Zold: A Fast Cryptocurrency for Micro Payments

Yegor Bugayenko
yegor256@gmail.com

May 28, 2018

Abstract

In the last few years digital currencies 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 the dominating currencies like Bitcoin and Etherium. Despite its popularity, Blockchain is not the only possible solution and is not the best for fast micro-payments. Zold is an *experimental* alternative that enables distributed transactions between anonymous users, making micro-payments financially feasible. It borrows the "proof of work" principle from Bitcoin, and suggests a different architecture for digital wallets maintenance.

1 Motivation

Bitcoin, the first decentralized digital currency, was released in January 2009 (Nakamoto 2008). During a few following years "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 (2014). At the moment, as Van Alstyne (2014) claimed, "the question is not whether Bitcoin has value; it

already does. 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 the 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" (Pilkington 2016). Very soon after the Bitcoin invention similar products were introduced, which were also based on the principles of Blockchain, such as Etherium (Buterin 2013).

Even though Blockchain is a sound solution of the double-spending problem, there could be other solutions, including different "proof-of" alternatives.[1] For example, Everaere et al. (2010) gave a summary of them and introduced their own; Boyen et al. (2016) described "a truly distributed ledger system based on a lean graph of cross-verifying transactions"; recently IOTA, a "tangle-based cryptocurrency," was launched (Popov 2017).

Zold also is a decentralized digital currency that maintains its ledgers at an unpredicable 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 of the majority of all existing cryptocyrrencies:

The first problem is that transaction processing is rather slow.[2] Karame et al. (2012) 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. (2015).

The second problem, as noted by Popov (2017), 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." As per Möser et al. (2015), "Bitcoin users are encouraged to pay fees to miners, up to 10 cents (of USD) per transaction,

[1] `https://goo.gl/aqzf2Q`: "Proof-of-Burn": instead of bringing the money together into computer equipment, the owner burns the coins. Here the coins to the address where they are irretrievable. By doing this, the owner gets a privilege to mine on the system. "Proof-of-Stake": the coins exist from the start, and the validators get a reward in the form of transaction fees. "Proof-Of-Capacity": one pays with the hard drive space. The more is the hard drive space; the more is the probability of mining the next block and earning a reward. "Proof-of-Elapsed-Time": one uses Trusted Execution Environment or TEE to ensure a random looter production.

[2] `https://goo.gl/sWiAWc`: "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 (though it currently needs 2000-4000 tps)."

irrespective of the amount paid" which especially hurts when transaction amounts are smaller than a dollar. Moreover, according to Kaskaloglu (2014), "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 of existing Blockchain-based digital currencies.

2 Principles

No General Ledger. 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. Section 4 explains how it works.

Proof of work. Similar to many other digital currencies—including Bitcoin, Etherium, Plancoin, Monero, Trinity, Plancoin, Dero, and many others—Zold nodes find consensus by comparing the amount of CPU power invested by each of them into finding hash suffixes, performing certain expensive and meaningless calculations. Section 3 describes the algorithm being used.

Root Wallet. Zold is a pre-mined[3] digital asset, similar to Ripple,[4] Cardano, Stellar,[5] EOS, NEO, Loki,[6] and many others. The only way to get ZLD is to receive it from someone else. The root wallet belongs to the issuer and

[3] `https://goo.gl/QBhbcT`: "A premine or instamine is where the developer or developers don't release the crypto currency in what can be considered a fair manner. Even Bitcoin can be considered to be instamined to a certain extent. A premine is where a developer allocates a certain amount of currency credit to a particular address before releasing the source code to the open community."

[4] `https://goo.gl/XAtPH8`: "When the Ripple network was created, 100 billion XRP was created. The founders gave 80 billion XRP to the Ripple Labs. Ripple Labs will develop the Ripple software, promote the Ripple payment system, give away XRP, and sell XRP."

[5] `https://goo.gl/CnQQwA`: "The stellar network started with 100 billion lumens. There is a 1% p.a. inflation, hence the current total of roughly 103.5 billion lumens. About 18 billion lumens are on the market and the other 85 is held by the stellar development foundation."

[6] `https://goo.gl/By5CR3`: "Over 7 million Loki is held in escrow for the Founder, Advisor, and Seed allocations. The Founder and Advisor allocations follow a 12 month lockup schedule, where 25% of each allocation is released every 90 days following mainnet launch. The allocations to Founders and Advisors are remuneration for services rendered to the LAG Foundation Ltd. The Seed allocation follows a similar schedule, with a 30% initial release and 20% every 90 days until the final release of 10%."

may have a negative balance, which can grow according to a pre-defined restrictive formula, explained in Section 5. All other wallets may only have positive balances.

Taxes. Unlike many other payment systems, Zold doesn't require its users to pay transaction fees. Instead, wallets have to pay regular "taxes" for the service of their maintenances. Taxes amounts depend on the amount of transactions in a wallet and the age of the wallet. Section 6 provides more details.

No Trust. The network of communicating nodes maintains wallets of users. Anyone can add a node to the network. It is assumed that any node may contain corrupted data, either by mistake or intentionally. Section 7 explains how nodes communicate and rate each other.

Open Source. Zold is a command line tool. Its entire code base is open source and hosted at the GitHub yegor256/zold repository.

Capacity. One currency unit is called ZLD. One ZLD by convention equals to 2^{32} *zents* (4,294,967,296). All amounts are stored as signed 64-bit integers. Thus, the technical capacity of the currency is 2,147,483,648 ZLD (two billion).[7]

Hexspeak. Wallet ID is a 16-digit hexadecimal number, which is not restricted by any formula. A user may make up any number, even using Hexspeak.

3 Proof of Work

The system consists of nodes (server machines), which maintain the data. In order to guarantee data consistency among all distributed nodes there has to be an algorithm of data segregation. Corrupted data must be detected earlier and filtered out as quickly as possible. Bitcoin introduced such an algorithm and called it *proof of work* (Nakamoto 2008).

Its fundamental principle is that each block of data must have a special number attached to it, known as *nonce*, which is rather difficult to calculate, because it requires a lot of CPU power. It is assumed that at any moment of time the majority of nodes in the network invest their CPU power into

[7]To compare, the total supply of some crypto currencies is: Bitcoin: 21m BTC, Ethereum;: 100m ETH, Ripple: 100b XRP, Litecoin: 84m LTC, Cardano: 31b ADA, Stellar: 103b XLM, NEO: 100m NEO, Dash: 19m DASH.

calculating the nonces for the data that is not corrupted. If and when for any reason some data gets corrupted, the amount of CPU power a part of the network decides to invest into its nonces calculation would be smaller than what the other part of the network invests into legal data. The latter part will quickly dominate the former and the nodes with corrupted data will be ostracized and eventually ignored (Nakamoto 2008).

Zold has borrowed this principle, although modified it. It also requires its nodes to invest their CPU power into meaninless and repetative calculations just to help us identify which part of the network they belong to: corrupted or not. Each Zold node has to calculate its *score*, which is as big as much CPU power the node has invested into its calculation.

Similar to Bitcoin nonces, Zold nodes repeatedly calculate cryptographic hashes, looking for consecutive zeros inside them. First, in order to calculate a score, a node makes the *prefix*, which consists of four parts, separated by spaces:

1. The current timestamp in UTC, in ISO 8601,
2. The host name or IP address, e.g. `b2.zold.io`,
3. The TCP port number,
4. The invoice.

For example, the prefix may look like this:

```
2018-05-17T03:50:59Z b2.zold.io 4096 THdonv1E@abcdabcdabcdabcd
```

Then, the node attempts to append any arbitrary text, which has to match `/[a-zA-Z0-9]+/` regular expression, to the end of the prefix and calculates SHA-256 hash of the text in the hexadecimal format. For example, this would be the prefix with the attached `16bda66` suffix:

```
2018-05-17T03:50:59Z b2.zold.io 4096 THdonv1E@abcdabcdabcdabcd
↪  16bda66
```

The hash of this text will be (pay attention to the trailing zeroes):

```
5fa0681f220a2779b03b46456a19b38c0b635c1573dc01401dafee510000000
```

The node attempts to try different sufficies until one of them produces a hash that ends with a few tailing zeroes. The one above ends with six zeroes.

When the first suffix is found, the score is 1. Then, to increase the score by one, the next suffix has to be found, which can be added to the first 64 characters of the previous hash in order to obtain a new hash with trailing zeros, for example:

```
2018-05-17T03:50:59Z b2.zold.io 4096 THdonv1E@abcdabcdabcdabcd
 ↪  16bda66 13d284b
```

Produces:

```
ce420bfdd2f6530db795e7ff4aa508bb0092735dd63d209da218cb78b000000
```

And so on.

The score is valid only when the starting time point is earlier than the current time, but not earlier than 24 hours ago. The *strength* of the score is the amount of the trailing zeros in the hash. In the example above the strength is six. The larger the strength, the more CPU power it takes to earn the score. All nodes in the network must have the same strength of their scores.

4 Wallets

There is no central ledger in Zold, like in many other digital currencies. Instead, each user has their own *wallets* (any number of them) with their own ledgers inside. Each wallet is an ASCII-text file with the name equal to the wallet ID. For example, the wallet in the file `12345678abcdef` may include the following text:

```
zold
0.6.4
12345678abcdef
AAAAB3NzaC1yc2EAAAADAQABAAABAQCuLuVr4Tl2sXoN5Zb7b6SKMPrVjLxb...
```

```
003a;2017-07-19T21:24:51Z; ffffffff9c0ccccd; Ui0wpLu7;
↪  98bb82c81735c4ee; For services;SKMPrVj...
003b;2017-07-19T21:25:07Z; fffffffffa72367; xksQuJa9;
↪  98bb82c81735c4ee; For food;QCuLuVr4...
0f34;2017-07-19T21:29:11Z; 0000000000647388; kkIZo09s;
↪  18bb82dd1735b6e9; -;
003c;2017-07-19T22:18:43Z; fffffffff884733; pplIe28s;
↪  38ab8fc8e735c4fc; For programming;2sXoN5...
```

Lines are separated by either CR or CRLF. There is a header and a ledger, separated by an empty line. The header includes four lines:

1. Network name, `[a-z]{4,16}`;
2. Software version, `[0-9]+(.[0-9]+){1,2}` (semantic versioning);
3. Wallet ID, a 64-bit unsigned integer in hexadecimal format;
4. Public RSA key of the wallet owner, in Base64.

The ledger includes transactions, one per line. Each transaction line contains fields separated by a semi-colon:

1. `id`: Transaction ID, an unsigned 16-bit integer, 4-symbols hex;
2. `time`: date and time, in ISO 8601 format, 20 symbols;
3. `amount`: Zents, a signed 64-bit integer, 16-symbols hex;
4. `prefix`: Payment prefix, 8-32 symbols;
5. `bnf`: Wallet ID of the beneficiary, 16-symbols hex;
6. `details`: Arbitrary text, matching `/[a-zA-Z0-9 -.]{1,512}/`;
7. `signature`: RSA signature, 684 symbols in Base64.

Transactions with positive amount don't have signatures. Their IDs point to ID fields of corresponding beneficiaries' wallets.

The `prefix` is a piece of text randomly selected from the RSA key of the beneficiary wallet. It is used for security reasons, in order to make impossible

"wallet masquerading" (pushing a new wallet with the same ID, but a different key).

The combination `id` + `bnf` must be unique in the entire wallet.

The RSA signature is calculated using the private key of the wallet and the following fields of transaction, separated by spaces: `bnf`, `id`, `time`, `amount`, `prefix`, `bnf`, `details`.

For example, this text may be used as a signing input:

```
12345678abcdef 003a 2017-07-19T21:24:51Z ffffffff9c0ccccd
↪  Ui0wpLu7 98bb82c81735c4ee For services
```

Each transaction takes 1284 symbols at most.

The order of transactions is not important, as long as their final balance is positive.

5 Mining Formula

The only way to get ZLD is to receive it from the *root* wallet with a system pre-defined ID `0000000000000000`. This wallet is the only one that may have a negative ballance. However, to prevent an uncontrolled emission of ZLD, the balance of this wallet must satisfy the formula:

$$t = \frac{h}{24 \times 1024}; \quad z = 2^{63} \times (1 - 2^{-t}).$$

Here h is the age of the root wallet in hours and z is the maximum amount of zents it can issue at that moment. The first six years will look like this:

Year	ZLD	Share
1st	470m	22%
2nd	837m	39%
3rd	1.1b	52%
4th	1.3b	63%
5th	1.5b	71%
6th	1.7b	77%

The limitation is hardwired in Zold software and can't be eliminated.

6 Taxes

Each wallet must have to pay *taxes* in order to be promoted by nodes. The maximum amount of tax debt a node can tolerate is 1 ZLD. This means that if the debt is smaller, all nodes must promote the wallet to their remote nodes. If the debt is bigger, a node will reject the wallet, which will make it impossible to make any new payments from it.

The amount of taxes to be paid is calculated by the following formula:

$$X = A \times F \times T.$$

A is the total age of the wallet, which is calculated as the difference in hours between the current time and the time of the oldest transaction in the wallet. T is the total number of transactions in the wallet. F is the fee per transaction/hour, which is equal to 7.48 zents (a one-year-old wallet with 4096 transactions must pay approximately 16 ZLD taxes annually).

In order to pay taxes the owner of the wallet has to select any remote node from the network, which has a score of 16 or more. Then, it has to take the invoice from the score, request the node to lock the score for a minute, and send the payment of 1 ZLD or less to that node. The score with exactly 16 suffixes has to be placed into the details of the transaction, prefixed by `TAXES `.

The most active remote node will be selected as tax receiver. It's up to the payer which node to select.

All tax payments inside a wallet must have unique scores. Duplicate tax payments are ignored.

7 Remote Nodes

Each node maintains a list of *remote nodes* (their host names and TCP port numbers), their scores and their availability information. When the node is just installed, the list contains a limited amount of pre-defined addresses. The list is updated both by user request and automatically in order to give priority to high-score nodes and the nodes with the highest availability. Moreover, the node adds new elements to the list retrieving them from all available remote nodes.

The built-in mechanism pays attention to the following factors of remote node *quality* (in order of importance):

1. Visibility: the payer has to know the node,
2. Availability: the amount of errors seen recently,
3. Knowledgeability: the amount of nodes this node is aware of,
4. Activity: the frequency of push requests the node originates,
5. Score: the one reported during the most recent handshake.

8 Fetch, Merge, and Propagate

First, to see a wallet, it has to be *fetched* from a number of remote nodes. The nodes may provide different versions of the same wallet, either because some data is corrupted or because modifications were made to the same wallet from different parts of the network. Each version retrieved from the network is stored in a local *copy* and gets a score assigned to it. The score of the local copy is a summary of all scores of the nodes that provided that copy. Let's say, there are 17 nodes in the network and they provided three different copies of the wallet:

```
copy-1: 78,090 bytes, 11 servers, 177 score
copy-2: 56,113 bytes, 4 servers, 69 score
copy-3: 97,132 bytes, 2 servers, 37 score
```

The fetch operation ends at this point. The next step is to *merge* all three copies into the local one, if it exists. The algorithm of merging is the following.

First, the copy of the wallet we are merging into, is added to the list, with the score zero:

```
copy-0: 55,991 bytes, 0 servers, 0 score
copy-1: 78,090 bytes, 11 servers, 177 score
copy-2: 56,113 bytes, 4 servers, 69 score
copy-3: 97,132 bytes, 2 servers, 37 score
```

Then, the copy with the highest score is assumed to be the correct one, which is the `copy-1` in this example.

Then, all other copies, in the order of their scores, are merged into the correct one, transaction by transaction, applied the following rules consequently:

1. If the transaction already exists, it's ignored;
2. If the transaction is negative (spending money) and its ID is lower than the maximum ID in the ledger, it gets ignored as a fraudulent one ("double spending");
3. If the transaction makes the balance of the wallet negative, it is ignored;
4. If the transaction is positive and its signature is not valid, it is ignored;
5. If the transaction is negative and it's absent in the paying wallet (which is fetched and merged first), it's ignored;
6. Otherwise, it gets added to the end of the ledger.

When merge is done, the modifications get *propagated* to other wallets available locally. Each transaction that has a negative amount is copied to the ledger of their receiving wallets (with a reversed sign), if it doesn't yet exist there.

9 Pay and Push

To send money from one wallet to another, the owner of the sending wallet has to add a negative transaction to it and sign it with the private RSA key.

At any moment of time any node may decide to push a wallet to another node. The receiving node accepts it, merges with the local version, and keeps locally. Then, it *promotes* the wallet to all known remote nodes.

10 RESTful API

There is a limited set of RESTful API entry points in each node. Each response has `Content-Type`, `Content-Length`, and `X-Zold-Version` HTTP headers.

`GET /` is a home page of a node that returns JSON/200 response with the information about the node, for example (other details may be added in further versions):

```
{
  "version": "0.6.1",
  "score": {
    "value": 3,
    "host": "b2.zold.io",
    "port": 4096,
    "invoice": "THdonv1E@0000000000000000",
    "suffixes": [ "4f9c38", "49c074", "24829a" ],
    "strength": 6
  }
}
```

`GET /remotes` returns the list of remote nodes known by the node, in JSON/200:

```
{
  "version": "0.6.1",
  "all": [
    { "host": "b2.zold.io", "port": 4096 },
    { "host": "b1.zold.io", "port": 80 }
  ]
```

`GET /wallet/<ID>` returns the content of the wallet, in JSON/200:

```
{
  "version": "0.6.1",
  "body": "..."
```

If the wallet is not found, a 404 HTTP response is returned.

If the client provided the pre-calculated MD5 hash of the wallet content in the `If-None-Match` HTTP header and it matches with the hash of the content the node contains, a 304 HTTP response is returned.

`PUT /wallet/<ID>` pushes the content of the wallet to the node. The node responds either with 202 (if accepted), 400 (if the data is corrupted), 402 (if taxes are not paid), or 304 (if the content is the same as the one the node already has).

11 Incentives

It is obvious that anonymous users will participate in Zold and maintain their nodes only if they have enough financial motivation to do that. Simply put, their expenses must be lower than the income they are getting in form of taxes. This Section analyzes the most obvious questions users may have, regarding their motivation.

11.1 To Stay Online

What is the reason for a node to stay online and spend its CPU power and network traffic? Each node is insterested in doing that because it hopes that wallet owners will pay taxes to its invoices. The software automatically decides which node to pay taxes to and the selection is made by the availability criteria. The node which is the most available and visible will get the majority of tax payments.

11.2 To Accept Wallets

Why a node would accept push requests and spend its storage space on the wallets coming in? If the node doesn't accept a push request, its availability rating decreases and other nodes will stop paying taxes to it.

11.3 To Advertise Other Nodes

What is the incentive to advertise other remote nodes via the `/remotes` RESTful entry point and why can't a node always return an empty list, expecting its clients to always pay taxes to it? The software automatically prioritizes remote nodes by the amount of remote nodes it promotes. The longer the list a node returns, the higher its chance to be at the top of the list.

11.4 To Promote Wallets

What is the incentive to promote wallets to remote nodes, spending network traffic for this operation? Each node ranks its remote nodes also by the

amount of push requests they send. Thus, in order to stay on top of the lists each node is interested to push wallets further.

12 Threats & Responses

It is obvious that a distributed system that consists of anonymous nodes even theorecially can't be 100% safe, reliable, secure and trustworthy. Zold is not an exception. However, it's designed in an honest attempt to mitigate all critical threats and make the system "reliable enough." This Section summarizes the most import of those threads and explains how Zold responds to them.

12.1 Double Spending Attack

It is possible to submit the same spending transaction to the same wallet and then push it to two different nodes in different parts of the network. They won't know about each other and will propagate those spending transactions to other wallets. Both two owners of those money receiving wallets will think that their money arrived, while only one of them is a legit receiver, the other transaction is fraudulent.

This will happen, but very soon one part of the network will dominate the other one, and one of the transactions will be rejected from the wallet, after a number of merge operations in all nodes of the network. The receiver of the money must be careful and always to the full fetch (from as many

12.2 51% Attack

A group of nodes can combine their CPU power in order to win the consensus algorithm and add fraudulent incoming transactions to a wallet. The fetching node will trust the wallet "as is" and will think that the balance of the wallet is larger than it actually is.

This may happen, but a fetching node may always re-validate the entire wallet, by checking RSA signatures of all transactions. This will take some time, but will provide an extra guarantee to the client.

12.3 Fraudulent Tax Refunds

Some nodes may resell their scores to their affiliated tax payers, and they refund them some amount of taxes back. This will be profitable both for the tax payers, since they will pay less taxes, and for the node owners, since they will receive the payments anyway.

This scenario is indeed possible, but it is assumed that since tax payments are supposed to be made in small increments and automatically, the majority of clients won't be interested in this fraudulent scheme.

12.4 Loss of Wallet

A wallet is just a text file, which can easily be lost by it owner.

This indeed is possible, but is not a risk at all, since all wallets are maintained by the network and anyone can easily pull any wallet back. The only sensitive part is the private key of the wallet. If that file is lost, the wallet can't pay anything anymore. This is the file all wallet owners must keep safe.

13 Conclusion

To be written...

References

Andreessen, Marc (2014). "Why Bitcoin Matters." *New York Times* 21.

Boyen, Xavier et al. (2016). *Blockchain-free Cryptocurrencies: A Framework for Truly Decentralised Fast Transactions*. Tech. rep. Cryptology ePrint Archive, Report 2016/871.

Buterin, Vitalik (2013). "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform." URL: https://github.com/ethereum/wiki/wiki/White-Paper.

Everaere, Patricia et al. (2010). "Double Spending Protection for E-cash Based on Risk Management." *International Conference on Information Security*. Springer, pp. 394–408.

Karame, Ghassan O. et al. (2012). "Double-spending Fast Payments in Bitcoin." *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, pp. 906–917.

Kaskaloglu, Kerem (2014). "Near Zero Bitcoin Transaction Fees Cannot Last Forever." *The International Conference on Digital Security and Forensics*. The Society of Digital Information and Wireless Communication, pp. 91–99.

Kiayias, Aggelos et al. (2015). "Speed-Security Tradeoffs in Blockchain Protocols." *IACR Cryptology ePrint Archive* 2015, p. 1019.

Möser, Malte et al. (2015). "Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees." *International Conference on Financial Cryptography and Data Security*. Springer, pp. 19–33.

Nakamoto, Satoshi (2008). "Bitcoin: A Peer-to-peer Electronic Cash System."

Pilkington, Marc (2016). "Blockchain Technology: Principles and Applications." *Research Handbook on Digital Transformations*, p. 225.

Popov, Serguei (2017). "The Tangle." URL: https://iotatoken.com/IOTA_Whitepaper.pdf.

Van Alstyne, Marshall (2014). "Why Bitcoin Has Value." *Communications of the ACM* 57.5, pp. 30–32.