Zold: A New Cryptocurrency

Green Paper

Yegor Bugayenko
yegor256@gmail.com
www.zold.io

0.4.0

June 28, 2018

In the last few years digital currencies have successfully demonstrated their ability to become an alternative financial instrument in many different markets. Most of the technologies available at the moment are based on the principles of Blockchain architecture, including dominating currencies like Bitcoin and Etherium. Despite its popularity, Blockchain is not the best possible solution for all scenarios. One such example is for fast micro-payments. Zold is an experimental alternative that enables distributed transactions between anonymous users, making micro-payments financially feasible and fast. It borrows the "proof of work" principle from Bitcoin, and suggests a different architecture for digital wallet maintenance.

The Market

Since its release in 2009, Bitcoin from "a libertarian fairy tale" and "a simple Silicon Valley exercise in hype" turned into "a catalyst to reshape the financial system in ways that are more powerful for individuals and businesses alike," according to Andreessen in "Why Bitcoin Matters." Even though Cheah et al. argues in "Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin" that "the fundamental value of Bitcoin is zero," it seems that "the question is not whether Bitcoin has value; it already does," according to Van Alstyne. "The question is whether the efficiencies of a cybercurrency like Bitcoin can be merged with the certainties of an honest central bank," they said in "Why Bitcoin Has Value."

The core component of Bitcoin is Blockchain technology, which "ensures the elimination of the double-spend problem, with the help of public-key cryptography" and "coins are transferred by the digital signature of a hash," explains Pilkington in "Blockchain Technology: Principles and Applications." Very soon after Bitcoin was created, similar products were introduced, which were also based on the principles of Blockchain, such as Etherium by Buterin, presented in *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.*

Even though Blockchain is a sound solution to the double-spending problem, there could be other solutions, including different "proof-of-X" alternatives.For example, Everaere et al. gave a summary of them and introduced their own in "Double Spending Protection for E-cash Based on Risk Management," Boyen et al. described "a truly distributed ledger system based on a lean graph of cross-verifying transactions" in *Blockchain-free Cryptocurrencies: A Framework for Truly Decentralised Fast Transactions*, recently IOTA, a "tangle-based cryptocurrency," was launched by Popov and explained in "The Tangle," Hashgraph claims in their *Hedera Hashgraph White Paper* to be "the world's first mass-adopted public distributed ledger", and so on.

The Problems

Zold is also a decentralized digital currency that maintains its ledgers through an unpredictable amount of anonymous and untrustable server nodes, trying to guarantee data consistency. The architecture of Zold is not Blockchain-based. The development of Zold was motivated by the desire to overcome two obvious disadvantages present in the majority of all existing cryptocyrrencies:

The first problem is that transaction processing is rather slow. Current rates for Bitcoin processing speed is 7 transactions per second (tps) while Paypal handles an average of 115 tps and the VISA network has a peak capacity of 47,000 tps. Karame et al. says in "Double-spending Fast Payments in Bitcoin" that "Bitcoin requires tens of minutes to verify a transaction and is therefore inappropriate for fast payments." It is inevitable, since "processing speed is at odds with the security aspects of the underlying proof-of-work based consensus mechanism" according to "Speed-Security Tradeoffs in Blockchain Protocols" by Kiayias et al. Ethereum, according to "Comparing Bitcoin and Ethereum" by Fekkes et al., can process "two times more transactions per second than Bitcoin is able to do," but this still is rather slow.

The second problem, as noted by Popov in "The Tangle," is that "it is not easy to get rid of fees in the blockchain infrastructure since they serve as an incentive for the creators of blocks." Möser et al. says in "Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees" that "Bitcoin users are encouraged to pay fees to miners, up to 10 cents (of USD) per transaction, irrespective of the amount paid" which especially hurts when transaction amounts are smaller than a dollar. Moreover, according to "Near Zero Bitcoin Transaction Fees Cannot Last Forever" by Kaskaloglu, "an increase in transaction fees of Bitcoin is inevitable."

Thus, the speed is low and the processing fees are high. Zold was created as an attempt to resolve these two problems.

The Features

Unlike all other crypto currencies, there is no central ledger in Zold. Each wallet has its own personal ledger. All transactions in each ledger are confirmed by RSA signatures of their owners.

Similar to many other digital currencies—including Bitcoin, Etherium, Monero, Trinity, Plancoin, Dero, and many others—Zold nodes find consensus by using the CPU power invested by each of them to perform certain expensive and meaningless calculations that result in finding hash suffixes, also known as "proof-of-work."

Zold is a pre-mined digital asset, similar to Ripple, Cardano, Stellar, EOS, NEO, Loki, and many others. One currency unit is called ZLD. Therefore, the technical capacity of the currency is 2,15 billion ZLD. To compare, the total supply of some crypto currencies is: Bitcoin: 21m BTC, Ripple: 100b XRP, Litecoin: 84m LTC, Dash: 19m DASH.

Zold has two obvious advantages comparing to many other similar solutions: it is fast and cheap. First, the speed of transaction processing literally has no limits, because all payments are made locally, on users' machines. Second, the cost of transaction processing is lower than most other payment systems can offer. To process a thousand transactions a user has to pay $500 in Bitcoin and $300 in Ethereum, while in Zold it is as little as $4.

There are more technical details available in the White Paper.