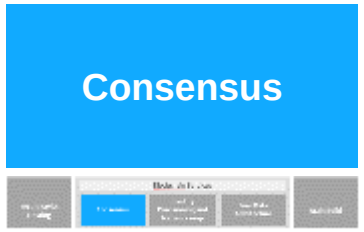
swisscom | Blockchain

Science Brunch 28

Blocker Blockchain aus Sicht eines Telcos

Daniel Haudenschild CEO Swisscom Blockchain AG

Zürich, 13.06.2018



Blockchains work because of trust

Blockchain creates trust through cryptology and immutability of the information encrypted on the blocks of the chain. A user knows, the ”rules” the blockchain uses are secure and cant be manipulated. Only through consensus can the protocol be changed.

Public Blockchain platforms

Public Eg. Bitcoin, Ethereum Homestea

Consensus mechanism

Mining

Private Blockchain platforms

Private Eg. Hyperledger, Ethereum Serenity, Corda

Consensus mechanism

Proof of Stake

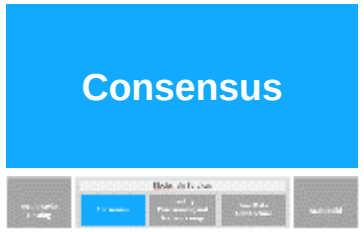
Public blockchains like BitCoin and Ethereum have an ecosystem of miners who validate and the blockchain.

To achieve the consensus to change a public blockchain the mining community plays a large role. They have a significant investment in assuring the continuity of the chain.

In a private blockchain, FinCo and OpCo may use a private chain. The trust in the private chain is based on the consensus required to influence the chain.

The consensus in private chains can be manipulated through dominance of the participants.

swisscom Blockchain

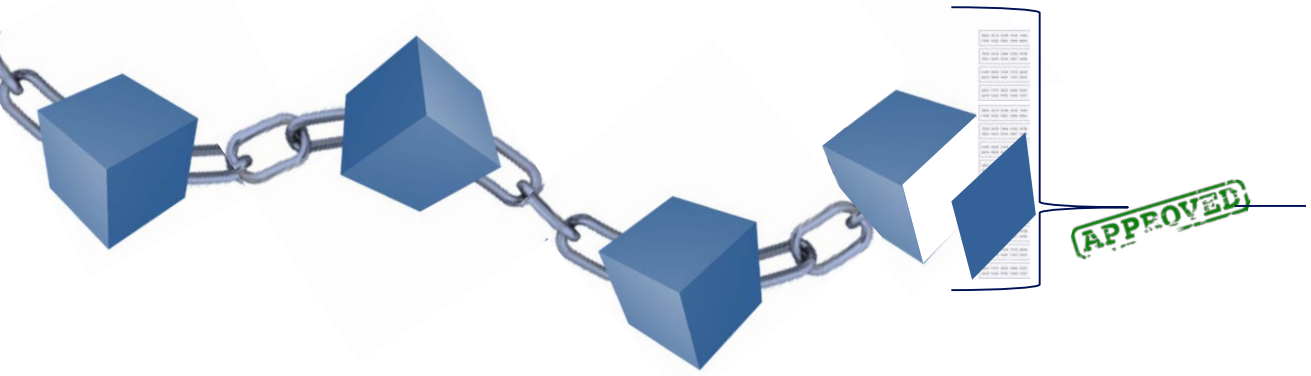


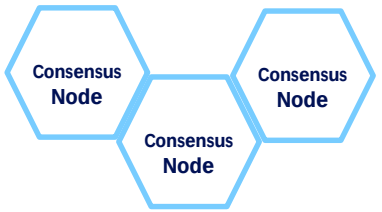
All Private blockchains need a trusted host

Managing consensus is one of the most critical steps in blockchains

Breakdown of a consensus mechanism can render the blockchain platform useless thereby compromising the data recorded on the blockchain. Below are some of the issues that can result when the consensus mechanism fails.

Consensus Nodes :





Validator nodes determine which transactions are immutably captured in the next block

Popular Consensus protocols :

Proof of Stake Eth. (Serenity)

A set of validators take turns proposing and voting on the next block, and the weight of each validator's vote depends on the size of its deposit (i.e. stake).

Proof of Authority Eth. (Serenity)

A PoA scheme is based on the idea that blocks may only be minted by trusted signers

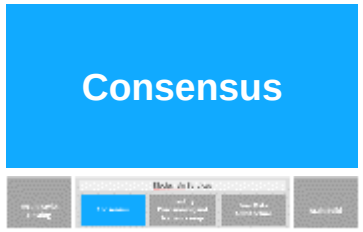
Reputation – (other…)

A reputation including time spent, nodes validated, bounty at risk, and “upvotes” allows for a reputation score.

Byzantine Fault Tolerance – (HyperLedger)

A set of replicated state machines vote to determine validity of the chain and voting by replicas for state changes.

swisscom Blockchain



What's the worst that could happen?

Malicious intent and other critical failures

Achieving consensus in a distributed system is challenging. Consensus algorithms have to be resilient to failures of nodes, partitioning of the network, message delays, messages reaching out-of-order and corrupted messages. They also have to deal with selfish and deliberately malicious nodes.

Consensus Failure

Certain consensus algorithms may not guarantee the ability to reach consensus.

Cheating

Validating nodes either individually or in collusion can independently maintain parallel forks in the blockchain of fraudulent transactions or altered reality that can been provided as proof to the auditor or external third party.

Poor Performance

Based on the design of the consensus algorithm, it may require more time under certain conditions for consensus to converge.

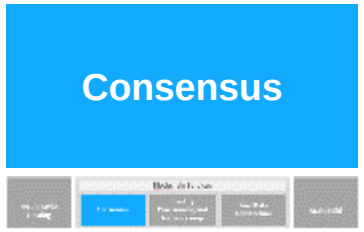
Censoring signer

Another interesting attack vector is if a signer (or group of signers) attempts to censor out blocks that vote on removing them from the authorization list.

Malicious signer

It may happen that a malicious user gets added to the list of signers, or that a signer key/machine is compromised

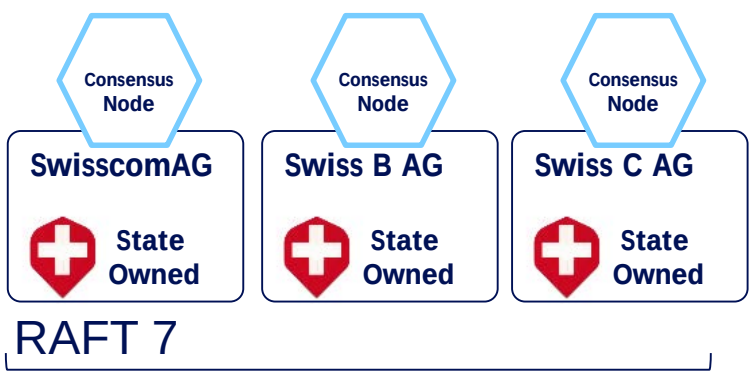
swisscom Blockchain



Hosting «Consensus as a Service»

Swiss hosting significantly reduces blockchain risk

Splitting the critical consensus protocol in several Swiss ICT companies Creates a globally unique asset in Switzerland. The safest blockchain consensus in the world.



Safety

Strong enforcement of rules and strength of the is the consistency of the shared state**.**

Liveliness

Ultra secure as diverse range of infrastructure in multiple locations.

Fault Tolerance

Extremely high redundancy.

Staking identity means voluntarily disclosing who you are in exchange for the right to validate the blocks.

Identity placed at stake serves as a great equalizer, understood and valued the same by all actors.

These companies are majority owned by the Government of Switzerland. The distribution is throughout various data centers and ensures a consensus protocol that is more resilient to malicious attack.

swisscom Blockchain

Work Stream A

Crypto Storage

Swisscom Blockchain has a full overview of secure storage requirements and business needs

Comfort of Deployment

Platform can be deployed in hot/cold storage, has built-in air gapping and integration capabilities.

Faraday Cage

No information on the insides of the appliance can be obtained from the outside through side channels such as audio and magnetic radiations.

Extensibility & Customisability

Using cryptographic agility, appliance can be made to securely store any type of Blockchain wallet.

Tamper-resistance & Resilience

Any attempt to open the appliance to read the secrets result in its automatic erasure.

Auditability

All actions that are performed on the appliance are recorded for audit and traceability.

Availability & Synchronisation

Appliances can be configured in cluster mode for increased performance, availability, and to ensure continuity even in times of attacks on some part of the infrastructure.

Strong authenticity

Any attempt to load or inject malicious software is detected by the platform and triggers alarms.

Work Stream B

Smart Contracts

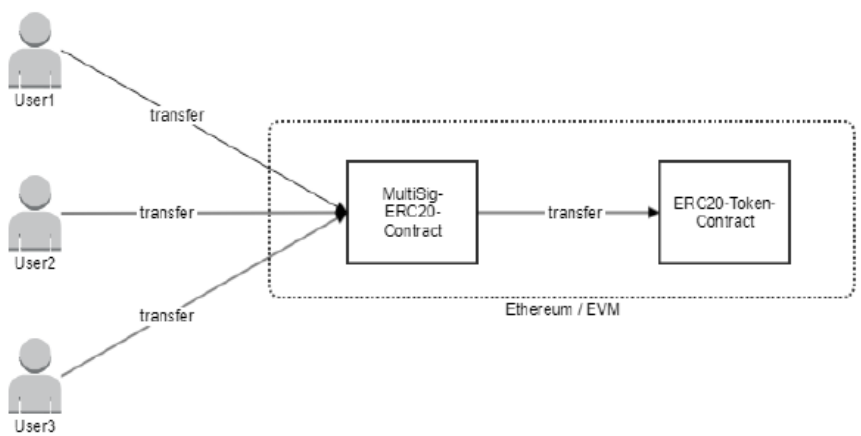
Smart Contract Deliverables - Multi-Sig Contract

Multi Signature contracts can have two different variations that Swisscom Blockchain has extensive experience

Multi Signature ERC20

Multi-Signature for ERC20 Token can be implemented as follow:

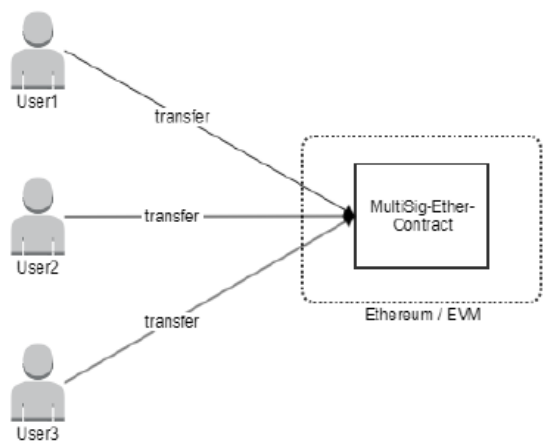
- There is a smart contract "MultiSig-ERC20-Contract" which owns the ERC20 Tokens.
- When there are three transfer transactions to the Multi-Sig Contract then the Multi-Sig contract will transfer the tokens.



Multi Signature Ether

Multi-Signature for Ether transfer can be implemented as follow::

- There is a smart contract "Multi-Sig-Ether-Contract". Which owns Ether.
- When there are three send ether transactions from the owners, the Ether will be sent to the recipient.



Swisscom Blockchain Training and Certification Program

In our Blockchain and Crypto Training we enable your organization in Blockchain and Crypto.

- Your **client facing employees** build up knowledge in order to be able to provide your customers **competent information**.
- Offer your **developers** an **attractive development path** and start building up **deep inhouse competences**.

Get the field experience of applied Blockchain from the Infrastructure leader in Switzerland:

Comprehensive Material

- Up to date course content that is being constantly
- Real world application cases
- Based on our extensive practical experience across industries

Hands-on Methodology

- Interactive learning experience led by a Swisscom Blockchain expert
- Focused on doing
- Sand box environments up and running to enforce your skills

Enterprise Perspective

- Blockchain evaluation with business logic & financial cases
- Constant coordination & alignment to create and provide a selection of topics customized to your goals

Access to Crypto Network

- Get in touch with the best crypto teams in Switzerland
- Learn from the most qualified engineers from the crypto valley
- Become the next best blockchain developer

Blockchain Vault Use Case

Multi-Signatures

- Full support of distributed architectures for load charging and recovery.
- We put all the keys **in the vault** and ensure access to these through dedicated workflows with hardware-assisted **strong authentication**.
- Flexible to use native blockchain multi-sig, smart-contract based, or no blockchain multi-sig.
- Addresses can be reassigned depending on IAM events with no risk of thief, DoS…