CRYUM

DECENTRALIZED SYSTEM
FOR
DIGITAL ASSET BASED ON
„BRANCHPIPE“
(BP)

BY

Twenty Three
number23@cryum.org
www.cryum.org

ABSTRACT

The CRYUM project and this document refer to a new technology called Branchpipe (BP) including an extended technology for transferring digital asset abbreviated as BP-Tx. In this case, Tx is an attribute that defines the type of operation for which this technology is designed. In this case, Tx defines transactions – transfer of digital asset within a decetralized network in a shared ledger with the goal of delivering efficient transfer without delay, processing several thousands of transactions at once, so that the use of the CRYUM cryptocurrency is not an environmental burden as we know from Blockchain technology. This document does not discuss a new cryptocurrency that is built on ERC20/Ethereum protocol to be presented to the world as a new pseudocurrency immediately available to investors as an ICO to lure capital. On the contrary, the document discusses the integration of highly anonymous transactions as well as the removal of transaction fees. The document discusses the main elements of the CRYUM network such as reaching a consensus within the network, integration of C-PoSg protocol or the description of use (Branchpipe). Some schemes represent only the basic analogy and do not describe detailed changes or specific editing methods for the CRYUM project. By combining these technologies and adjusting them to the discussed project, we have composed 5R – five rules/basic rules of a cryptocurrency: 1) no fees, 2) instant transactions, 3) 100% anonymity, 4) no energy consumption, 5) low volatility.

Keywords

Blockchain, Pipeline, Blind Signature, Nodes, Consensus, Branched Pipeline, Transactions, Hash, Timestamps

CONTENT

INTRODUCTION

We imagine a world in which people are independent from authorities and banking systems. Our trust towards each other depends on third parties that mediate it. For decades, we have been dependent on these intermediaries to secure our trust towards each other. A handful of organizations control such amount of data, that if one of them crashes (intentionally or not), chaos will prevail in the world. Payment systems as we know them are built on credibility, security and regular auditing; only verified companies with valid certificates can process and accept payments. For their services and investments in a constantly available and secure network, they ask for fees for each processed transaction. Which, moreover, take a day or more, depending on how many other intermediaries they flow through. This exact business model was supposed to be made cheaper and replaced by blockchain. The truth is, however, that this didn't happen, because transactions travel slowly, the currency's value is volatile and fees are often higher than in commercial bank houses.We want a technology that is able to transfer funds from one continent to another safely, quickly, anonymously and free of charge. Our ambition was to create a real cryptocurrency based on a technology other than blockchain, whether it is Bitcoin or Ethereum via ERC20, which is so popular today for creating pseudocurrencies. Pseudocurrencies built on ERC20 do not bring innovative solutions because they still use the same logic and engine as Ethereum. We wanted a cryptocurrency that is going to be fast, without fees and with no energy consumption.

1. CURRENT SITUATION

1.1 History

It all started in 2008 when Satoshi Nakamoto, whose identity is still unknown, published a document called „Bitcoin: A Peer-to-Peer Electronic Cash System“. In his work, he described a peer-to-peer version of electronic cash which is known as Bitcoin. Over the last 10 years, this theory has evolved into a pioneer technology with a huge potential of use. However, we must not forget that even today, there are lots of people who claim that Blockchain equals Bitcoin, which is obviously not true. In its core, blockchain is an open decentralized ledger that is able to permanently record transactions without the need of verification by a third central authority. This technology was supposed to reduce transaction costs dramatically. However, time has shown that transaction fees are often even higher than the value of the transaction itself. Despite current drawbacks, entrepreneurs have invested a considerable amount of resources into this technology. It is safe to assume that 15% of financial institutes use a block technology, despite the pressure coming from these institutes. Following Bitcoin, a new cryptocurrency has entered the market – Ethereum, which has introduced so-called „smart contracts“. Vitalik Buretin was the co-founder of the Ethereum and Bitcoin magazine. He was among the first to contribute to the Bitcoin database. Later on, he was met with misunderstanding from the Bitcoin community and thus decided to introduce another block chain called Ethereum. The main difference between Bitcoin and Ethereum is that Ethereum is able to also record other assets such as loans, contracts or other currencies. Ethereum was released in 2015 and is based on smart contracts. This technology has caught the attention of various companies and developers. Ethereum was supposed to reduce transaction time and fees. However, fees still do not meet the requirements of a properly usable digital currency without central authority. Blockchain works on the concept of proof of work, where a very costly calculation that consumes a huge amount of energy takes place.

1.2 General terms

1.2.1 Coin

All currencies with transactions recorded in a block chain such as Bitcoin, Litecoin, Ripple, etc. that indicate only a change in numerical value are called „coins“. They can be understood as fixed digital assets stored in a block. Bitcoin coins work on a block with a Bitcoin protocol. It is impossible to exchange these coins in another network that works on an entirely different block. Bitcoin, along with other currencies, is based on blockchain technology which nowadays poses problems connected with huge energy consumption of PoW.

1.2.2 Token

Token and coin can appear to be related, but in practice they are two separate terms used in transferring digital asset. Tokens work above the block and are not a separate currency and do not form a separate block chain. Coins are supposed to be a currency that can be exchanged for goods and services, while tokens are understood as anything we can exchange. Tokens are created by using a template on a platform such as Ethereum and work thanks to smart contracts. Ether tokens, e.g. on the ERC20 protocol, can be assembled even by a beginner programmer. However, they are created by spending coins. It is typical for tokens to serve as a currency in a specific application which they are an inseparable part of. Of course, transferring them is not free and fees should be taken into account when sending a transaction.

1.2.3 Blockchain.

Blockchain is a public ledger in which transactions are recorded and confirmed. It is a record of events that is shared between many parties. And, more importantly, as soon as an information is entered, it can not be modified. Block chain is a distributed database, which means that not all memory-based devices within the database are connected to a common processor. It keeps an ever-growing list of organized records called blocks. Each block has a timestamp and a link to the previous block.

1.2.4 Protocol

Protocol can be defined as a set of rules by which a specific entity or a group of entities is controlled. It is basically a programmed software that defines rules of how processes e.g. in the network should be processed or how entities are supposed to communicate with each other. We can take the internet as an example. Today, the internet runs on a relatively „thin“ layer of protocols such as TCP/IP, SMTP, HTTP and HTTPS. These protocols specify rules for computers within the network so that they can communicate efficiently. If we think about what a protocol is, we realize that we are already using one without even knowing.

2. OUR PHILOSOPHY

Our ambition was to create a real cryptocurrency that uses a technology similar to blockchain with all attributes of a cryptocurrency, but with instant, free and zero-energy transactions. We can see from practice that no currency is able to meet the rules of a functioning financial system – volatility, fees and others. These problems are the most common among cryptocurrencies. These are not standard rules such as encryption, verification and decentralization. We had to define 5 basic rules (5R) of a future cryptocurrency. In order for the digital currency to work in a monetary system, we have set 5R only for Cryum.

<table>
<tr><td colspan="6"><b>CRYUM</b></td></tr>
<tr><td><b>Standard</b></td><td>Decentralized</td><td>Cryptography</td><td>No double spent</td><td colspan="2">Trust</td></tr>
<tr><td colspan="6"><b>Five rules (5R)</b></td></tr>
<tr><td><b>Our extended features</b></td><td>1st R
No fees</td><td>2nd R
Instant transactions</td><td>3rd R
100% anonymous</td><td>4th R
No energy requirements</td><td>5th R
Low volatility</td></tr>
</table>

3. CRYUM TECHNOLOGY

3.1 Branchpipe

Branchpipe (BP) or Branchpipe Transaction (BP-Tx) is a technology that is being used in practice for the first time for transferring funds in decentralized systems. The idea of BP was created as a combination of „Branched-chain“ (chemical structure) and „Pipelining“ (in computing, a pipeline, also known as a data pipeline, is a set of data processing elements connected in series, where the output of one element is the input of the next one).

Both ideas were combined and adjusted so that they meet the requirements of an innovative transaction. Some components and original names have remained from the original ideas and are combined into Branchpipe , which represents the branching of pipelines into segments connected into a chain so that they can be disconnected from each other, shared and transactions can be carried out at the same time.

This allows BP to transfer any digital asset within the network and, among others, create subsystems running in parallel with a different type of asset. BP introduces a new look at security, speed and efficiency of transferring digital asset. Its strength lies in the branching of a pipeline, so that it creates a branched ledger structure. BP is built on the idea of pipeline computing that allows the segmentation of parts and not putting it in a block chain, as we know from Blockchain technology. In BP, the instructions (transactions) themselves are already associated with an additional branching element called a pipeline adapter.

Transactions that form a pipeline are arranged so that the resulting parameter of the previous transaction is the entry parameter of the next one. However, if we take a look at the issue in detail, we can see that each pipeline has its own chain that can be shared within the network partially or complexly.

Nodes that process the corresponding operations are always bound to the last known result of the deduction receipt, comparing the balances for the given chain. Besides that, they also check the pipeline adapter whether data was changed or not. In practice, for TxnP, it is enough to verify Tx1P for the relevant part. Tx1P can only consist of 3 deduction receipts, which, in the process of verifying and comparing hashes, are fast and have low hardware demands. Thus, it is possible to verify several thousand transactions at a time and sort them, meaning that a transaction is instantly recorded simultaneously with other transactions. To enter a branch and create a separate chain, an admission ticket is required, i.e. receive funds for the first time from anyone (more in the Double spending section). Balance, input and output hashes calculated from ledger parameters that are connected with each other can not be modified and thus any verification is easily executable for any node of a Branchpipe . The last Lh_n of a transaction contains information that enables the verification of validity and thus prevents double spending of coins, because two identical deduction receipts can not exist within the network.

Figure 1:
Branchpipe Transaction

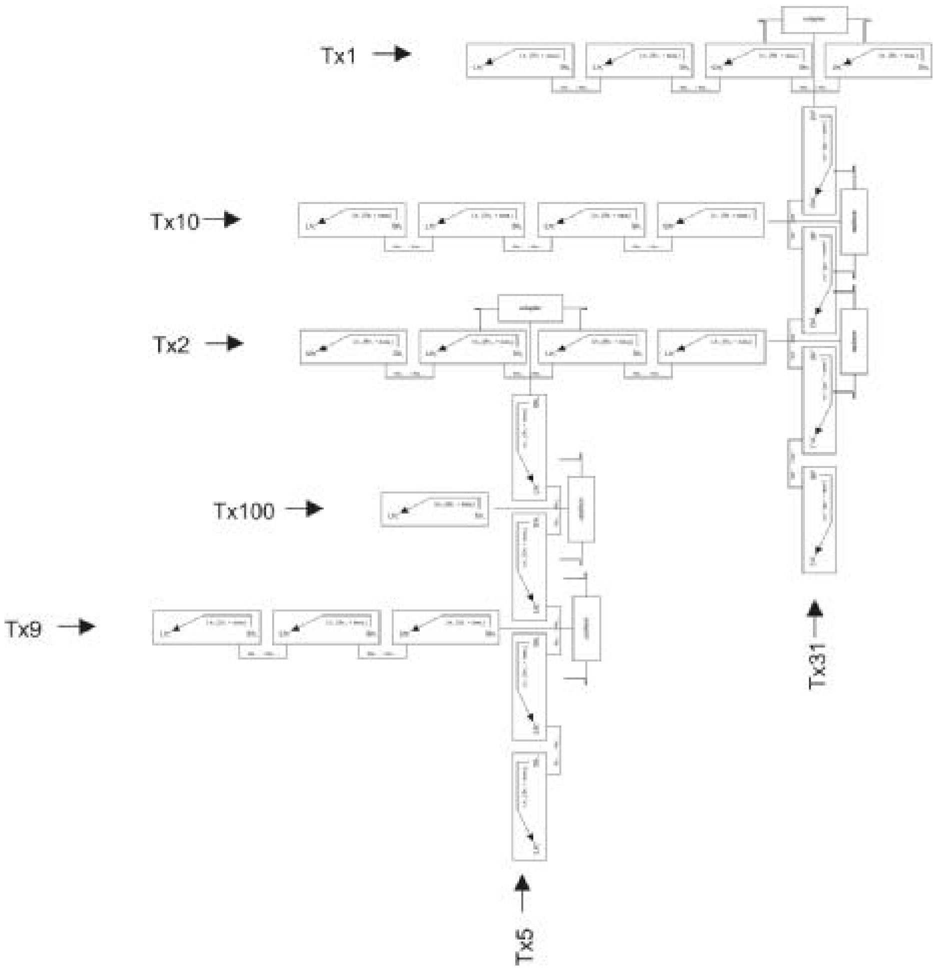
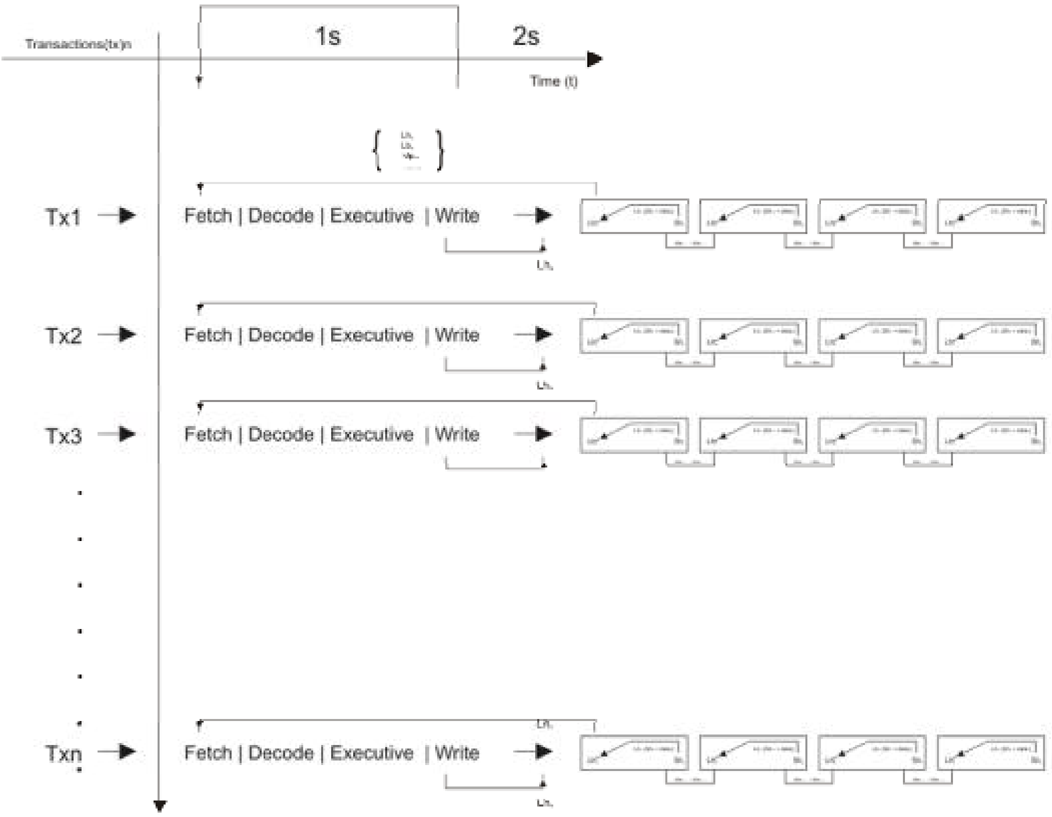


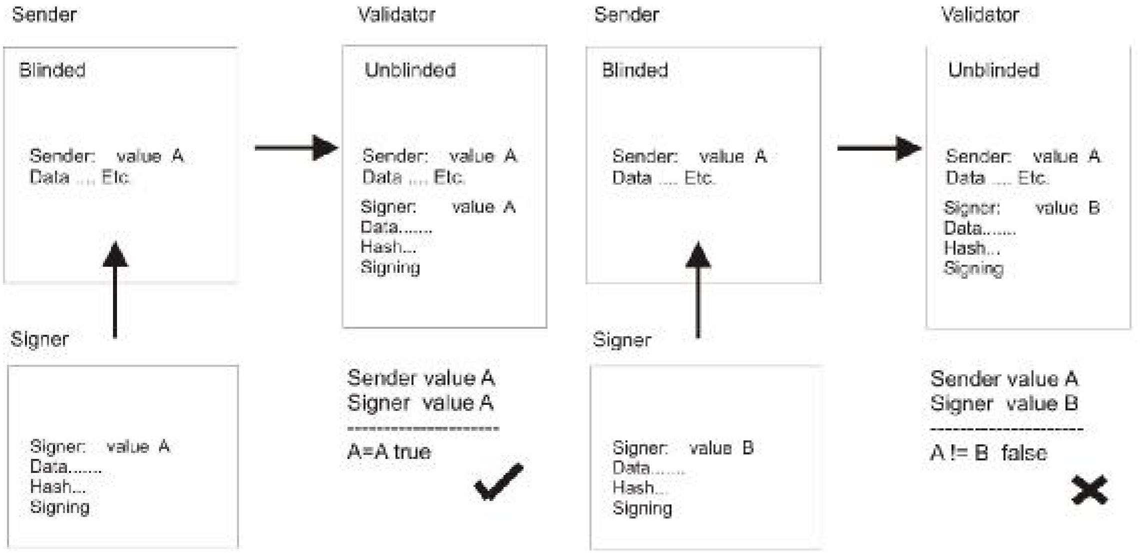
Figure 2:
Real time processing of transactions on several pipelines at once


Transactions(tx)n
1s
2s
Time (t)
Tx1
Tx2
Tx3
Txn
Fetch | Decode | Executive | Write
Fetch | Decode | Executive | Write
Fetch | Decode | Executive | Write
Fetch | Decode | Executive | Write

3.2 Blind signature

According to David Chaum, the concept of blind signature can be illustrated by common paper documents. A carbon envelope contains a document which needs to be signed. The document is facing the coloring part, just like with a carbon-paper. The signatory then signs the envelope which stamps his signature on the document. The signatory has signed a document without knowing its content. We have also developed the idea of honesty. We insert value „A“ into the document and we expect the signatory to insert the same value and sign it. After revealing a part of the document (no need to reveal it whole), the information whether the signatory was honest or not remains hidden. In the CRYUM network, this principle is used in combination with other elements, such as when will a user attach to the signature the value of their balance, which, after revealed, is compared to the existing balance. If the values match, the user was honest, and if not, the user cheated about their balance and the transaction is declined.

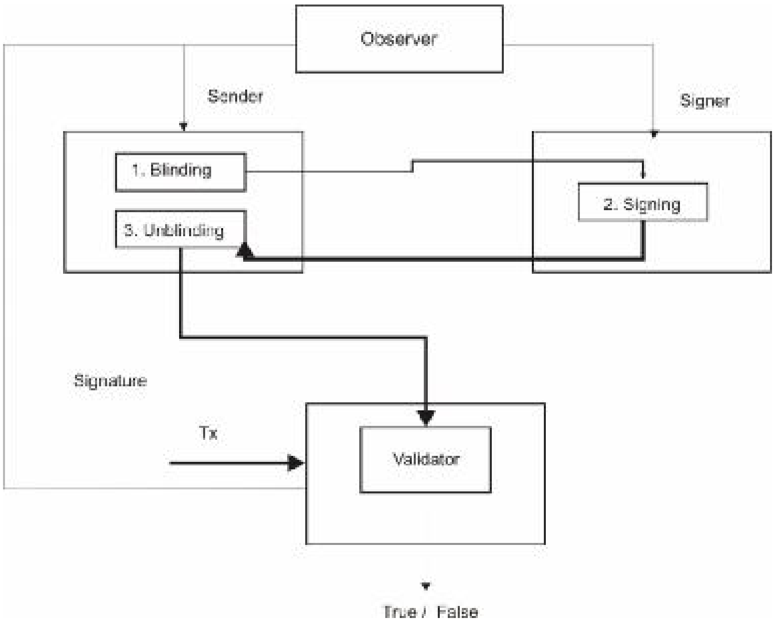
True False



Practical use varies, but the fact remains that blind signature solves anonymity in the network, among other things.

The principle works as follows. When you withdraw money from a bank, the bank gives you your cash without anyone knowing what you are buying. However, if you carry out a transaction like this on the level of credit cards or other systems, you must tell the operator who you are, as well as report to the merchant and operator at which bank you are carrying out the transaction. With blind signatures, nothing like this exists. Thus, the use of blind signatures for protecting privacy has a huge potential. Blind signature ensures signing of the document without opening it. If we add the option to attach data that we do not know about to the document and we do not know its content, but it is expected from us to express honesty (e.g. last balance), then it becomes an excellent verification instrument, because anything we attach to the blind signature must be identical with the contents of a closed envelope that we have signed. Analogically, if anything does not match, the document will be deemed invalid. Blind signatures allow the use of cryptographic functions for the creation and use of keys. Various publications and authors define the use of blind signatures in their own words and view on the problem. Thus, we need to keep in mind that the technology of blind signatures within the CRYUM network was adjusted to meet the requirements of the network in combination with cryptographic and hash functions, timestamps and other functions to achieve the desired result. For illustration, here is a scheme of how blind signatures work.

Figure 3: Basic flow of a blind signature structure



Obviously, the scheme of blind signatures illustrated in this document represents an analogy of how this technology works. Blind signature can also contain modified elements that are not public and are inserted into the „envelope“ anonymously. If there are more envelopes like this, where each envelope’s opposite side contains information that all parties insert, this information must match after revealing documents. Otherwise, the operation is invalid. Information distribution, evidence that sealed envelopes were not opened and the verification process was accomplished, as well as evidence that a signatory exists and a trusted person knows him, is ensured by C-PoSg protocol, for example.

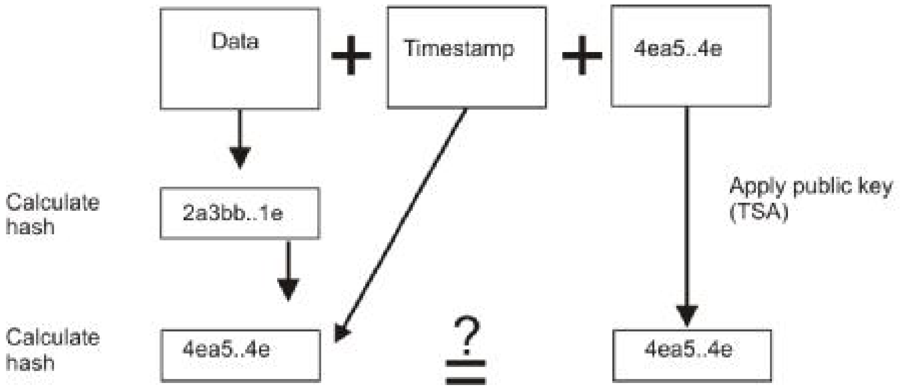
3.3 Proof of Signatory (C-PoSg)

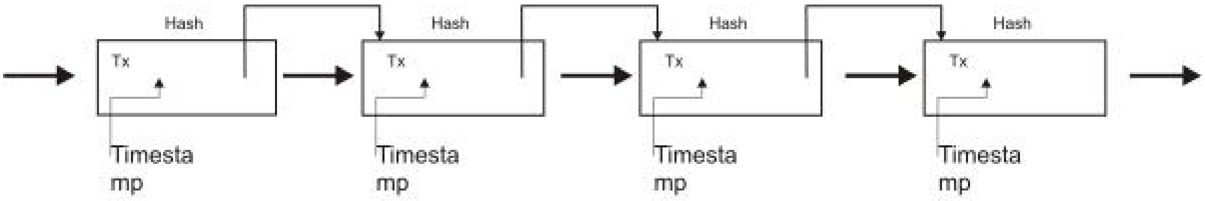
One form of identity verification includes a trusted witness – someone who the notary knows personally and who also personally knows the signed person. A trusted witness must arrive with the signatory at the time when the document is being verified. The best practice is that the notary gives an oath or confirmation to the trusted witness and the witness signs an honorable statement, which states that he verifies the identity of the signed document. Due to the requirement that a trusted witness is personally known by the notary and that the witness personally knows the signed person, this method of identity verification is most commonly used by notaries. PoSg represents a form of proof called Proof of Signatory (not Proof of Signature!). It is the implementation of the real practice of notary verification into CRYUM's software logic. The observer node resulting from the consensus of voting and selection as a trusted element for the transaction (avoidance of false witness) becomes the sender of information during the transaction, as well as the observer of the transactions's validity itself. His task is to ensure the flow of information, so that he oversees the transaction validation and to mediate the transaction between the user and the validator. He delivers requests in the network to the user and guarantees that the user is a valid element and that the information was delivered exactly to him. The observer is unable to identify the intention of the user and does not rely on his honesty (false submission of information by the user who logged in to the network and subsequent processing is described in other sections of this publication). The observer's role is to deliver information between parties while overseeing the Validator's work. PoSg also includes a blind signature element that guarantees anonymity within the network while entering information or signing so that the original content is not published. Any document that is delivered open, modified, with corrupt honesty (see Double spending section) or with any other protocol violation will be declined by the network. For transactions, only one commission group can be assigned to one wallet (the commission group consists of a Validator and an observer, or a group of Validators and observers). Double spending attempts are going to exclude one group automatically. In case envelopes processed by the network have not been modified, digital signatures are valid, timestamps also do not differ and no information that would disrupt the sums of control hashes or other information was false, the Validator considers the transaction submitter valid and can continue to gathering information about checking the sum of balances against the last change receipt of the transaction submitter. Proof of signatory authentication and transaction validity authentication within the CRYUM network is designed after a standard system that works on the principle of notaries and is the highest instance of legitimacy. Of course, the CRYUM network does not rely on honesty in the network, but has a thoroughly designed system of conditional elements that can only end with two values – 0 and 1. Thus, the result can only be a single value of 0 or 1 and the result of regular fulfillment of cumulative conditions must be 1. However, the system may not wait for the result of sums of conditions, but it can stop the transaction at any time and decline it if any result is 0. More information is available in the Consensus section.

3.4 Timestamp

The CRYUM network uses timestamps on all levels of communication. It is the basic pillar of trust and irreplaceability of the document. It would be helpful to describe the creation of a timestamp by computing the hash (imprint) from the document to which we want to insert the timestamp and sending the hash to the certification authority. The certification authority then combines the hash supplied by us with its internal time generator (time is not detected from the sender but from the certification authority, thus time can not be faked by the creator of the document) and returns the generated timestamp that we store together with the original document. The process can be fully automated – without the need for human intervention both on the sender's side and on the certification authority's side.

Figure 4 Timestamp diagram





4. CRYUM NETWORK

4.1 Consensus

Consensus theory is an essential element of a decentralized network. It is a situation where nodes agree on e.g. balance, voting or other parameters necessary for decentralized networks to work properly. Since there is no central authority, the network itself has to rely on achieving a state where an information that is in a partial dispute is correct and validated. Consensus has a drawback, for example, the intrusion of bad nodes – intruders, who would try to gain an image of legitimacy to the system and push for their own interest, such as convincing the network of a different account balance. Consensus in the CRYUM network represents the majority vote, which is formed by the mutual consent of group members (nodes). Consensus admits the consent of majority, but also the presence and expression of minority disagreement, which poses a difficult task for nodes – to agree on a correct outcome, especially if there are group members that did not receive information, for example about first deduction, and their result would appear as neutral behavior. Neutral behavior is a display of results demonstrated by nodes performing the state of abstention from voting. In this case, the result value is not „0“ but a blank string. It is a special case when the sequence has a length of zero – „“. Thus, there are no symbols in the string. Consensus is a hard to describe calculation that appears to be correct. It is a set of mathematical operations and logic so that step-by-step decision making comes to a successful end. Blockchain considers all blocks that have been stored to be correct. A possible result in blockchain is that the node with the longest block chain is considered true. Branchpipe allows real-time comparison of short chains for individual transactions, making it work faster. Consensus is then the perfect match of e.g. last balances and checksums that are compared with stamps which are represented by the majority of participating nodes with a valid network registration. One of the features we could use is to reach consensus by using the statistical function modus(x). Modus is the most frequently occuring value. However, we must not forget that the real value of consensus must by approximately 2/3 or 66% of the parties involved including nodes that did not show any value and their chain length state is = „0“. These nodes show chain length = „0“ only if e.g. there is no Lhtx (this is an occurance while getting the „balance“ value with a zero value deduction receipt, i.e. we are going to make a transaction for the first time).

Expression of consensus by using: mod(x).

Mo_b = mod (b1 , b2 , ... , bn);
Mo_b = x,y,z;

Conflict in decision making:

```
int arr[ ]  = { x, y, z};
int size =  * (&arr + 1)  - arr ;
size ;  // count mod = 3
if  size > 1   =  false / repeat consensus
```

Mo_b = mod (b1 , b2 , ... , bn);
Mo_b = x;

Correct decision:

```
int arr[ ]  = { x };
int size =  * (&arr + 1)  - arr ;
size ;  // count mod = 1
if  size  = 1   =  true /  = mod = x
```

Expression of percentage ratio for agreeing with value mod(x)

Registered nodes	RNn = TrNn = (RN_1 + ...) = 100u
Unregistered nodes	XNn = TxNn = (XN_1 + ...) = 130u
Nodes total	TNn = TrNn + TxNn = 230u

if TrNn = 100u = RNn = 100%
if TNn = 230u = XNn = 230%
if TrNn ≥ TNn = true
if TrNn < TNn = false

TrNn = 100u

$Mo_{b\,=}$ mod (b_1 , b_2 , ... , b_{100});
$Mo_{b\,=}$ **x;**
CountNodes = 78u from 100u
$Consenus_X$ = Cn > 2/3 = Cn > 66,66u = Cn > 66% = true

The example mentioned above is one of the possible solutions of match on nodes that hold the requested amount. It uses the function mod(x), which is the most frequently occuring value within a given statistical set. Thus, if nodes deliver a value into the statistical set, it is then very simple to calculate which value occurs most frequently on the nodes. The question remains whether to take into account nodes that have participated on the consensus or to take into account the credibility of these nodes while defining the ideal extent of consensus from the total number of registered nodes against the result of mod(x). For example, it can be 2/3 = 66,66%.

4.2 Transactions and Payment Verification

Transactions travel across the network as a submitted document of trust for paying the entered amount to another person with the certainty that the transaction will be carried out correctly without fraud (this is the system analogy). If all conditions were met, funds will be added immediately. Nobody can modify the document’s content additionally and it will be permanently stored in the pipeline as a change receipt of our own account, which is known as a ledger. Transactions are declined without any exception if they do not meet any condition of the system algorithm as a control product of results from each algorithm involved in processing the operation. In addition to adhering to the network protocol, it is also required to: reach a consensus, count sums, compare, check signatures, check the status of $L_b > 0$, acquisition and verification of a valid output hash from the last known deduction receipt, etc.

If all information is correct and each algorithm ends with the value „1“:
Then the following applies:

$$\text{result state} = R_a = (A_1 * A_2 * \dots\dots A_n) \quad = \; 1 \quad \text{true}$$

If any algorithm ends with the value „0“:

Then the following applies:

$$\text{result state} = R_a = (A_1 * A_2 * \dots\dots A_n) \quad = \; 0 \quad \text{false}$$

The probability of an impossible occurance equals zero: $P(0) = 0$, the probability of a possible occurance equals one: $P(\Omega) = 1$ and for the probability of any occurance A, the following applies: $0 \leq P(A) \leq 1$. The system will use this probability every time it receives the value „0“ from the sum of the results of algorithms. Example: $R_a = (1*1*0\dots..)$; generally, the previously mentioned equation applies to the CRYUM network for all types of processes that run across the network.

In case of a result $R_a = 1$, the transaction is recorded into a part of the pipeline and all other nodes receive information for future transactions. At a given time, it is possible to carry out several transactions at once indepent of each other. Thus, each transaction has its own validator (notary), observer (witness) and transactor (transaction participant).

In case the result $R_a = 0$, the transaction is discarded and ledger deduction can not be carried out. In this case, the last known records are valid without change. Funds are never going to be substracted from the sender and added to the recipient. The process of carrying out the transaction is cancelled as a process and begins again from start.

4.3 Double spending and illegal transaction

Double spending poses one of the risks of decentralized networks because someone is going to attempt to withdraw their own funds for example twice, resulting in a sum higher than balance. Another problem is the withdrawal of funds that we have never owned or withdrawal of more funds than we actually own. To be able to carry out any payment, we have to be „invited“ into the network first by addition of funds to our account and thus the actual possible deduction of funds creates us an adapter that connects us to our own chain. The adapter is bound by a chain so that it contains all input information that allows us to carry out our first future transaction. If we do not have an adapter, none of the nodes will allow us to carry out a transaction. Double spending if an adapter exists: If an attacker attempts to withdraw funds twice, a vote on the composition of the commission shall also take place twice. The protocol allows for the ongoing transaction to appoint only one commission. If a commission exists and we create another commission, the original one composed of nodes will nullify its instructions, making the operation invalid. Furthermore, every transaction is arranged in its own chain with its own output hash, which can only exist in the network once, never twice. On the other hand, transactions in blockchain are put into blocks and then the blocks are connected in a chain. Unauthorized withdrawal of funds provides a number of elements that prevent this operation if all nodes have information about our balance and transactions that are very short because it is only a part of a branch and thus it is impossible to substract a value higher than we own. It is also necessary in the case of blind signatures to inform the nodes about the amount we want to transfer and how much we own. If an attacker sends false information about their own balance, their transaction is never going to be accepted and will be automatically declined.

Example:

User		Cryum networks / nodes	Result
My balance:	$M_b = x$	if M_b != C_b	false
Sending amount	$S_a = y$	if $S_a > M_b$	false
		if $S_a > C_b$	false
		if $M_b == C_b \geq S_a$	true

Diagram false:

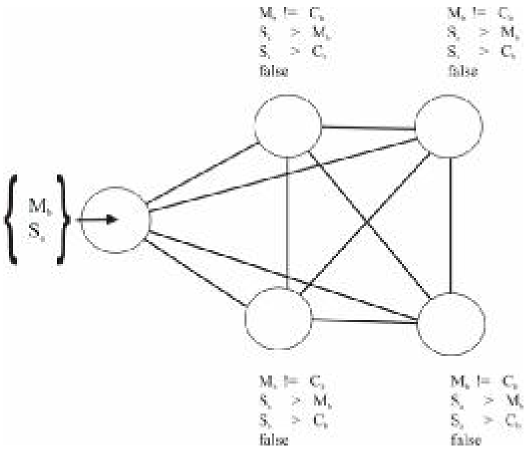
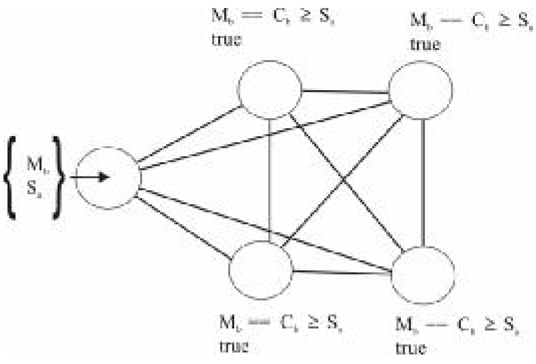


Diagram true



4.4 Wallets

GettBit is the first instant wallet in the world and is usable within the CRYUM network for managing digital assets. The wallet is created by processing access codes and remains active until logout. This means that there is no wallet access data stored in the entire network. The system allows you to create access codes through a sophisticated algorithm and use them for online communication whenever needed, even when the wallet is not registered in the network. This ensures maximum anonymity, as the system does not require email, username, phone number or IP address. All transactions created within the CRYUM network are anonymous and only transaction participants can reverse check a transaction through a transaction explorer within the wallet. Nobody can ever delete, modify, block or steal a wallet, even in the case of an attack. Two users can not have the same wallet within the system. Keep in mind that if you lose your wallet access code, it is impossible to recover it and activate your wallet.

Wallet address format: CRYUMNq8ZcXxX...

4.5 Smart Contract

In 1994, Nick Szabo, a legal scholar and a cryptographist realized that a decentralized ledger could be used for smart contracts, i.e. block contracts or digital contracts. In this format, contracts could be converted to a computer code, stored and replicated in a system and controlled by a network of computers that operate a block chain. This would also lead to feedback such as money transfer and receiving a product or service. Smart contract is defined as trust between a user and a computer system that processes a withdrawal receipt and provides a change receipt against the asset recipient and sender so that the transferred content is not modified, stolen or transferred to another person. The CRYUM network provides a myriad of solutions. An example is the use of a token that a user has received while mining – the network believes that the token has been acquired legally and the user’s asset (reward for his work) will be added to their account.

4.6 Privacy and Trust

The fundamental problem of one of the five rules CRYUM 5R was to define privacy. Many decentralized networks act as anonymous, but actually carry enough publicly available information to track a transaction. Unless it is within a network, there is a huge amount of wallets that associate identity with a transaction. They are wallet services that, in addition to wallet information, often require data such as email, name, etc. This data then simply associates transactions with digital wallet owners. CRYUM is designed so that nobody knows who submitted a transaction to whom. It is impossible to read any information that could identify a user from any operation in the network (balance acquisition, transaction) that is delivered or mediated to a user, e.g. a request provided by an observer node. All users in the network except their own wallet addresses use a dynamically assigned network ID (ae4aa4b12fe...........) for each specific operation and wallet address is converted to a hash. The idea of integrating anonymous transactions into the network is based on the work of David Chaum from 1983 called „Blind signature for untraceable payments“. It was this publication that has developed the idea of implementing, among other things, the theory of Blind signatures, which also comes from this author. If there is no information in the network that can be identified and it will not be stored in a readable form, it is impossible to associate the physical sender or recipient of the transaction with e.g. the wallet address or the transferred amount. Transactions can be verified only by the parties involved by using a control hash. If this receipt is stolen or used by another user, the result will be = „0“.

4.7 No Fees

The entry parameter of the network's functioning does not impose any additional costs connected with energy consumption or more demanding hardware that would carry out countless calculations. For this reason, transferring digital asset within the CRYUM network is absolutely free. Free transfer is an ideal platform for using the CRYUM network for common financial operations, micropayments or e-commerce payments. Free transactions are one of the basic rules (5R).

CONCLUSION

We have tried to bring you closer to the functioning and principles of BP technology - BP-Tx in detal, which is described in this document. For a deeper explanation of BP and network integration, it would be necessary to write a more detailed study that would cover specific features and processes of how it is possible to combine elements as required so that it can answer various questions of readers. However, the document discusses the principle that was designed to make the current blockchain technology more efficient. The technology - BP-Tx (Branchpipe Transaction) in combination with a number of innovations and elements taken from real life, such as the creation of the basic C-PoSg protocol, have achieved an effective tool for transferring digital asset. The result of this work is a combination of innovation, technology and protocol that can handle transactions in the network quickly, securely, reliably and without consuming energy. We defined the basic five rules (5R) that we wanted to implement into current definitions of cryptocurrencies to eliminate shortcomings and to make cryptocurrencies an effective tool for exchanging digital asset without a central authority, or to use the technology for other decentralized applications ("dApps"). Thus, CRYUM now represents the ability to transfer transactions from one continent to another for free. It is possible to transfer the lowest possible amount of CYM with no transaction fee, which makes CRYUM the perfect tool to be used in micropayment networks or in payments for goods and services online or in real life. Furthermore, CRYUM introduces zero energy consumption for its mining and issuing coins into circulation, thus ensuring validation of transactions. We have defined a green currency that consumes 0 Wh of energy, compared to conventional networks. By integrating blind signatures, the C-PoSg protocol, consensus and other elements described in this document, we have achieved absolute anonymity while using the network and transferring digital content. The BP or BP-Tx has managed to store a transaction instantly and has made it possible to create instant transactions without delay for all participants at a given moment and not be bound to filling blocks with delayed transactions. We believe that BP-Tx is an innovative way and a leap forward for next-generation distributed systems for exchanging digital asset. The BP-Tx system deliveres almost zero latency and allows a myriad of transactions to be processed at once with the ability to work with several different types of digital asset at the same time.

REFERENCES

Elkamchouchi H, Abouelseoud Y., Vol. (2)–No (2), A New Blind Identity - Based Signature Scheme with Message Recovery, The Online Journal on Electronics and Electrical Engineering (OJEEE) https://www.researchgate.net/profile/ Yasmine_Abouelseoud/publication/220336776_A_New_Blind_Identity-Based_Signature_Scheme_with_Message_Recovery/links/55e0032708aede0b572bb906/A-New-Blind-Identity-Based-Signature-Scheme-with-Message-Recovery.pdf

Fischer, Michael J., Nancy A. Lynch, and Michael S. Paterson. (1985) “Impossibility of distributed consensus with one faulty process.” Journal of the ACM (JACM)

Gatewood Tim, (2015), Verifying the Identity of the Signer, by American Association of Notaries http://www.notarypu blicstamps.com / articles/verifying-the-identity-of-the-signer/

Hamacher C., Vranesic Z., Zaky S., Manjikian N.,(2012). „Computer Organization and Embedded Systems“, McGraw-Hill, ISBN 9780077418809, 710 p

Chaum D., (1983). „Blind signatures for untraceable payments“, Advances in Cryptology Proceedings of Crypto. 203p.

Chaum D. (1983) Blind Signatures for Untraceable Payments. In: Chaum D., Rivest R.L., Sherman A.T. (eds) Advances in Cryptology. Springer, Boston, M

Marr B., (2018) , The 5 Big Problems With Blockchain Everyone Should Be Aware Of https://www.forbes.com /sites/ bernardmarr/2018/02/19/the-5-big-problems-with-blockchain-everyone-should-be-aware-of/2/#4eaa61ed67bc

Miller V.S. (1986) Use of Elliptic Curves in Cryptography. In: Williams H.C. (eds) Advances in Cryptology — CRYPTO ’85 Proceedings. CRYPTO 1985. Lecture Notes in Computer Science, vol 218. Springer, Berlin, Heidelberg

Nakamoto S, (2008). Bitcoin: A Peer-to-Peer Electronic Cash System Satoshi Nakamoto https://bitcoin.org/bitcoin.pdf

Shamir A. (1985) Identity-Based Cryptosystems and Signature Schemes. In: Blakley G.R., Chaum D. (eds) Advances in Cryptology. CRYPTO 1984. Lecture Notes in Computer Science, vol 196. Springer, Berlin, Heidelberg.