SJSU SAN JOSÉ STATE UNIVERSITY

SJSU Undergraduate Research Grants

SharedWealth: Disincentivizing Pool Mining

Sonja Boytcheva Thomas Austin

Dept. Of Computer Science, College Of Science

Abstract

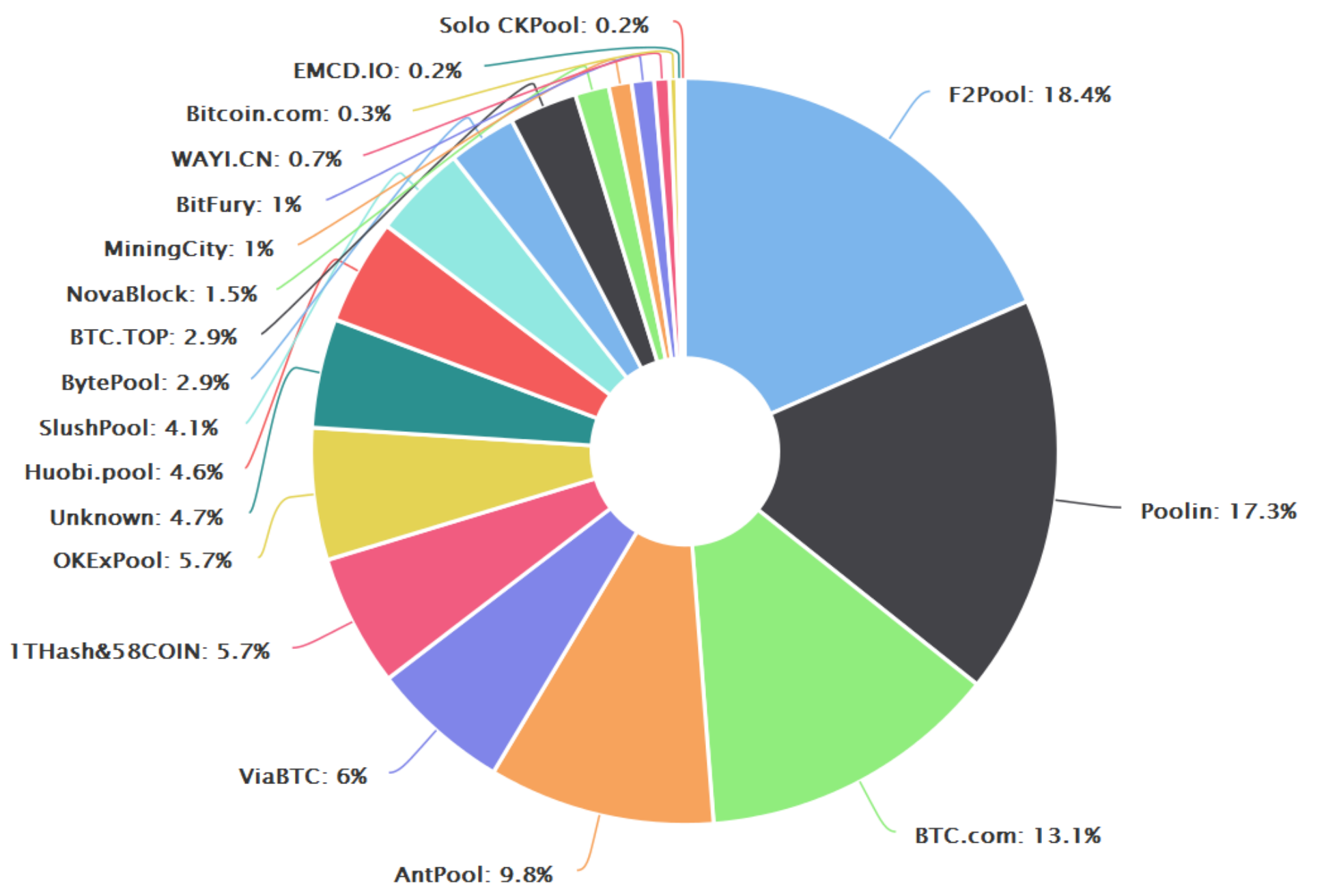
One of the main goals of the Bitcoin cryptocurrency is decentralization, in order to ensure that no single entity within the network is too powerful. However, Bitcoin utilizes a winner-takes-all reward scheme, which results in a high irregularity in reward payouts among solo miners. This has led to the formation of mining pools, which provide more regular payouts for miners, but at the cost of centralization of the network. This project aims to provide an open-source framework to model an alternate block reward scheme, SharedWealth, which makes payout more regular among miners without the need for mining pools to form.

Project Activities

- Simulate mining pools in a Bitcoin-like cryptocurrency
- Build an open source framework, SpartanGold, to model this cryptocurrency: https://github.com/antimony123/spartan-gold
- Develop a revised protocol, SharedWealth, which models a burn-and-mint alternative to Bitcoin's winner-takes-all approach
- Fork the SpartanGold codebase to simulate the SharedWealth protocol

Mining Pools

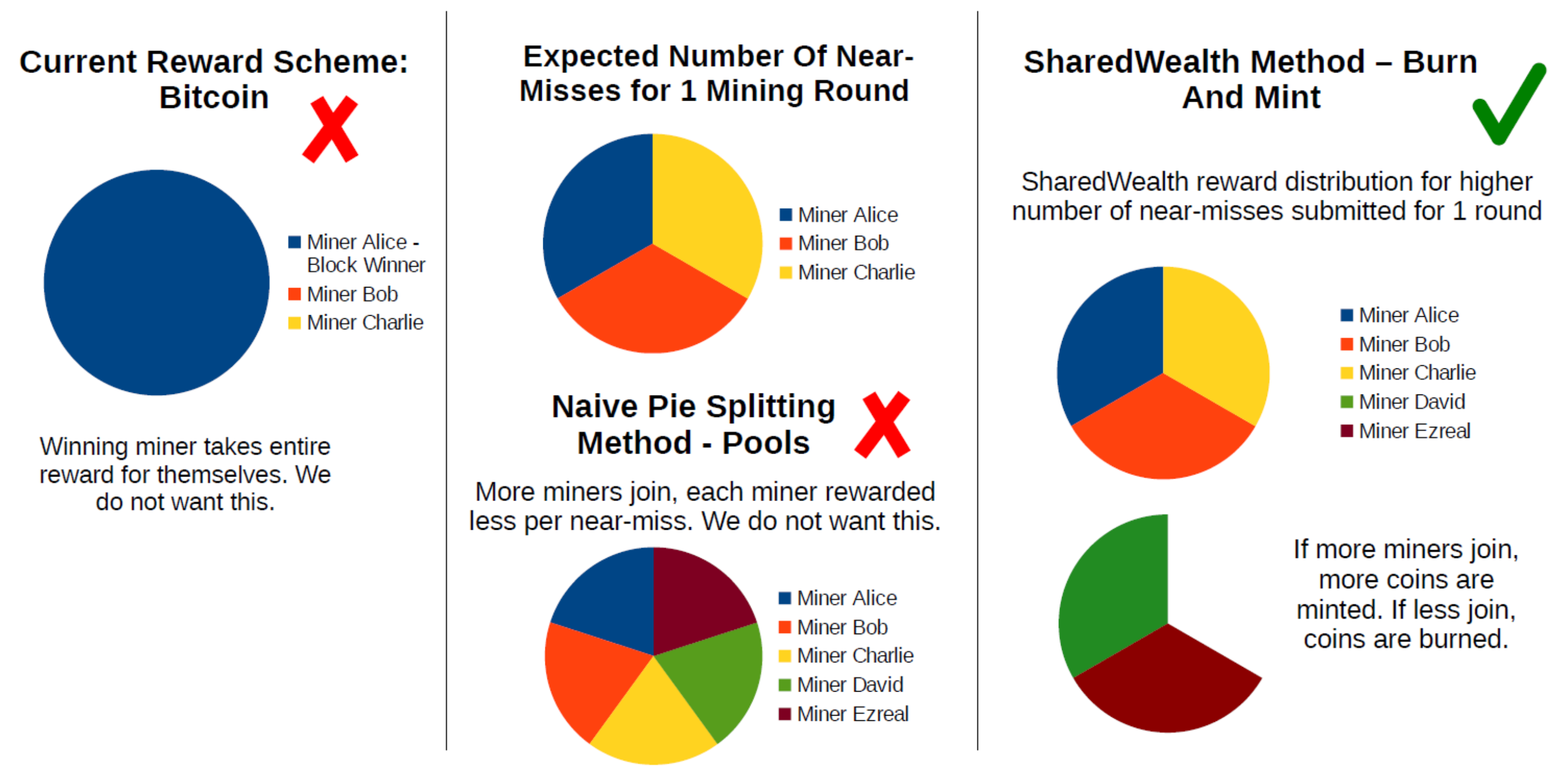
- Bitcoin's winner-takes-all reward scheme creates uneven payout for miners
- Miners pool their hash rates together to guarantee a steadier payout
- However, this reduces decentralization



Source: blockchain.info/pools

  - Currently, the top 4 Bitcoin mining pools control more than 50% of the hash rate.
- This centralization could undermine the stability and trust of the network
  - For instance, a single pool can decide to censor transactions (feather forking)

Reward Schemes



Current Reward Scheme: Bitcoin

Winning miner takes entire reward for themselves. We do not want this.

Expected Number Of Near-Misses for 1 Mining Round

Naive Pie Splitting Method - Pools

More miners join, each miner rewarded less per near-miss. We do not want this.

SharedWealth Method – Burn And Mint

SharedWealth reward distribution for higher number of near-misses submitted for 1 round

If more miners join, more coins are minted. If less join, coins are burned.

Research Questions

- How regular are payouts in a winner-takes-all system, e.g. Bitcoin?
- How are mining rewards distributed among miners when pool mining?
- What alternate reward schemes, different from winner-takes-all, will more evenly distribute rewards among miners?
- Can we achieve a similar payout regularity with SharedWealth?
- Is SharedWealth vulnerable to coin hopping attacks?

Citations

S. Nakamoto. Bitcoin, A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf. Oct 31 2008.

M. Rosenfeld. Analysis of Bitcoin Pooled Mining Reward Systems. https://arxiv.org/abs/1112.4980. Dec 22 2011.

A. Miller, et. al. Nonoutsourceable Scratch-Off Puzzles to Discourage Bitcoin Mining Coalitions. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 680–691.

J. Bonneau, et. al. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In 2015 IEEE Symposium on Security and Privacy, pp. 104-121.