Zold: A New Cryptocurrency

Green Paper

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

0.6.0

July 1, 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 Ethereum. 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, explained in details in the White Paper.

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. Even though Cheah et al. argues 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."

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. Very soon after Bitcoin was created, similar products were introduced, which were also based on the principles of Blockchain, such as Ethereum by Buterin.

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, Boyen et al. described "a truly distributed ledger system based on a lean graph of cross-verifying transactions," recently IOTA, a "tangle-based cryptocurrency," was launched by Popov, Hedera claims 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 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 Kiayias et al. Ethereum, according to 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, 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 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 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 mostly at the market of micro payments.

The Features

First, 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. This enables high scalability and performance.

Second, similar to many other digital currencies, including Bitcoin, Ethereum, Monero, 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," initially introduced by Back in 1997. This guarantees data consistency and eliminates a possibility of double-spending.

Third, Zold is a pre-mined digital asset, similar to Ripple, Cardano, Stellar, NEO, and many others. Zold algorithmically limits its total supply, which is 2,15 billion ZLD. To compare, the total supply of some other currencies is: 21m in Bitcoin, 100b in Ripple, 84m in Litecoin, and 19m in Dash. Bohr et al. explains that cryptocurrencies limit their total suply in order "to protects against inflationary forces," so does Zold in order to protect its market value.

Forth, the speed of transaction processing in Zold literally has no limits, because all payments are made locally, on users' machines and then pushed to the network for merging and storing.

Fifth, the cost of transaction processing is lower than what most other payment systems can offer. To process a thousand transactions a user has to pay (approximately) $500 in Bitcoin, $300 in Ethereum, $45 in Litecoin, $12 in Ripple, and $9 in Bitcoin Cash. In Zold it is as little as $4, which makes it one of the most cost effective cryptocurrencies.

The Roadmap

Zold is a GitHub-hosted open source software product, just like most other cryptocurrencies. Its first experimental version was created and launched by Yegor Bugayenko, the CEO of Zerocracy, on May 27, 2018. A distributed network of nodes, which are running Zold software, is maintained by anonymous volunteers. The development of further versions and the maintenance of existing ones depends on the activity of GitHub contributors, partially sponsored by Zerocracy, Inc.

Just like SEC chairman Jay Clayton recently mentioned, "cryptocurrencies like Bitcoin are not securities." Similar to Bitcoin and Ethereum, ZLD is a cryptocurrency, not a security. It is distributed by Zerocracy as a digital gift to those who actively contribute to Zerocracy ecosystem, the development of Zold software, and the maintenance of nodes.

Aside from programming, Zold enthusiasts may contribute their monetary assets, like US dollars, to any project managed by Zerocracy. In exchange, they get rewarded with ZLD digital coins. Later, they are able to trade their ZLD coins to other digital currencies and fiat money, through exchanges or directly.

It is assumed that the market price of ZLD will grow due to its technical advantages and the popularity of Zerocracy platform among programmers and software companies.