

BITSHARES 2.0: CONSENSUS MECHANISM

Fabian Schuh, Daniel Larimer
Cryptonomex, Cryptonomex.com*

Blacksburg (VA), USA

{fabian, dan}@cryptonomex.com

Abstract—

1 Introduction

2 Delegated Proof-of-Stake (DPOS)

<https://github.com/cryptonomex/graphene/wiki/witness-rng>
<https://github.com/cryptonomex/graphene/wiki/witness-scheduler>

3 Transactions as Proof-of-Stake (TaPOS)

4 Distinction from Traditional Consensus Schemes

5 Attack Vectors

6 Conclusion

Litarture

References

- [1] Investopedia, “Contract for Difference,” <http://www.investopedia.com/terms/c/contractfordifferences.asp>.
- [2] “MF Global,” <http://www.forbes.com/sites/francinemckenna/2012/07/16/auditors-all-fall-down-pf-gbest-and-mf-global-frauds-reveal-weak-watchdogs/>.
- [3] “Mt. Gox,” <http://www.wired.com/2014/03/bitcoin-exchange/>.
- [4] “Bitstamp,” <http://www.coindesk.com/bitstamp-claims-roughly-19000-btc-lost-hot-wallet-hack/>.
- [5] “Bitcoin Exchange BitFinex’ Hot Wallet Hacked,” <https://www.cryptocoinsnews.com/breaking-bitcoin-exchange-bitfinex-hot-wallet-hacked/>.
- [6] “Coinbase,” <http://coinbase.com>.
- [7] “Coinbase case demonstrates the pitfalls of regulatory compliance,” <http://cointelegraph.com/news/112319/coinbase-case-demonstrate-the-pitfalls-of-regulatory-compliance>.
- [8] “Is Coinbase Bringing ‘Big Brother’ to Bitcoin Accounts?” <https://www.cryptocoinsnews.com/coinbase-bringing-big-brother-bitcoin-accounts/>.
- [9] D. Larimer, “Stable currencies are impractical and undesirable,” <http://bytemaster.github.io/article/2014/12/31/Stable-Crypto-Currencies-are-Impossible/>.
- [10] Wikipedia, “Alternative Trading System,” http://en.wikipedia.org/wiki/Alternative_trading_system.
- [11] —, “Prediction Market,” http://en.wikipedia.org/wiki/Prediction_market.
- [12] Daniel Larimer, “Creating a Fiat/Bitcoin Exchange without Fiat Deposits,” <https://bitcointalk.org/index.php?topic=223747.0>.
- [13] —, “Overpaying for Security,” <http://letstalkbitcoin.com/is-bitcoin-overpaying-for-false-security/#.Ui-p9WTFT7s>.
- [14] —, “Bitcoin and the Three Laws of Robotics,” <http://letstalkbitcoin.com/bitcoin-and-the-three-laws-of-robotics/>.
- [15] Adam Ernest, “Follow My Vote,” <http://followmyvote.com>.
- [16] Cédric Cobban, “Follow My Vote,” <http://peertracks.com>.
- [17] “DACPlay,” <http://dacPLAY.org>.
- [18] Ripple Labs, “Multisig / Transaction Proposal,” https://wiki.ripple.com/Multisig#Transaction_Proposal.
- [19] Oleg Andreev, “Blind signatures for Bitcoin transactions (second draft),” <http://oleganza.com/blind-ecdsa-draft-v2.pdf>.
- [20] Federal Reserve Bank of St. Louis, “Dataset: St. Louis Adjusted Monetary Base (AMBSL),” <https://research.stlouisfed.org/fred2/series/AMBSL/downloaddata?cid=124>, Aug. 2015.
- [21] “The trade is the settlement,” <http://t0.com/>.
- [22] “BitShares 2.0: General Documentation,” *BitShares Whitepapers*, 2015.
- [23] “BitShares 2.0: Financial Smart Contract Platform,” *BitShares Whitepapers*, 2015.
- [24] “BitShares 2.0: Distributed Consensus,” *BitShares Whitepapers*, 2015.
- [25] “BitShares 2.0: Growth Considerations,” *BitShares Whitepapers*, 2015.
- [26] “BitShares 2.0: Historical Overview,” *BitShares Whitepapers*, 2015.
- [27] “BitShares 2.0: Identity Management,” *BitShares Whitepapers*, 2015.

*This work was supported by Cryptonomex and honorable members of the bitsharestalk.org community.