Byteball: A Decentralized System for Storage and Transfer of Values*

Anton Churyumov
tonych@byteball.org

Abstract

Byteball is a decentralized system that allows tamper proof storage of arbitrary data, including data that represents transferrable value such as currencies, property titles, debt, shares, etc. Storage units are linked to each other such that each storage unit includes one or more hashes of earlier storage units, which serves both to confirm earlier units and establish their partial order. The set of links among units forms a DAG (directed acyclic graph). There is no single central entity that manages or coordinates admission of new units into the database, everyone is allowed to add a new unit provided that he signs it and pays a fee equal to the size of added data in bytes. The fee is collected by other users who later confirm the newly added unit by including its hash within their own units. As new units are added, each earlier unit receives more and more confirmations by later units that include its hash, directly or indirectly.

There is an internal currency called ‘ bytes ’ that is used to pay for adding data into the decentralized database. Other currencies (assets) can also be freely issued by anyone to represent property rights, debt, shares, etc. Users can send both bytes and other currencies to each other to pay for goods/services or to exchange one currency for another; the transactions that move the value are added to the database as storage units. If two transactions try to spend the same output (double-spend) and there is no partial order between them, both are allowed into the database but only the one that comes earlier in the total order is deemed valid. Total order is established by selecting a single chain on the DAG (the main chain) that is attracted to units signed by known users called witnesses. A unit whose hash is included earlier on the main chain is deemed earlier on the total order. Users choose the witnesses by naming the user-trusted witnesses in every storage unit. Witnesses are reputable users with real-world identities, and users who name them expect them to never try to double-spend. As long as the majority of witnesses behave as expected, all double-spend attempts are detected in time and marked as such. As witnesses-authored units accumulate after a user ’ s unit, there are deterministic (not probabilistic) criteria when the total order of the user ’ s unit is considered final.

Users store their funds on addresses that may require more than one signature to spend (multisig). Spending may also require other conditions to be met, including conditions that are evaluated by looking for specific data posted to the database by other users (oracles).

Users can issue new assets and define rules that govern their transferability. The rules can include spending restrictions such as a requirement for each transfer to be cosigned by the issuer of the asset, which is one way for financial institutions to comply with existing regulations. Users can also issue assets whose transfers are not published to the database, and therefore not visible to third parties. Instead, the information about the transfer is exchanged privately between users, and only a hash of the transaction and a spend proof (to prevent double-spends) are published to the database.

* Abstract and Section A to B are translated by Kensuke ITO(QVMGJX367QTJD4TLFYGZNKB256CVTQVX). Section C to D are translated by someone(byteball address is here).

1 Introduction

In Orwell ' s 1984, the protagonist Winston Smith works in the Records Department of the Ministry of Truth as an editor, revising historical records, to make the past conform to the ever-changing party line and deleting references to unpersons people who have been "vaporised," i.e. not only killed by the state but denied existence even in history or memory [1]. What we present here is data storage that is not rewritable. It is a distributed decentralized database where records can neither be revised nor deleted entirely.

Bitcoin [2] was the first system to introduce tamper proof records designed for the specific purpose of tracking the ownership of electronic currency units known as bitcoins. In Bitcoin, all transfers of the currency are represented as transactions that are digitally signed by the current owner of the coin, transactions are bundled into blocks, and blocks are linked into a chain (blockchain) secured by proof of work (PoW) that assures that large computing resources have been invested into building the chain. Any attempt to rewrite anything contained in the chain would therefore require even larger computing resources than those that have already been expended.

Soon after Bitcoin appeared, it became clear that this was more than just a trust-free P2P electronic currency. Its technology became a source of new ideas for solving other problems. At the same time, Bitcoin ' s deficiencies and limitations equally became clear. Byteball is designed to generalize Bitcoin to become a tamper proof storage of any data, not solely transfers of a single electronic currency, and remove some of the most pressing deficiencies that impede a wider adoption and growth of Bitcoin.

Blocks. In Bitcoin, transactions are bundled into blocks, and blocks are linked into a single chain. Since the blocks are linked linearly, their spacing in time and their size are optimized for near-synchrony among nodes, so that the nodes can share a new block with each other much faster than it typically takes to generate a new block. This ensures that nodes most likely see the same block as the last block, and orphaning is minimized. As Bitcoin grows, blocks become increasingly unwieldy. They are either capped in size, in which case the growth is also capped, or they take too long to propagate to all nodes of the network, in which case there is greater uncertainty about which block is last, and more resources are wasted on extending chains that would later be orphaned. In Byteball, there are no blocks, transactions are their own blocks, and they need not connect into a single chain. Instead a transaction may be linked to multiple previous transactions, and the whole set of transactions is not a chain but a DAG (directed acyclic graph). DAG-based designs have received much attention recently [3-5].

Cost. Bitcoin transactions are secure because it is prohibitively expensive to redo all the PoW included in the blocks created after the transaction. But that also means that it is necessary to pay to build the legitimate PoW that is strong enough to ward off any attackers. This payment is spent for the electricity required to build the PoW. What is important to note here, is that this money goes outside the Bitcoin ecosystem to energy companies meaning that the community of Bitcoin holders as a whole is bleeding capital. In Byteball, there is no PoW, instead we use another consensus algorithm based on an old idea that was known long before Bitcoin.

Finality. Transaction finality in Bitcoin is probabilistic. There are no strict and simple criteria for when you can say that a transaction will never be reversed. Rather, you can only argue that the probability of a transaction being reversed exponentially decays as more blocks are added. While

this concept is perfectly clear to those versed in math, it might be a difficult sell to an average Joe who is used to expecting a black-or-white picture in matters of money ownership. To complicate things even further, transaction finality also depends on its amount. If the amount is small, you can be reasonably sure nobody will try to double-spend against you. However, if the amount at stake is greater than the block reward (12.5 BTC at the time of writing), you might speculate that the payer could temporarily rent hashpower to mine another chain of blocks that doesn ' t contain the transaction that pays to you. Therefore, you have to wait for more confirmations before being sure enough that a high-value transaction is final. In Byteball, there are deterministic criteria for when a transaction is deemed final, no matter how large it was.

Exchange rate. The Bitcoin price is known to be quite volatile. The bigger problem is that this price is not only volatile, it is not bound to anything. Share and commodity prices are also very volatile but there are fundamentals behind them. Share price is largely a function of company earnings, revenue, debt-to-capital ratio, etc. Commodity prices depend, among other factors, on costs of production with various suppliers. For example, if the oil price falls below the production costs of some suppliers for a long time, these suppliers will eventually shut down, decreasing production and causing the price to go up. There is a negative feedback loop. In Bitcoin, there are no fundamentals, and no negative feedback. A Bitcoin price of $500 is no more justified than a price of $50,000 or $5. If the Bitcoin price moves from where it is now, this movement alone will not create any economic forces that would push the price back. It ' s just wild. In Byteball, the base currency, bytes, is used to pay for adding data into the Byteball database. You pay 1,000 bytes to add 1Kb of data. It is a measure of the utility of the storage in this database, and actual users will have their opinion on what is a reasonable price for this. If the price of byte rises above what you think is reasonable for your needs, you will find ways to store less bytes, therefore you need to buy less bytes, demand decreases, and the price falls. This is negative feedback, common for all goods/services whose demand is driven by need, not speculation. Besides paying in bytes, one can issue other assets and use them as means of payment. These assets might represent, for example, debt expressed in fiat currencies or in natural units (such as kWh or barrels of oil). The price of such assets is naturally bound to the underlying currencies or commodities.

Privacy. All Bitcoin transactions and balances of all addresses are visible on the blockchain. Although there are ways to obfuscate one ' s transactions and balances, it is not what people have come to expect from a currency. Transactions in bytes (the base currency) in Byteball are equally visible, but there is a second currency (blackbytes), which is significantly less traceable.

Compliance. Bitcoin was designed as an anonymous currency where people have absolute control over their money. That goal was achieved; however, it made Bitcoin incompatible with existing regulations, and hence inappropriate for use in the financial industry. In Byteball, one can issue assets with any rules that govern their transferability, from no restrictions at all, like Bitcoin, to anything like requiring every transfer to be cosigned by the issuer (e.g. the bank) or restricted to a limited set of whitelisted users.

2 Database structure

When a user wants to add data to the database, he creates a new storage unit and broadcasts it to his peers. The storage unit includes (among other things):

- The data to be stored. A unit may include more than one data package called a message.

There are many different types of messages, each with its own structure. One of the message types is payment, which is used to send bytes or other assets to peers.

- Signature(s) of one or more users who created the unit. Users are identified by their addresses. Individual users may (and are encouraged to) have multiple addresses, like in Bitcoin. In the simplest case, the address is derived from a public key, again similar to Bitcoin.
- References to one or more previous units (parents) identified by their hashes.

References to parents is what establishes the order (only partial order so far) of units and generalizes the blockchain structure. Since we are not confined to one-parentone-child relationships between consecutive blocks, we do not have to strive for near-synchrony and can safely tolerate large latencies and high throughputs: we ’ll just have more parents per unit and more children per unit. If we go forward in history along parent-child links, we ’ ll observe many forks when the same unit is referenced by multiple later units, and many merges when the same unit references multiple earlier units (developers are already used to seeing this in git). This structure is known in graph theory as directed acyclic graph (DAG). Units are vertices, and parent-child links are the edges of the graph.

3 Native currency: bytes

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

4 Double-spends

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

5 The main chain

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキスト

です。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

6 Witnesses

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

7 Finality

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

8 Storage of nonserial units

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

9 Balls

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

10 Last ball

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

11 Witness list unit

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

12 Unit structure

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

13 Commissions

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これは

サンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

14 Confirmation time

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

15 Partitioning risk

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

16 Censorship

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

17 Choosing witnesses

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプル

テキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

18 Skiplist

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

19 Light clients

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

20 Multilateral signing

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

21 Addresses

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキスト

です。これはサンプルテキストです。これはサンプルテキストです。

21.1 Definition syntax

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

21.1.1 Logical operators

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

21.1.2 Delegation to other addresses

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

21.1.3 Signitures and authentifiers

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

21.1.4 Definitiuon templates

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

21.1.5 Cosigning

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

21.1.6 Querying whether an address was used

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

21.1.7 Data fees

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

21.1.8 Markle data fees

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプル

テキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

21.1.9 Self-inspection

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

21.1.10 Negation

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

21.2 General requirements

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

22 Profiles

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

23 Attestations

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

24 Assets

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

24.1 Bank issued assets

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

24.2 Non-financial assets

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これは

サンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

24.3 Bonds

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

24.4 Commodity bonds

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

24.5 Funds

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

24.6 Settlements

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキスト

です。これはサンプルテキストです。これはサンプルテキストです。

25 Private payments

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

26 Fixed denominations assets

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

27 Texts

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

28 Arbitrary structured data

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

29 Voting

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。これはサンプルテキストです。

30 Private Messaging

For private payments to work, users need a way to securely deliver private payloads to each other. Users, or rather their devices, also need to communicate to assemble signatures for multi-sig addresses. Since we cannot expect user devices to be constantly online and easily reachable (most of them will be behind NAT), we need a store-and-forward intermediary that is always online, easily reachable, and able to temporarily store any data addressed to a user device. In Byteball, such an intermediary is called the hub, and its operation is similar to email. A hub is a Byteball node that additionally offers a service of storing and forwarding private messages to connected devices. There can be many hubs. Each device that runs a wallet code subscribes to a hub of its choice, and can be reached via this hub (the home hub). The choice of home hub can be changed at any time. Each device has a permanent private key that is unique to the device. The hash of the corresponding public key (more precisely, the hash of the single-sig definition based on this public key) is called the device address, and it is written in base32 like the payment addresses. The full device address, including its current hub, can be written as DEVICEADDRESSINBASE32@hubdomainname.com. If the device moves to another hub, the part of its full address before @ stays the same. Unlike email, the name cannot be already “ taken ”. Every device connects to its home hub using websockets. The hub sends the new messages to the device and the device stays connected to the hub, so that if a new message arrives while the device is connected the new message is delivered immediately. The hub doesn ’ t keep copies of the messages that were successfully accepted by the device. The connection to the hub is TLS encrypted. When a device wants to send something to another device, it connects to the recipient ’ s hub and sends the message. Unlike email, there is no relay the sender connects directly to the recipient ’ s hub. All communication between devices is end-to-end encrypted and digitally signed so that even the hub (who is the only man in the middle) cannot see or modify it. We use ECDSA for signing and ECDH+AES for encryption. Before exchanging encrypted messages the devices must be paired, i.e. learn each other ’s public key. This can happen in various ways, e.g. by scanning a QR code that encodes the public key and hub domain name of one of the devices, by sending this information over email, or by clicking a byteball:// link on a secure website. For forward security, every device generates a temporary private key and uploads the corresponding public key to its home hub. Afterwards, the device rotates the key from time to time but keeps a copy of the previous key in case someone sent a message to the previous key while the hub was replacing it. The hub keeps only one version of the temporary public key per

subscribed device. The sending device follows these steps to send a message:

1. connects to the recipient ' s hub;
2. receives the current temporary public key of the recipient from the hub;
3. generates its own one-time ephemeral key pair;
4. derives ECDH shared secret from the recipient ' s temporary public key and own ephemeral private key;
5. AES-encrypts the message using this shared secret;
6. adds its own ephemeral public key;
7. signs the package with its own permanent key; and
8. sends it to the hub.

The recipient device verifies the signature, derives ECDH secret using the peer 's ephemeral public key and own temporary private key, and decrypts the message. If the sending device fails to connect to the recipient ' s hub, it encrypts the message to the recipient ' s permanent key (this encryption is not forward secure since it uses a permanent key) and stores the encrypted message locally for future retries. The purpose of this encryption is to avoid having unencrypted messages lying around. After connection to the recipient ' s hub succeeds, the device sends this encrypted message, thus encrypting it again (this time, with forward security), so the message is double-encrypted. Note that this is not because single encryption is insufficient, but because we don ' t want to store unencrypted content for an indefinite time while the connections are retried. Note that the communication is among devices, not users. Users may (and are recommended to) hold several devices, such as a laptop, a smartphone, and a tablet, and set up multisig addresses with redundancy (such as 2-of-3) that depend on keys stored on multiple devices. When a user needs to sign a transaction, he initiates it on one of his devices. This device then sends the partially signed transaction to the other devices using private messages, collects all the signatures, and publishes the transaction. The private keys stored on each device should never leave that device. When the user replaces one of his devices in a 2-of-3 address, he just uses the other 2 devices to change the address definition and replace the key of the old device with the key of a new device. The private messages can also be used for encrypted texting between devices. These messages are strictly peer-to-peer, never go into the Byteball database, and can be safely discarded after they are read. When users pay in blackbytes or other private assets, they have to send private payloads and absolutely need devices that can communicate. They need to know each other 's device addresses before they even learn each other ' s payment addresses. Once their devices have established communication, the payee can send his payment address to the payer via chat message. Such a payment scenario also makes it easy to generate a unique payment address for every incoming payment. A merchant can run a chat bot that communicates with users via text messages. When the user is ready to pay the bot generates a new payment address and sends it to the user in a chat message.

31 Conclusion

We have proposed a system for decentralized immutable storage of arbitrary data, including data of social value such as money. Every new unit of data implicitly confirms the existence of all previous units. Revision of past records similar to that in 1984 becomes impossible, as every new unit also implicitly protects all previous units from modification and removal. There is an internal

currency that is used to pay for inclusion of data in the decentralized database. The payment is equal to the size of the data to be stored, and other than this payment there are no restrictions on access to the database. Other assets can also be issued and their ownership can be tracked on the database. When tracking payments in the internal currency and other assets, double-spends are resolved by choosing the version of history that was witnessed by known reputable users. Settlement finality is deterministic. Assets can be issued with any rules that govern their transferability, allowing regulated institutions to issue assets that meet regulatory requirements. At the same time, transfers can be hidden from third parties by sending their content privately, directly from payer to payee, and publishing spend proofs to ensure that each coin is spent only once.

References

1. Quoted from Wikipedia https://en.wikipedia.org/wiki/Nineteen_Eighty-Four.
2. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, 2008.
3. Sergio Demian Lerner. DagCoin, https://bitslog.files.wordpress.com/2015/09/dagcoin-v41.pdf, 2015.
4. Serguei Popov. The Tangle, http://iotatoken.com/IOTA_Whitepaper.pdf, 2016.
5. TomHolden. Transaction-Directed Acyclic Graphs, https://bitcointalk.org/index.php?topic=1504649.0, 2016.
6. Linked timestamping, https://en.wikipedia.org/wiki/Linked_timestamping.
7. Atomic cross-chain trading, https://en.bitcoin.it/wiki/Atomic_cross-chain_trading.
8. https://github.com/bitcoin/bitcoin
9. Gavin Wood. Ethereum: A Secure Decentralised Generalised Transaction Ledger, http://gavwood.com/Paper.pdf.