Smart Contract Oracles

Nina Minnich and Karoline Rabe

***Abstract*—The abstract goes here.**

I. Introduction

This demo file is intended to serve as a "starter file" for IEEE conference papers produced under LaTeX using IEEEtran.cls version 1.8b and later. I wish you the best of success.

mds
August 26, 2015

II. Methodology

III. Smart Contracts

A. Priciples and Applications

Smart Contracts are scripts, which translate contract clauses into software code and execute them autonomously. Once implemented, these scripts cannot be manipulated, ensuring that the self-enforcement process will proceed according to the predefined rules in a deterministic way. Smart Contracts can ensure an efficient contracting process and reduce transactions costs by replacing the trusted third party, like courts or a notary [1] [2].

Smart Contracts can be used for many different applications. An easy example would be a website which is sold from one contractual party to another. As soon as the purchaser pays price, which was stored in the Smart Contract, it will automatically transfer the property rights of the webiste. If physical objects are included, even a car rental service can be controlled by a Smart Contract. The script would watch if the payments occur in the agreed period and in case the borrower is overdue, the code will block the electronic car key. [3] [4]

B. Blockchain

Subsection text here.

1) Network, Blocks and Mining:

2) Consensus Mechanism: The content of the Blockchain is replicated in the decentralized peer to peer network, therefore all nodes in the network have to find a consensus regarding updates to ensure that only one network state is recognized as "the truth" by all parties. Especially in trustless networks like the Blockchain, special mechanisms have to be found for this purpose. [5]

Proof of Work was the consensus mechanism used for Bitcoin. It means that some nodes in the network, the so called miners, have to solve cryptographical puzzles based on hash functions. There are CPU and memory based PoW variants but both have in common, that the solving time can be adapted by choosing the difficulty of the puzzle. No matter if the miners have to spend CPU cycles or wait for memory queries, PoW consumes always a decent amount of ressources, which is the main drawback of this consensus mechanism. [5] [6] *Proof of Stake* on the other hand is much less expensive than PoW regarding energy consumption because the puzzle's difficulty is adapted on the miner's stake in the network. The stake measures the participation in the Blockchain network and is mostly expressed by the amount of coins, that a miner holds in the respecive cryprocurrency. Alternatively, there is also *Proof of Burn*, where miners have to burn coins in order to mine new blocks and add new content to the Blockchain. Burning means sending money to an address where it cannot be spent. [5]

The presented consensus mechanisms are suitable for public Blockchains, but there are also other architectures, which are based on private Blockchains or decentralized networks with some trusted parties. Especially for the last-mentioned, easier consensus mechanisms can be implemented, like *Proof of Authority*, where the trusted parties update the Blockchain alternatly. In private Blockchains, where nodes are authenticated and a minimum of trust is assumed, communication based protocols like PBFT can be used, where all participants in the network have a right to vote and the consensus is reached through multiple voting rounds. [5]

C. Technical Structure

Subsubsection text here.

D. Data Feeds and Processing

IV. Oracles

V. Conclusion

The conclusion goes here.

Acknowledgment

The authors would like to thank...

References

[1] T. H. Meitinger, "Smart contracts."

[2] M. B. C. T. C. Spancken, Marius; Hellenkamp, "Kryptblockchain und smart contracts," Master's thesis, FH Mnster University of Applied Sciences, 2016.

[3] A. Jung, Reinhard; Plazibat, "Blockchain: Heiliger gral oder berbewerteter hype? erkenntnisse aus der finanzindustrie," September 2017. [Online]. Available: https://elibrary.vahlen.de/10.15358/0935-0381-2017-K-46.pdf

[4] L. Lee, "New kids on the blockchain: How bitcoins technology could reinvent the stock market," *Hastings Business Law Journal*, vol. 12, no. 2, 2016.

[5] R. Z. M. C. G. O. B. C. W. J. Dinh, Tien Tuan Anh; Liu, "Untangling blockchain: A data processing view of blockchain systems," ???

[6] S. Golze, "Fairness in berlastsituationen mittels proof-of-work funktionen," phdthesis, Technische Universitt Berlin, Jun. 2009.