
ITU

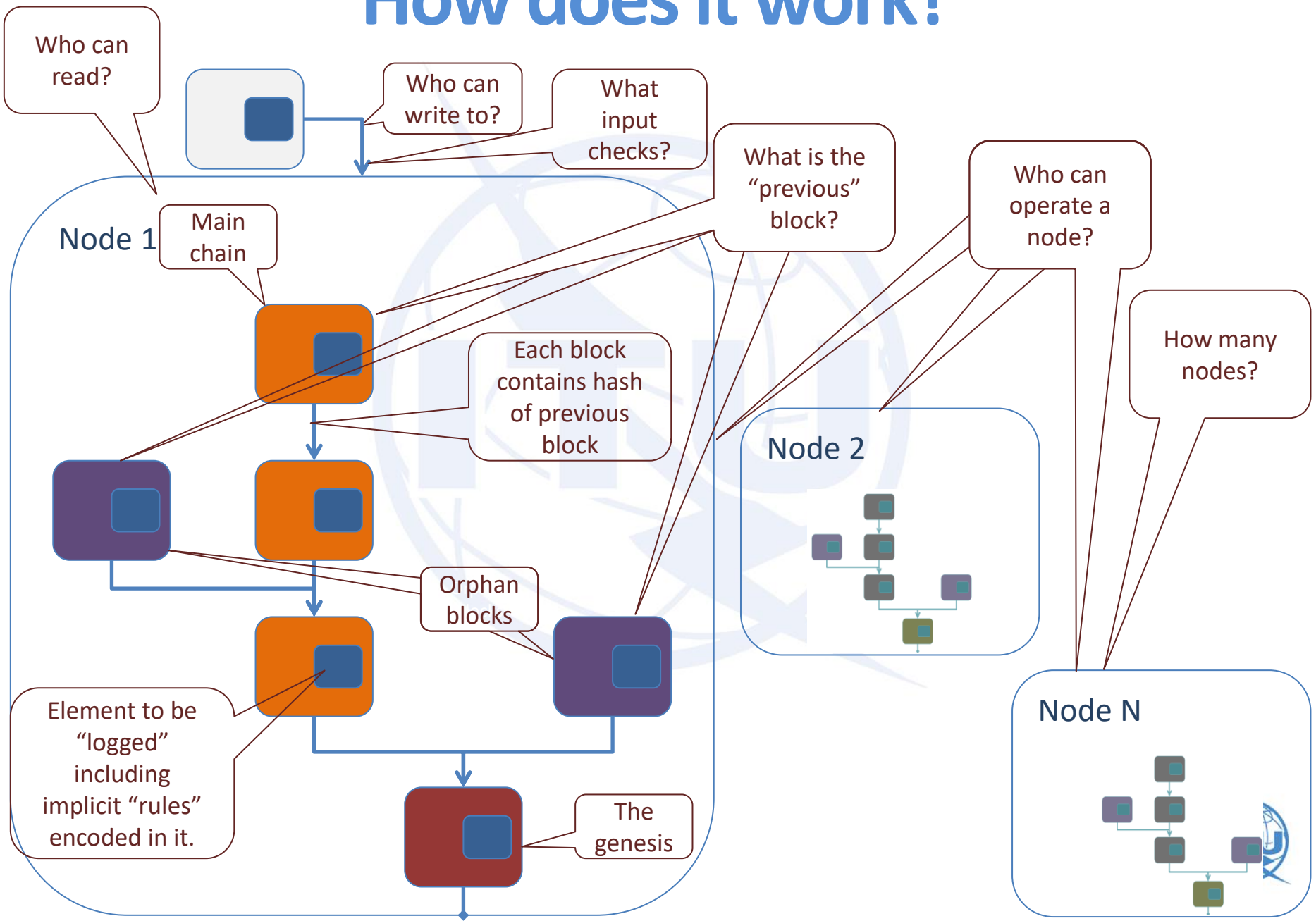
ITU Workshop on "Security Aspects of Blockchain" (Geneva, Switzerland, 21 March 2017)

Understanding Blockchain Security

Dr. Rolf Lindemann
Nok Nok Labs, rolf@noknok.com

Geneva, Switzerland, 21 March 2017

How does it work?



Summary (1)

- The term blockchain is not well defined today.
- We have to be careful what to put into publicly readable blockchains.
  - Cryptographic algorithms get weaker over time, but the data remains in the blockchain.
  - Originally we thought that hashed passwords are secure, we shouldn't repeat that mistake.
  - Analyzing "big data" sometimes can de-anonymize records.
  - People and systems fail, we need to make sure the impact of a failure remains acceptable (even from a privacy perspective).
- Democracy is based on "one vote per head". One vote per "computing power unit" is not the same as you can buy computing power with money.

Rolf Lindemann,
Nok Nok Labs

Summary (2)

- Several enhancements of Bitcoin blockchains have been proposed.
- Standardizing replacement of deprecated crypto algorithms should be investigated.
- Standardizing authentication (for non-public blockchains) supports interoperability
- Typically blockchain elements are signed. Sometimes it is helpful to require some “Level of Assurance” for related keys. Standardizing key attestation supports interoperability.

Rolf Lindemann,
Nok Nok Labs

Weaknesses

- No transactions can be deleted-ever ➔ Node data volume and required processing time for verifications always increases. This is already causing intense debates.

Bitcoin price began the week riding a swell that began during the late hours of Sunday evening, registering a high of $1,063 on the Bitstamp Price Index (BPI).

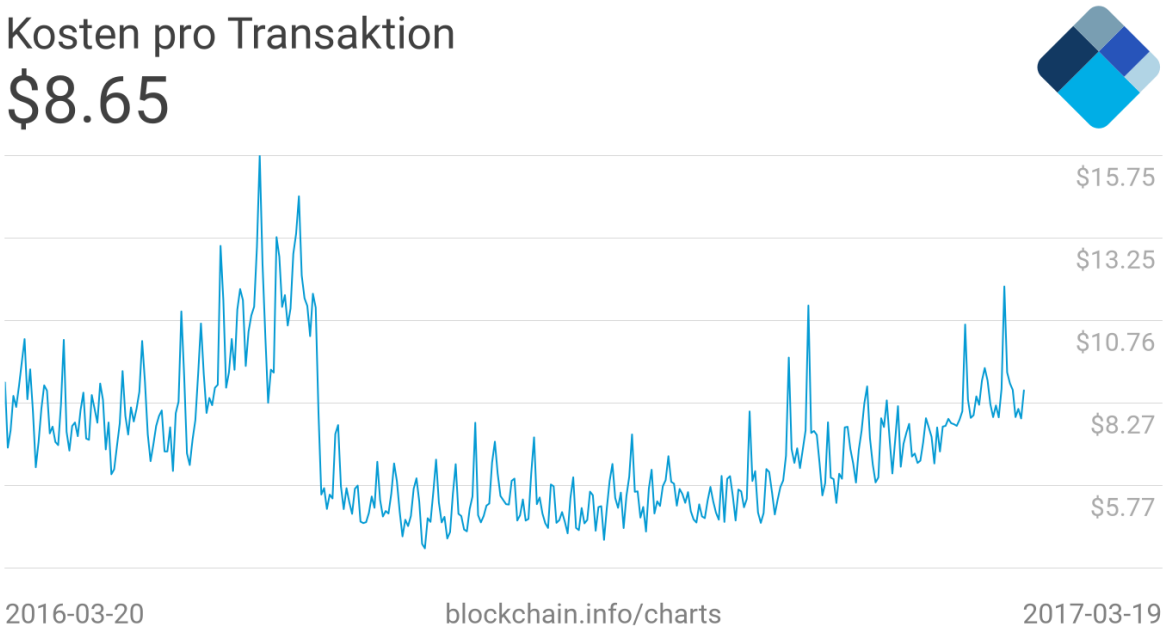
The uncertainty and ongoing debate surrounding bitcoin's scalability solutions with Segregated Witness or SegWit and Bitcoin Unlimited has contributed to significant volatility in the price of the cryptocurrency in recent days.

A hardfork statement toward the end of last week by 18 major bitcoin exchange revealed a contingency plan of listing Bitcoin Unlimited as an alternative cryptocurrency, with its own token. In the immediate aftermath of the collective stance, bitcoin sunk to a 30-day low, losing nearly a fifth of its value as price struck a low of $938 on Saturday.

Rolf Lindemann,
Nok Nok Labs

Weaknesses

- Cost per transaction is relatively high – too high fir micropayments



MINING COST

Total Miners Revenue	
% earned from transaction fees	
% of transaction volume	
Cost per Transaction	7.84 USD

Rolf Lindemann,
Nok Nok Labs

Weaknesses

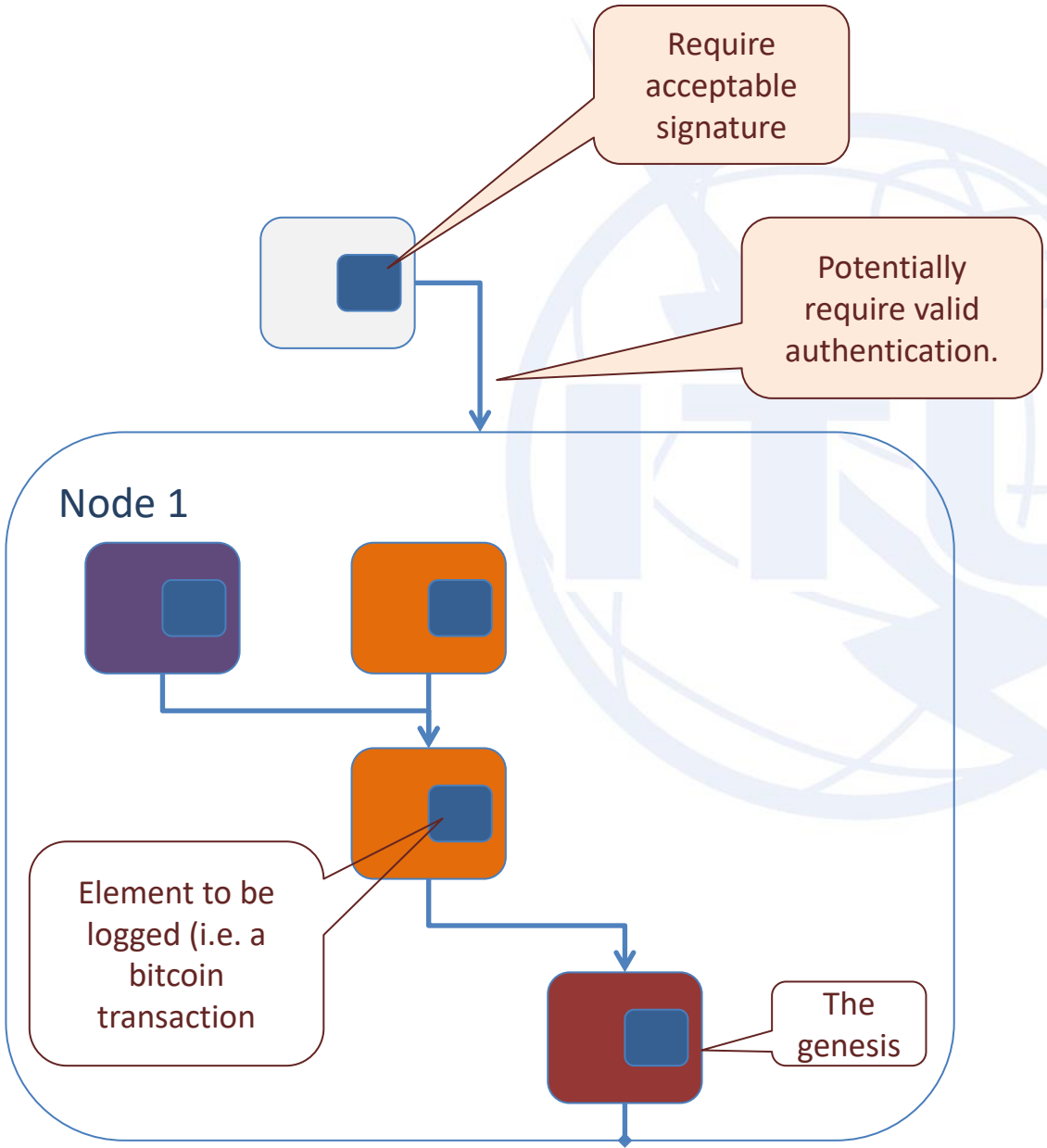
- Equal Rights
  - Assume “Miners Club A“ owns 50% computing power of the Blockchain system.
  - Assume “Miners Club B” owns 30% computing power of the Blockchain systems.
  - Assume “Miners Club C” owns 10% computing power of the Blockchain system
  - Assume all those Miners Clubs decided following a “My Miners Club First” strategy, i.e. whenever some other miner has successfully added a new block N they start adding new blocks ignoring block N.

Opportunities

- Several initiatives (Otonomos, Mirror, Symbiont, Eris/monax.io, …) look into smart contracts.
- Today the rules in Bitcoin and smart contracts cannot easily reflect the strength of a signature (of the block to be written to the blockchain). But we know that in today's world the "Level of Assurance" plays an important role.
- There is a potential of adding attestation (for signing keys) to blockchain.

Rolf Lindemann,
Nok Nok Labs

Opportunities



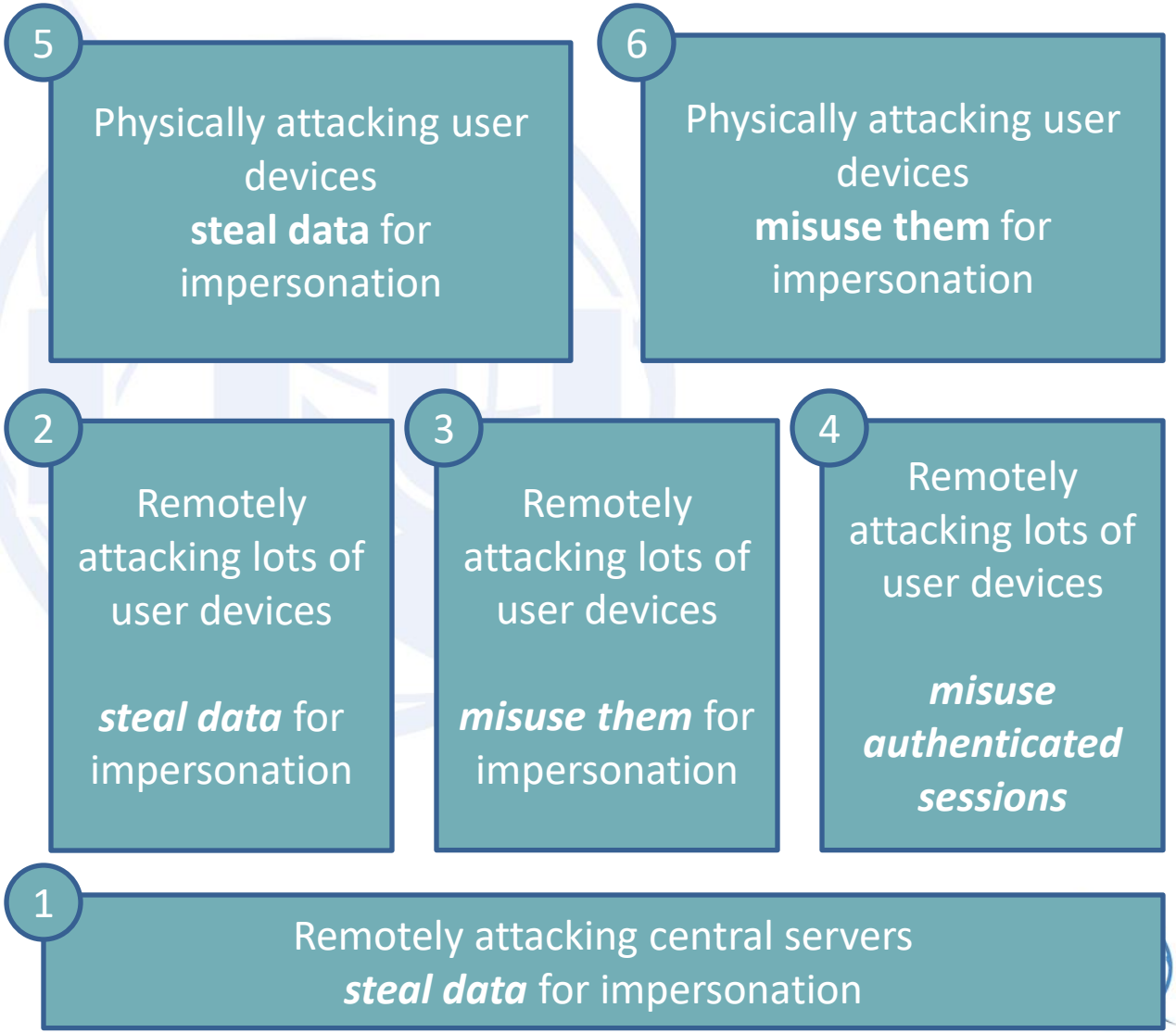
In some environments you might require the signing key to be kept securely or to even involve user approval for signing. So we might want to standardize key attestation for such cases.

Some environments prefer private blockchains (see Hyperledger Fabric, Symbiont, …).
Standardizing authentication will help interoperability.

Attack Classes

Physical attacks possible on lost or stolen devices (≈3% in the US in 2013)

Scalable attacks



The Identity Stack