
  - Majority Attacken
  - Nothing at Stake





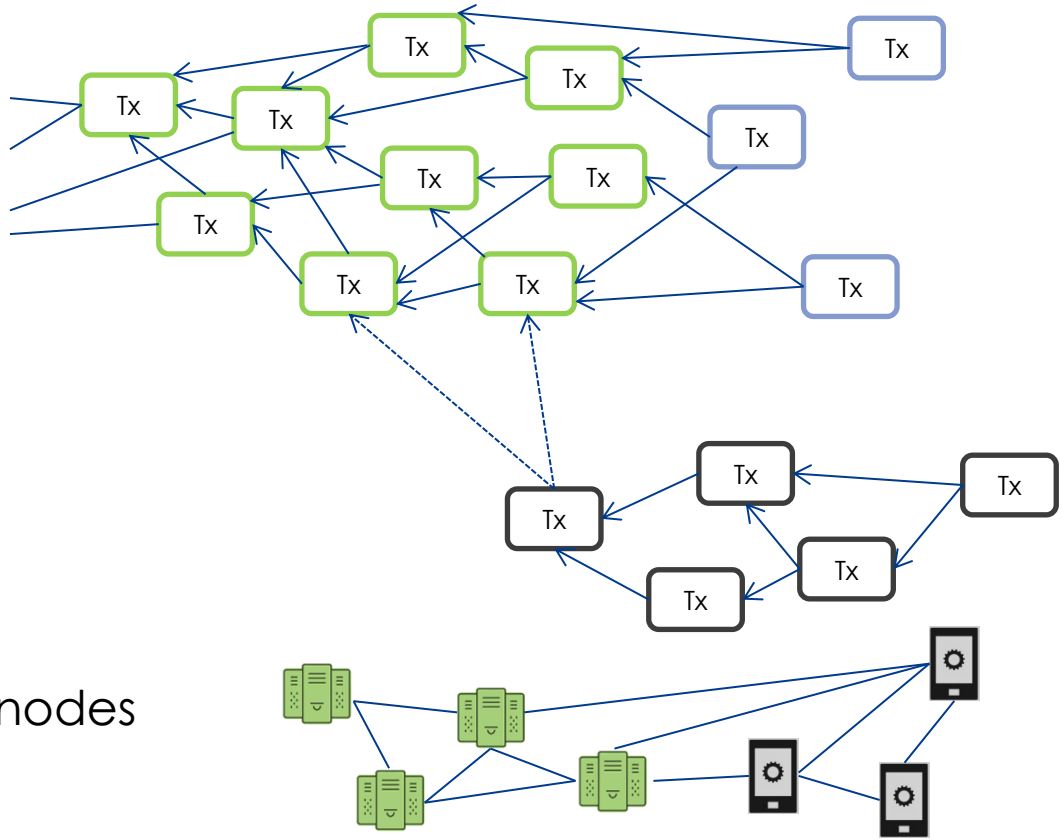
esatus AG
Enforcing Information Security

2. Directed Acyclic Graph (DAG)

Directed Acyclic Graph (DAG)

esatus AG
Enforcing Information Security

- Anwendungen
  - Byteball
  - IOTA
- Stärken
  - Hohe Skalierbarkeit
  - Offline Modus (IOT)
  - Keine Blöcke / Gebühren
- Schwächen
  - Mindestanzahl Transaktionen
  - Große Abhängigkeit von Fullnodes



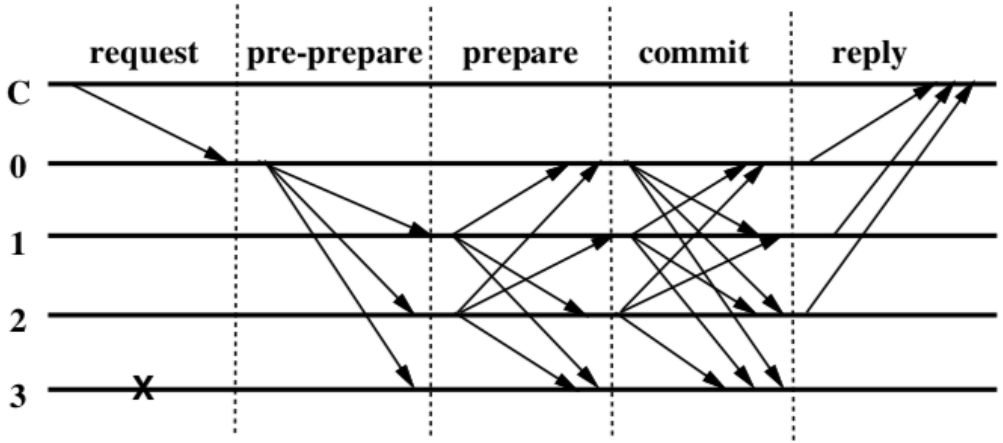
esatus AG
Enforcing Information Security

3. BFT-Algorithmen

Practical Byzantine Fault Tolerance (PBFT)

esatus AG
Enforcing Information Security

- Anwendungen
  - Hyperledger Fabric
- Stärken
  - Ursprung Sensortechnik
  - Hohe Skalierbarkeit
  - Effizienz
- Schwächen
  - Majority Attacke bei 1/3
  - Konsortium Verfahren



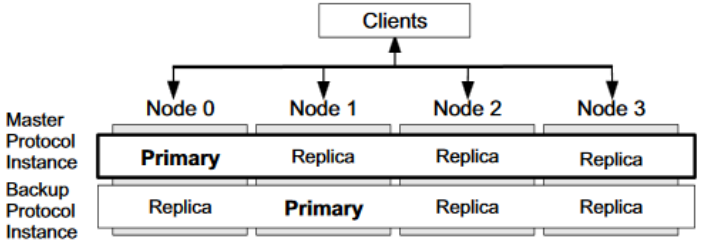
PBFT Schema [1]

1: http://pmg.csail.mit.edu/papers/osdi99.pdf

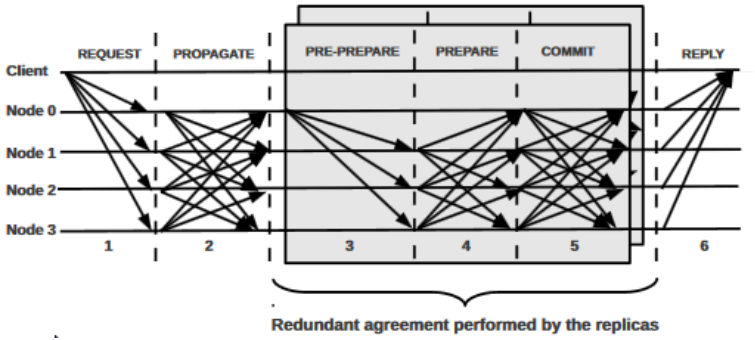
Redundant Byzantine Fault Tolerance (RBFT)

esatus® AG
Enforcing Information Security

- Anwendungen
  - Hyperledger-Indy (sovrin)
- Stärken
  - Hohe Skalierbarkeit
  - Effizienz
- Schwächen
  - Majority Attack bei 1/3
  - Konsortium Verfahren



RBFT Protocoll Steps [1]



RBFT Protocoll Steps [1]

1: https://pakupaku.me/plaublin/rbft/5000a297.pdf

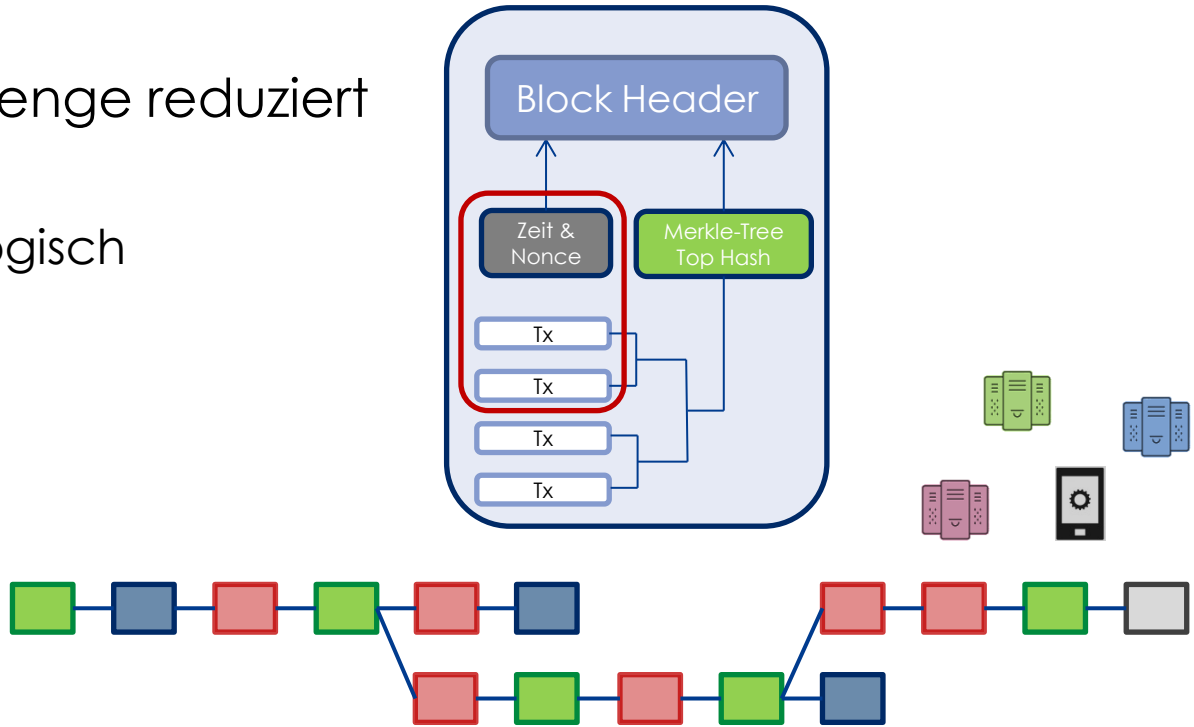
esatus AG
Enforcing Information Security

4. Forschung

PoW on a Blockchain

esatus® AG
Enforcing Information Security

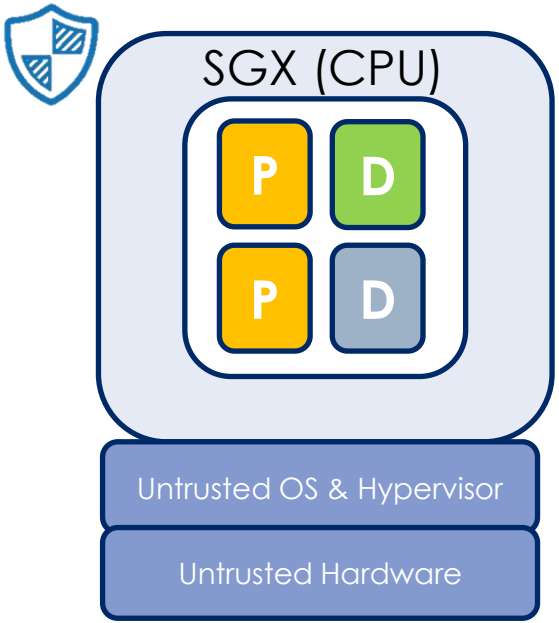
- IBM Patent 26. April
- Nonce wird auf Teilmenge reduziert
- Stärken
  - Ökonomisch / Ökologisch
  - IOT fähig
- Schwächen
  - Unerforscht
  - Kalibrierung unklar
  - Nur IOT Devices?



Proof of Ellapsed Time

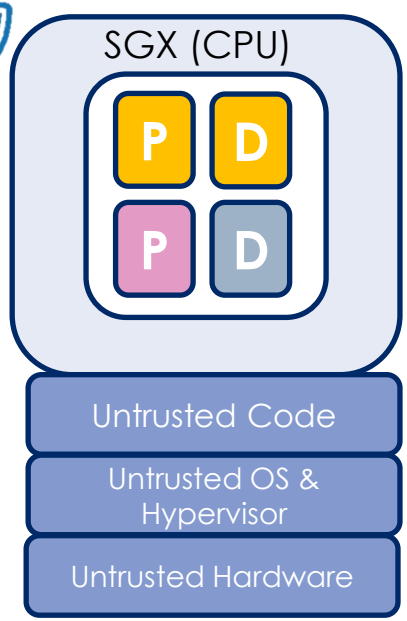
esatus AG
Enforcing Information Security

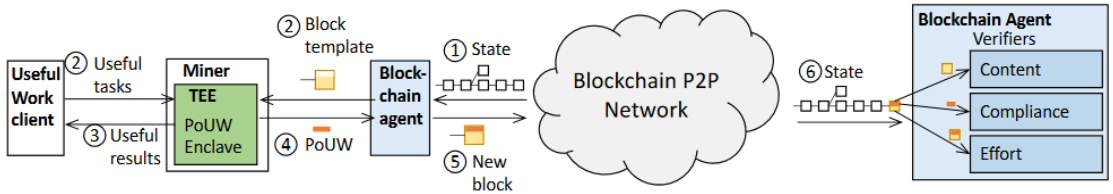
- Intel Patent
- „Simuliert“ PoW (schläft)
- Vorteile
  - Ökonomisch / Ökologisch
  - IOT Fähig
- Schwächen
  - Stale Chips Problem
  - Broken Chips Problem
  - Teilweise dezentralisiert



Proof of Useful Work (PoUW)

- Intels Security Guard Extension (SGX)
- Vorteile
  - Ökonomisch / Ökologisch
  - IOT Fähig
- Schwächen
  - Teilweise dezentralisiert



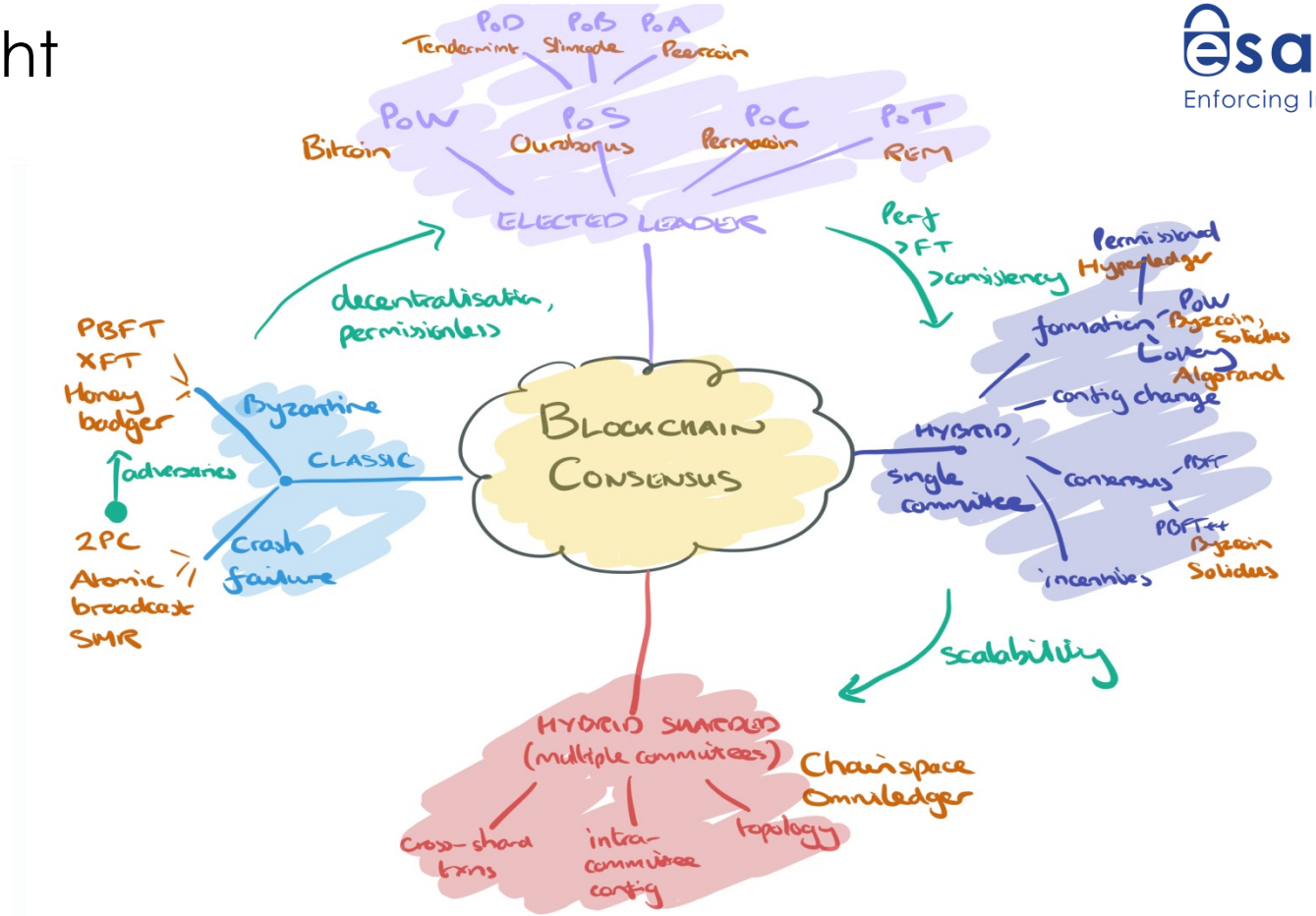


Architektur REM [1]

1: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-zhang.pdf

Übersicht

esatus AG
Enforcing Information Security



https://adriancolyer.files.wordpress.com/2018/02/blockchain-consensus-overview.jpeg

Quellen

esatus AG
Enforcing Information Security

- https://www.usenix.org/sites/default/files/conference/protected-files/usenixsecurity17_slides_fan_zhang.pdf
- https://coincierge.de/2018/ethereum-upgrade-sharding-jetzt-auf-github-bis-2020/
- https://byteball.org/Byteball.pdf
- https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf
- http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20180115425.PGNR.&OS=dn/20180115425&RS=DN/20180115425

Quellen

esatus AG
Enforcing Information Security

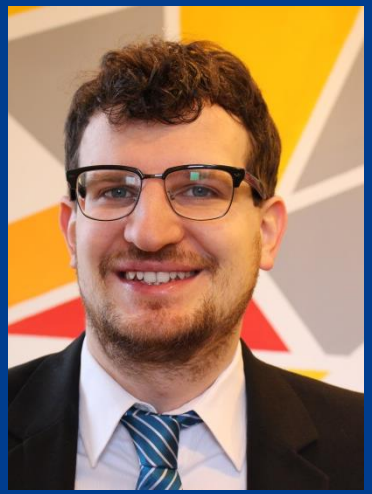
- https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs
- https://medium.com/kokster/understanding-hyperledger-sawtooth-proof-of-elapsed-time-e0c303577ec1
- http://iotatoken.com/IOTA Whitepaper.pdf

Questions & Answers

esatus® AG
Enforcing Information Security

Ansprechpartner

esatus AG
Enforcing Information Security



IT Consultant

Philipp Lang
Tel.: +49 171 4927307
p.lang@esatus.com

esatus AG | www.esatus.com

Copyright

esatus AG
Enforcing Information Security

Herausgeber: esatus AG

Copyright Fotos: Tomasz Zajda/Fotolia; bismillah_bd/Fotolia; tostphoto/Fotolia; envfx/Fotolia

esatus® AG
Enforcing Information Security

Vielen Dank für Ihre Aufmerksamkeit!