FEBRUARY, 2018

POSITION PAPER

V. 2.1

ENECUUM

Contents

1. Abstract **3**

2. Disclaimer **4**

3. Introduction 5

3.1. Scalability 5

3.2. Security 5

3.3. Privacy 6

4. Product Description **7**

4.1 Transactions 8

4.2 Blocks 10

4.3 Branches 11

4.4 Hybrid Consensus Algoritms (PoW, PoA, PoS) 13

4.5 SHARNELL Smart Contracts 14

4.6 Jettons and Marks 15

5. Problems and Solutions 17

5.1. Scalability 17

5.2. Security 18

5.3. Privacy 19

6. Use cases **20**

6.1 ICO Platform 20

6.2 Banking, Corporate, Insurance Companies 20

6.3 Distributed Computations 21

6.4 Decentralized Storage 21

6.5 Micropayments, Fintech Services and IoT 21

7. List of References 23

1. Abstract

Currency is to economy, what language is to speech with a natural historic competition, borrowed features, and things lost in translation. A language evolves in direct proportion to the number of its users and with the amount of pronounced/written/read material, i.e. “transactions” carried in it. What keeps it alive and saves it from extinction is its circulation and the Darwinist ability to adapt to a change. Most traditional currencies developed naturally, similar to most dialects, whereas constructed languages had little to no chance of survival, in spite of their claim to a global success due to well-planned features and lack of such artifacts as, say, irregular verbs.

Now that we’ve entered the world of cryptocurrencies and the blockchain, despite them being constructed languages of a sort, it is becoming clear that the acquired ability to adapt to a change is what makes a platform a preferred means of transaction. While many known blockchains have rigid and clumsy designs, Enecuum’s one is highly adaptive and truly decentralized, with participants being able to vote for desired new changes with no entailing protocol modification. Yet, if needed, changes in the blockchain parameters can also be introduced through a modified protocol version. You will find all the technical explanations below sharing the same core idea: We trust that our enhanced privacy, security and scalability, and, more importantly, ability to change and adapt make Enecuum the blockchain of tomorrow that comes to stay.

It is CONSTRUCTED TO LIVE.

2. Disclaimer

Waiting from KWM

3. Introduction

Since the Bitcoin creation in 2009, its underlying blockchain technology has opened up new prospects for the world economy evolution. The subsequent emergence of smart contracts [1] allowing to automatically conduct credible transactions on pre-determined conditions significantly expanded its application potential. We believe that the blockchain is capable of revolutionizing many areas of financial and economic activity, such as trade, financial markets, voting and even logistics.

Today almost all leading institutions engage in a competition to develop the best solution. The largest banks and corporations are forming consortiums, while governments are looking for ways to create a legal foundation for the technology.

Existing solutions, Ethereum being a most prominent, are already providing ample opportunities for their application in various areas. Nevertheless, for further development and mass popularization of the blockchain technology, it is necessary to overcome a number of problems that can be grouped into these three categories: Scalability, security and privacy.

3.1. Scalability

The flipside of all the advantages of a decentralized blockchain system is its limited bandwidth. In fact, most existing consensus-building mechanisms in the distributed registry present a trade-off between a large number of transactions per second and degree of network centralization [1]. Thus, the desire to increase the number of processed transactions often leads to growing risks associated with the system reliability. Besides, as the size of a blockchain grows, it demands more disk space, a wider Internet connection and higher computational power. All that may result in decreasing number of full nodes and have a negative impact on the security of the entire network (cf. 5).

3.2. Security

In addition to problems associated with scalability, there is a number of threats produced by various features of the blockchain architecture itself. For example, the Proof of Work-based transaction confirmation mechanism led to a high degree of mining capacities aggregation in China where the cost of electricity is one of the lowest in the world. This fact greatly increases various risks associated with the centralization of the system, for instance, an opportunity for conducting the 51% attack[2].

[1] Smart contract a.k.a cryptocontract - code that is stored, verified and executed on a blockchain. Smart contracts allow the performance of credible transactions without third parties.

[2] 51% Attack – a hypothetical attack on a blockchain done by a group of miners controlling more than 50% of the network's mining hashrate, or computing power.

Another source of danger is smart contracts which, unlike the blockchain itself, can be easier subjects to vulnerabilities and bugs that have already resulted in millions of dollars of losses for users and inflicted an irreparable damage to the industry reputation. The number of smart contracts in use will continue to grow, while existing ways of identifying their weak spots are still ineffective.

One more hot-burning issue these days is the network management problem due to effective power centralization through concentration of authority in the hands of a small clique, people who can present modifications to the core protocol [2]. If and when opinions of this group contradict interests of the community, it may lead to a conflict that can completely paralyze the process of system modernization that necessary for its stable development, and therefore lead to a split in the community (cf. 5).

3.3. Privacy

Most existing blockchain systems presume transparency of all carried transactions. It limits their commercial attractiveness and infringes individual privacy. While transparency is the one of the main advantages of a distributed registry, this property is not always desirable, especially when it comes to transfers between business counterparts, various financial transactions, and other kinds of transactions that users would prefer to keep private.

These issues are being confronted by a large number of developers working in dozens of different projects. As a result, more and more ad hoc blockchain platforms are designed every day to solve specific tasks in various areas. This brings to us to another problem related to cross-interaction of different types of distributed networks, and several cross-chain projects have already been launched to tackle it.

Nevertheless, a universal solution that effectively solves the above-mentioned problems in one protocol has yet to be presented. We are sure this solution is Enecuum, a blockchain system based on a fundamentally new structure that allows a full realisation of all advantages of the distributed registry technology in everyday life (cf. 5).

4. Product Description

Enecuum is a next generation decentralized blockchain platform with unique features that help implement an indefinite number of secure and well-scalable blockchain services and decentralized applications.

One of Enecuum's key advantages over other platforms is the HyperDAG[3] - a data model for storing and writing transactions, with flexible settings that offer new opportunities for practical application of the blockchain technology in the world economy. HyperDAG supports creation of separate branches where the rules can be tailored to solve any business problems including the one of quick and cheap handling a large number of transactions. Furthermore, this solution allows to integrate the sharding technology[4] that is successful in solving the scalability problem.

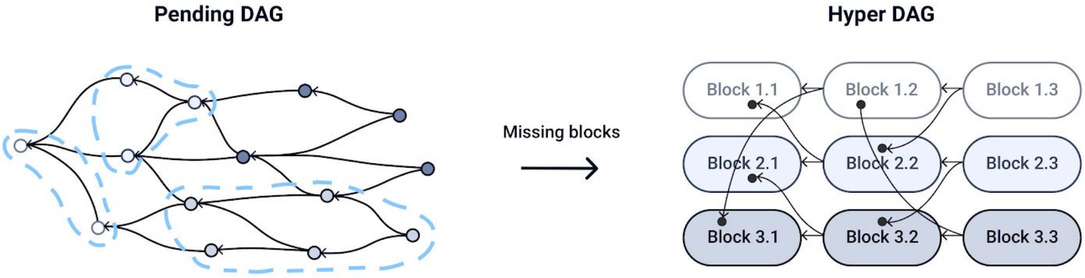

Figure 1. Pending DAG as a part of a HyperDAG

Enecuum uses a hybrid consensus algorithm combining the Proof of Work (PoW) [3], Proof of Stake (PoS) [4] and Proof of Activity (PoA) [5] algorithms. *The latter is applied for the first time in real life.* This combination makes it possible to confirm transactions from virtually any device connected to the network. That, in turn, leads to the maximum possible decentralization of the system and its high resistance to various types of attacks.

SHARNELL Smart Contracts[5] [20] also contribute to the high security level of Enecuum through the use of linear logic[6]. Linear logic allows to carry out a reliable automatic certification of smart contracts prior to their publication in the system guaranteeing an absence of potential vulnerabilities, misuse, freezes, deadlocks, and other undesirable outcomes.

[3] HyperDAG (Hyper Directed Acyclic Graph) - a graph in which a generalized edge can join any number of vertices.

[4] Sharding – the process of storing data records across multiple machines while keeping consistency of this data. Sharding is an effective approach to meeting the demands of data growth in the system.

[5] SHARNELL Smart Contracts – new type of smart contracts invented at Enecuum. These contracts consist exclusively of math formulas and business oriented linear logic. SHARNALL stands for Shared Noncommutative Exponential Linear Logic.

[6] Linear logic - a non-classical logic of actions and resources allowing to describe dynamics of processes and resource handling. It can be considered as a suitable interface between logic and computer science because it can manipulate the events of real world in natural way.

What is more, Enecuum is a highly adaptive system, inasmuch as the users can take part in its development and vote for other participants' proposals in regard to improving system functionality. There are two ways to factor in changes of system parameters:

Either to branch the project repository on GitHub[7] and present a modified version of the protocol (likely to be used by experienced developers) or to vote for adjustment of any network parameters that do not require protocol modification. The latter is provided by the system architecture and can be used by all holders of the ENQ cryptocurrency, after the test period when the voting algorithm is open for the users to present changes to the Enecuum's consensus model. During the test period, the Enecuum team effectively retains full control over the protocol for testing and debugging purposes.

Enecuum has been developed using Haskell, a programming language where the major characteristics are stability of execution and minimized chances of side effects, while a custom version of Cryptonight[8] [6] (Keccak + AES + X11) as the core cryptographic protocol has been chosen for its high resistance to ASIC devices.

The system currency is ENQ coins that are generated according to the system specific parameters and paid out to miners as a reward for spending their computational power. ENQ coins can be received and sent with no fees. They can also be used as a payment for publishing smart contracts into the network, performing complex mathematical computations on a smart contract, creating custom macroblocks, new tokens and branches, and participation in PoS mining.

4.1 Transactions

Today there are two main approaches to storing transactions in distributed registries: In the form of blocks (Bitcoin, Ethereum and many others) and in the form of a directed acyclic graph [9] (IOTA, Byteball, Universa). The advantage of the former is its high reliability that is achieved through 100% registry duplication among all nodes on the network. However, that approach imposes certain restrictions on the network speed and scalability. On the other hand, in the latter, DAG, there are no blocks, and every new incoming transaction refers to up to several previous ones effectively confirming them. As a result, registries of this type can quickly process large amounts of transactions, but their level of security raises certain concerns in the community [12].

We combined these two approaches and created a fundamentally new method for recording transactions called HyperDAG. Its key difference from the DAG is that a transaction entering the system can refer not only to a single previous transaction, but also to a group of them residing in a block (Figure 2). This way HyperDAG successfully combines advantages of both approaches and, at the same time, remedies their shortcomings, being able to process

[7] Enecuum at GitHub: https://github.com/Enecuum
[8] Cryptonight – a proof-of-work algorithm. It is designed to be suitable for ordinary PC CPUs, but currently no special purpose devices for mining are available.
[9] Directed acyclic graph - a directed graph that has a topological ordering, a sequence of the vertices such that every edge is directed from earlier to later in the sequence.

thousands of transactions per second while having a high level of cryptographic protection against attacks.

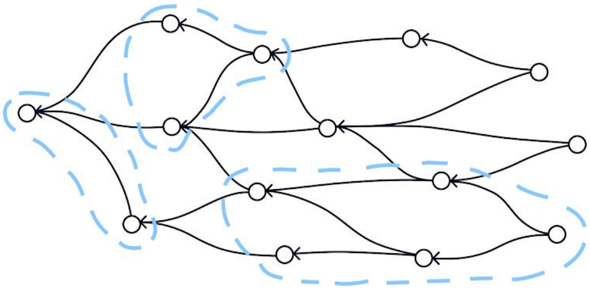

Figure 2. Principles of HyperDAG: Neighboring transactions are grouped into blocks

Such method of representing transactions offers vast opportunities for their sorting, analysis and sampling. For example, it is possible to create different branches (chains of blocks) in the frame of one network, and also apply the sharding technology that increases the network speed and eliminates the need for 100% registry duplication among all the nodes.

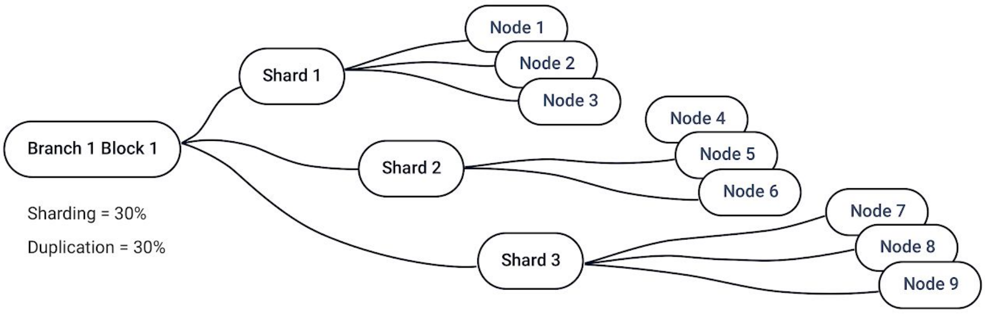

Figure 3. Sharding

In Enecuum, transactions have several parameters: Duplication[10], sharding and quality of service (QS; in our case the speed of a transaction). While duplication increases overall security of the system, it restrains its speed. Sharding produces the opposite effect. By default, duplication is given 30%, sharding - 30%, QS - none. The option to change these settings allows for easy scalability and creation of unique services within individual branches of the system.

[10] Duplication - duplicating data (transaction records, etc) on all nodes on the network to achieve a high reliability of the ledger.

4.2 Blocks

The moment HyperDAG accumulates a sufficient number of transactions to start assembling a block, the block creation process is started. Analyzing specified parameters of each transaction, miners determine its value for the system and add it into a corresponding block. Thanks to the introduction of double hash links to previous transactions[MD1], up to *n* blocks containing different transactions can be mined at once, which essentially accelerates transaction throughput *n-fold*. Limit of *n* is dynamic and can be, for example, *1000*, calculating to *1000 x 62 x 40 = 2,480,000* transactions per second, where 40 is the maximum number of transactions in the smallest block, *62* is the number of devices in a PoA team verifying transactions (64 members in a team in total), and *1000* is the number of blocks being mined simultaneously.

In Enecuum, the block size does not have a fixed value and may vary from 4 KB to 4 MB. Essentially, minimum size blocks can be created to reach the minimum delay in speed per operation, and as the load on the network increases, so does the block size. In case a user needs a block of the size bigger than 4 MB, the system also supports combining any number of blocks into a macroblock, i.e. a possibility to store unlimited volumes of data in the blockchain.

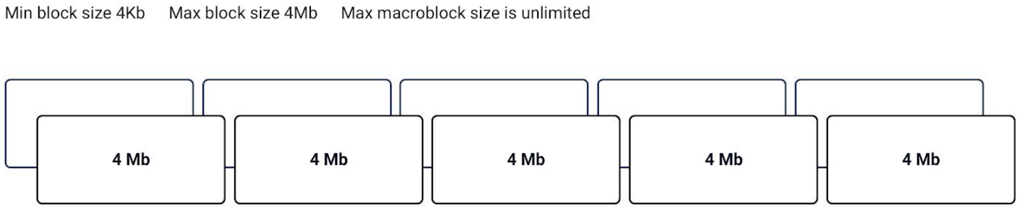

Figure 4. Varying block size

Bitcoin-NG protocol is introduced into Enecuum macroblocks [12] to reduce the latency between creation of blocks, so that each microblock inside a macroblock is created in realtime and adds transactions to the blockchain immediately upon their arrival. This way we do not have to wait until a macroblock is completed, its hash is found, and it is synced between all nodes on the network.

Structurally, a block consists of 3 main sections represented in the following picture:

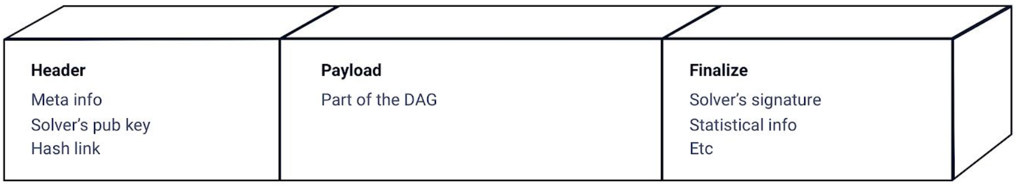

Figure 5. Block structure

4.3 Branches

Using HyperDAG to store transactions enables creating branches (chains of blocks) containing only homogeneous transactions. Each branch is, in essence, a separate blockchain, and, at the same time, is a part of the whole system. Each branch may dictate its own specific rules for creation and confirmation of new blocks. Nodes do not have duplicate all auxiliary Enecuum branches.

Schematically, the process of allocating blocks by branches is represented in Figure 6. Different colors represent transactions of different types that go into the appropriate branch.

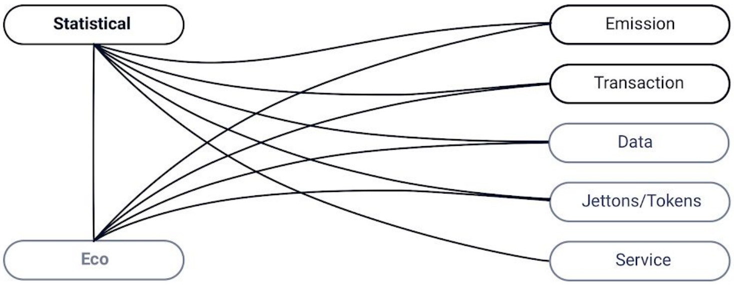

Figure 6. Allocation of different blocks to different branches

The main branches of the system are:

1. **The Transactional Branch** that includes all ordinary transactions between the users of ENQ.

2. **The Emissive Branch** that contains transactions generating new ENQ coins as mining reward.

3. **The Statistical Branch** that accumulates and analyzes statistics on the operations in the system. It contains data on the overall number of nodes, mining records, block sizes and a multifold of other parameters, incl. PoA mining reward sizes.

Also, Enecuum supports creation of an unlimited number of other branches of the following types:

1. **Ecological branches** to filter out for suspicious operations and transactions that failed validation. If, for example, a newly created wallet sends an unusually large quantity of outcoming transactions, they will first go to the ecological branch for a detailed analysis.

2. **Jetton[11] branches** to provide ample opportunities for implementing different scenarios. If, for instance, a user creates a jetton and issues tokens on its basis, all operations with this jetton and the tokens can be encrypted and stored in a dedicated jetton branch. Moreover, these jetton branches may have their own rules, e.g. all nodes can be recognized as valid, in turn transactions coming from them can be processed much faster, since there is no need for the consensus between all network members.

3. **Service branches** to create decentralized services, e.g. for polling, surveying, instant messaging, document management, etc. Transactions in service branches can include additional information thus reaching a high enough level of flexibility to solve any business problem using blockchain.

4. **Data branches** to introduce decentralized repositories. The principles of operation are similar to those of the BitTorrent protocol, however, instead of traditional hashing, Enecuum offers its own solution - the seamless hash algorithm[12]. It enables authorized access to a part of any size in the encrypted file, without rehashing and sharing the hashtable between the nodes again, which cannot be done in BitTorrent.

[11] Jetton - a system object, a cryptographic surrogate, serving as both an access key and base for tokens with a custom value.

[12] Seamless hash algorithm - Enecuum's invention, a hashing algorithm that provides a direct access to a file part of varying size without the need to recreate and re-distribute the hashtable between all the sharing nodes.

4.4 Hybrid Consensus Algoritms (PoW, PoA, PoS)

In Enecuum, consensus is achieved through interaction between the following three mining algorithms: Proof of Work (PoW), Proof of Activity (PoA) and Proof of Stake (PoS). This combination makes it possible to achieve the maximum degree of network decentralization, while significantly increasing both the network security level and its speed.

The transaction confirmation process implemented in Enecuum can roughly be divided into 3 stages corresponding the algorithms mentioned above.

There are two approaches to the first stage. The regular one is where miners connected to the PoW network calculate the hash for blocks of varied size, each for its own block, in parallel. After a hash satisfying current requirements for its complexity is found, a miner fills the block with transactions and translates it to the network for the second stage involving transaction verification by PoA miners. The second approach is for a PoW miner to calculate the hash, create a macroblock and hold it open for a team of PoA miners to fill it with microblocks containing transactions.

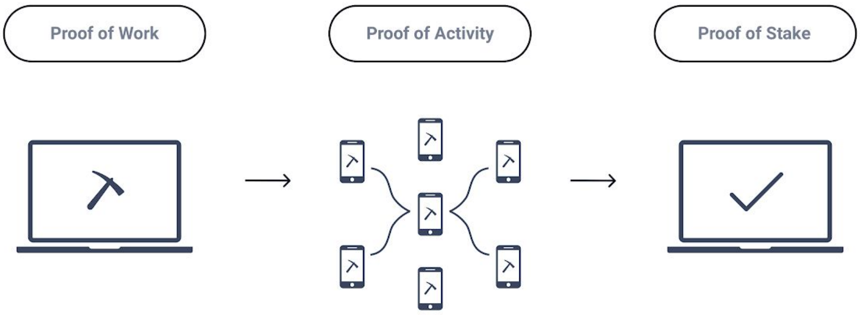

Figure 7. Hybrid consensus algorithm

During the second stage, PoA miners, divided into teams act correspondingly to the chosen PoW scenario. In case of the first PoW scenario described above, they check the hash in the translated block's header and verify the transactions in the block. In case of the second PoW scenario, they check the hash in translated block's header, create a microblock, fill it with transactions, and send it to the macroblock of the PoW miner. In total, a team send to the marcroblock 62 microblocks each containing 40 transactions. Then, depending on the transactions included in the block, attach PoA miners attach it to one of the system's branches. Checking the block hash for correctness does not require large computational capability, and this operation can be performed even by most simple devices, including a mobile phone. The same applies for microblock creation, filling it with transactions and transaction verification. The process of a PoA team formation involves calculating a hash to enter the team. Each team can have max 64 participants and is organized based on analysis of several parameters, including the node's geographic location and other parameters, in order to achieve the highest consensus security level.

During the third stage, PoS miners continuously re-check balances of all the wallets in the system. For this activity, PoS miners receive a portion of the mining reward, in the form of an interest. The interest depends on the miner's balance in two ways: First, the system defines the minimum and maximum balance thresholds outside of which a miners is not able to gain any interest whatsoever, and second, the interest grows as the PoS miner's balance grows from the minimum to maximum threshold.

In contrast to existing reward methods, where the network generates new coins immediately upon discovering a valid block, Enecuum, at this stage, issues marks[13] (see section 4.6 for details) that are added to the wallet balance, whereas the real mining payment is performed, on average, once a day. This way the system is protected against possible attacks on the mining algorithm as well as attempts to gain control over the majority of the computational capacities (e.g. through ASICS).

By default, the mining reward is distributed between the participants as follows: PoW - 70%, PoA - 20%, PoS - 10%. However, the presence of a statistical branch (cf. 4.3) enables the system to control this distribution scheme, protecting its interests from possible abuse.

4.5 SHARNELL Smart Contracts

Smart Contracts in Enecuum are written in JavaScript and executed on Google's V8 engine. The system supports two types of contracts:

1. "Light" (logical) smart contracts that are composed exclusively of mathematical formulae and based on the business-oriented SHARNELL linear logic. Linear logic is completely predictable, hence minimizing a chance of any potential vulnerability.

Logical smart contracts consist of a “data card” containing conditions and parameters, and the formula itself which takes into account these conditions and probabilities with the possibility of full or partial achievement and actuating. Each condition of a logical contract is placed in the data card and assigned a corresponding symbol. Later, a mathematical formula is created fully reflecting the terms of the contract. The π-calculus system[14] is used to ensure computations are run in parallel.

This type of contracts is ideal for performing the most common operations, such as multisig, escrow and so on. In the first version of our system they will be created via a graphical editor based on Petri Nets[15].

[13] Mark - in Enecuum, a special tag denoting a specific function of the tagged object.

[14] π-calculus - a formal algebra for concurrent, communicating and mobile systems. It provides a tool for the high-level description of interactions, communications, and synchronizations between a collection of independent agents or processes.

[15] Petri Net - a.k.a place/transition (PT) net, is one of several mathematical modeling languages for the description of distributed systems. A Petri Net is a bipartite graph that consists of two types of nodes: Places and transitions connected by directed arcs.

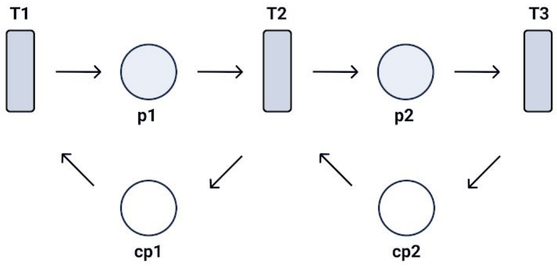

Figure 8. Smart contracts

2. "Heavy" smarts-contracts that contain code intended for solving more complex problems, such as conducting scientific calculations and training neural networks. They are executed in a dedicated branch of the system with a payment for the calculations. The payment is given in ENQ coins at a user-defined rate. They also use the π-calculus system, and channel system with session types.

4.6 Jettons and Marks

As was noted earlier, the system supports the notion of a jetton. A jetton is a cryptographic surrogate, similar to a token, and can be created by any user of the system. A jetton is used to create a dedicated branch where circulation of the ENQ coins is not intended. A jetton is used both as an access key to the corresponding branch and the decryption key for the transactions in this branch, and can be freely transferred between the users of the system.

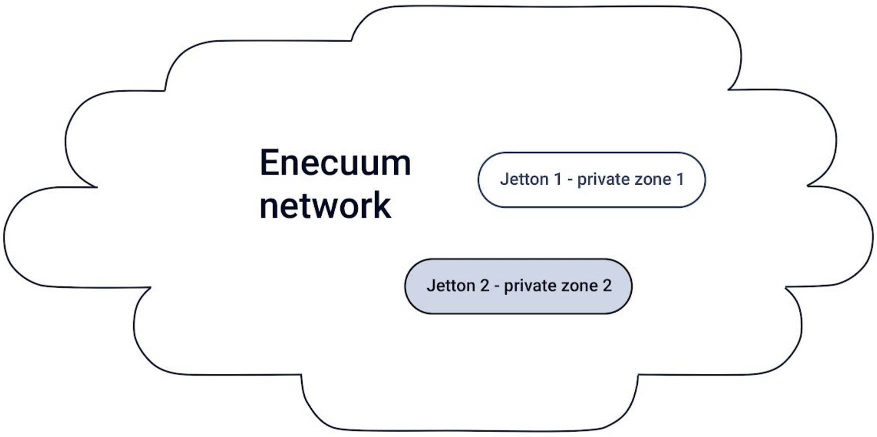

Figure 9. Jettons and jetton branches (Global ENQ network, Jetton branch #1, Jetton branch #2)

A jetton can be the base for tokens accepted for circulation in the corresponding jetton branch. Conversion of these tokens into the main system currency (ENQ) will occur via the corresponding jetton.

The key purpose of jetton branches is to facilitate creation of a blockchain-based flexible environment for easy interaction between businesses and their customers.

Marks are another tool that extends the functionality of Enecuum. Marks are used to label tokens, transactions or wallets and do not exist as a separate unit, but only coupled with a payment unit. Marks are used to denote specific functions of the tagged objects and ensure a strict execution of the stipulated terms or certain tasks. The purpose of a mark is final, cannot be changed and is determined prior to its creation.

The system provides the following types of marks:

- **Transaction Acceleration Marks that promote a higher speed or a transaction.**
- **Proofs Remuneration Marks** that are converted into ENQ coins upon data accumulation in the statistical branch (cf. 4.3).
- **Token Labeling Marks** that impose custom rulesets on the payment unit, e.g. limiting the list of actions applicable to the marked unit and stating it can only be transferred to the wallets containing a corresponding mark. This functionality facilitates effective management of state and corporate budgets, purchase control and directed loan management.

5. Problems and Solutions

5.1. Scalability

One of the most important problems facing an open blockchain system is that of cheap and secure handling of a large number of transactions, which is necessary for a global scale adoption and adaptation of the technology. The throughput of Bitcoin and Ethereum is often compared to the VisaNet system capable of processing over 50,000 operations per second [14] - a number thousands times greater than the current throughput of most popular cryptocurrencies. Given the number of cryptocurrency users growing globally at an enormous speed, the peak times fees for transactions in the current decentralized systems reach prohibitive levels rendering business implementation of those system useless.

A simple increase of block size may look capable of raising the number of processed transactions, but in fact is only a partial and temporary solution to the problem. The data in the block stored there permanently and that means the size of blockchain will keep growing steadily. With an increase in throughput, its size will grow even faster. As a result, only big corporations will be able to allocate enough resources to store and update this vast data set, which is likely to lead to an increasing centralization of the network.

Using HyperDAG (cf. 4.1) to record and store transactions, Enecuum is ideally suited for implementation of the sharding technology allowing for division of the blockchain into several smaller parts presented by separate branches or parts of those branches and processed in parallel. Combining sharding with varying block size, Enecuum can efficiently handle tens, even hundreds of thousands of transactions per second without jeopardizing the security of the system. The resulting commission for transactions in most cases is be zero or minimum.

In addition, the support of an unlimited number of branches in the system makes it possible to create on the basis of those branches various decentralized business applications, without the need for their own blockchain or more workload on the main Enecuum branch. Each branch can have a custom ruleset individually tailored to reflect service-specific needs. Furthermore, each branch can either be open for all the members of the system or be private with a defined list of participants. If the transaction speed or block size need to be upgraded in a certain branch, it can introduce its own nodes to modify the consensus rules. The only constraint in this case is the nodes capacity in this branch.

Enecuum’s architecture already supports macroblocks of unlimited size - a unique solution allowing the protocol to scale in parallel with the growing performance of modern CPUs.

5.2. Security

Low Decentralization Problem

First generation of blockchain systems used PoW for transaction confirmation. PoW is a reliable algorithm with a proved efficiency in protecting network from various types of attacks, such as DoS and spamming. As popularity and value of cryptocurrencies increased, PoW mining turned into a large-scale business with hundreds of millions of US dollars investments.

As a result, a low electricity and labor cost in China led to a massive aggregation of mining capacities in this geographic area. Naturally, this situation put the system security at jeopardy due to potential collusion between large pools of miners and an increased 51% attack possibility. The later emergence of ASIC devices further exacerbated the problem, as using regular mining rigs lost any economic sense, and led to an even higher degree of mining capacities centralization in the hands of large investors [16].

The combination of three types of mining and the use of the Cryptonight cryptographic protocol in Enecuum makes it possible to achieve a maximum degree of decentralization in the system, not only geographically but also in regards to different device types and social strata. All that makes Enecuum one of the most secure distributed registries. In addition to that, the presence of the statistical branch (cf. 4.3) in the system, collecting and analyzing blockchain status data, furthermore protects it from potential threats of various types evenly distributing the degree of influence on the consensus among all its participants.

Vulnerabilities in Smart Contracts

The invention of smart contracts gave the whole cryptocurrency industry a powerful push, but to
date their implementation has many weak spots. Once a smart contract is published in the blockchain, it is closed for modification, hence an error during its creation can result in multimillion-dollar losses for its users - a situation that happened not once in various cryptocurrency projects [16].

The existing methods of assessing the security of smart contracts mostly boil down to manual code audit by the developers in the community and are extremely inefficient, as the number of smart contracts being created grows outstrippingly fast and so does their complexity. Besides, Ethereum, the most popular platform for smart contracts, proposes to write them in a specific programming language, Solidity [17], which is yet to gain popularity in the developer community. It results in a drastic shortage of experienced Solidity developers and does not alleviate the problem.

The linear logic, used in the implementation of SHARNELL Smart Contracts, takes the security of this technology to a new level. It introduces reliable automatic testing of every smart contract before it is published in the blockchain this way minimizing chances of any errors and potential vulnerabilities.

In addition, the proposed languages is JavaScript, which is one of the most popular scripting programming languages, so a large number of professionals can engage in creating SHARNELL Smart Contracts effectively reducing the cost of smart contract development.

Centralization of Power over the Blockchain

The failed Segwit2x upgrade of the Bitcoin network and its hard-fork that resulted in creation of Bitcoin Cash speaks of disagreements in the community regarding the future of the first cryptocurrency [18]. Unfortunately, Bitcoin's architecture is arranged in the way that its miners, developers and ordinary users have different motives shaping their views on the need to present various changes to the protocol [2]. As a result, the community is split into separate groups, acting exclusively on their own interests, which slows down the process of evolutionary adaptation to changing market conditions and can effectively lead to system obsolescence.

Enecuum solves this problem by providing users with an equal opportunity to influence the platform improvement process by conducting an on-chain voting for users' proposals on any parameters optimization or introduction of new tools. Moreover, the implementation of any changes in the Enecuum blockchain will be a most secure process, as changes can be tested for potential failures in one of the auxiliary branches prior to their release in the main system branch.

5.3. Privacy

A popular belief is that cryptocurrencies are anonymous and thus provide ample opportunities for illegal activities. Indeed, despite the fact that all transactions inside the network are transparent and open, real individuals and companies behind them are unknown. However, this is not entirely true, since every operation in an open blockchain leaves a digital trace kept there forever, and a detailed analysis performed on this trace can help determine real counterparties with a high degree of accuracy. Hence, if intruders manage to match a public address with a real person or company, they can gain access to important confidential data and cause irreparable damage [15] [19].

The jetton branches (cf. 4.3) will offer Enecuum users a means for conducting transactions in a private mode minimizing risks of identity disclosure. A jetton is the key encrypting transactions in the branch, thus only its owners are be able to see details of the transactions carried in it. If ENQ coins, the main system currency, need to be introduced into the branch, a jetton also becomes a medium of exchange between the tokens issued in that branch and ENQ coins. This way a jetton serves as an encryption key reliably protecting transactions inside the jetton branch from outside attention, while using capacity of the entire network to confirm such transactions guarantees minimum delays.

6. Use cases

6.1 ICO Platform

The high throughput of the Enecuum blockchain allows startups to raise funds at any scale, without the risk of a network hang-up. Hence, all investors can be sure they can participate in the ICO and quickly receive their tokens. Since smart contracts in Enecuum are implemented in JavaScript, they are easy to write for any web developer, thus cost of their creation decreases significantly. In addition, the use of linear logic helps eliminate potential vulnerabilities in smart contracts and minimizes the risks of hacking.

The use of the “cancellation model” allows to implement complex crowdsales with step-by-step raising and return of the funds to the investors, at any stage of the process. System-specific notation of tokens, similar to the ERC-20 notation, simplifies of the tokens created on the basis of Enecuum to a cryptocurrency exchange service after the ICO.

6.2 Banking, Corporate, Insurance Companies

Using Enecuum’s jettons and marks, banks and government agencies are able to reliably control targeted spending of received credit and budget funds, and companies are able to conduct secure payments between themselves with no fear of sensitive information or trade secrets disclosure.

For instance, Bank A creates its own jetton and issues USD and EUR tokens on its basis. Having made an agreement with Bank B on substituting real USD and EUR with these tokens in conducted operations, Bank A transfers to Bank B this jetton as the encryption key. Now no one except for Bank A and Bank B can decrypt transactions containing these tokens.

As another example, Bank A that has a database of the customers with businesses serviced in it assigns different marks to these customers based on the nature of their business (construction company, industrial equipment supplier, etc). Now the bank can issue a business a directed loan in tokens having a specific mark, for this business to build a new production facility. The business can only use these tokens to pay certain predefined organizations, spending them according to the purpose of the issued loan.

Moreover, the possibility to add annotation to transactions allows to start a blockchain-based insurance service that keeps each client’s history. The service can keep user ratings directly in the blockchain and determine insurance coverage for each user by conducting automatic calculations via smart contracts.

6.3 Distributed Computations

The system ability to run "heavy" smart contracts in dedicated branches allows for performing complex calculations that require high computational power without increasing workload on the main Enecuum branches (useful for neural networks training, scientific calculations, rendering computer graphics, JS libraries, etc). Payment for using such “heavy” smart contracts is performed in ENQ coins at a flexible rate, similar to the transaction price concept in the Ethereum blockchain. Creating the request to perform the calculations, the customer sets the price and miners decide whether it is beneficial for them to provide their computational power for the task. In the case miners agree to the terms, the customer’s funds are reserved by the smart contract for future payment. When the task is completed and valid results are provided, the funds are released and automatically transferred to the miners.

6.4 Decentralized Storage

Application of the sharding technology and possibility to change the transaction duplication parameters allow for effective use of disk space on users' devices. For instance, if 4 users provide 5 GB of space each and the duplication and sharding parameters set to 50%, the effective storage capacity for files is 10 GB. Extrapolating these pattern to the entire network, the size of the “global decentralized disk” will grow proportionally preserving the availability of data and a sufficiently high speed of access. It means users can build on top of the Enecuum blockchain such services as decentralized hostings, cloud data storage services and content delivery networks.

Again, applying smart contracts and jettons as encryption keys on top of such data branches, users can create complex paid access services with decentralized (and immutable) content paid for in tokens.

6.5 Micropayments, Fintech Services and IoT

Regular use scenario implies zero fee for user transactions. Naturally, with the growing number of users and the emergence of decentralized applications on top of the Enecuum blockchain, the workload on the system will increase. However, the possibility to create separate branches with their own consensus rulesets that stimulates miners’ activity creates conditions beneficial for implementation of micro-transaction services.

In the case a micro-transaction service does not become centralized, the fee for its transactions remains zero. Even if such service starts making a lot of micro-transactions from a single wallet, only a small fee is levied. For example, for a microcredit service that makes 10,000,000 transactions a day, all its transactions can be easily recorded in several large macroblocks of 10 MB each. The fee will be calculated per block, thus it will be extremely low per transaction.

This is a perfect case to apply Enecuum's functionality to the Internet of Things. An implementation of a simple client for PoA mining on various devices will be able to completely cover their carried transaction fees. Besides, the Enecuum network protocol is designed to provide a high availability of such devices by establishing a mesh network[16] between them.

[16] Mesh network - A mesh network is a local network topology in which the infrastructure nodes connect directly, dynamically and non-hierarchically to as many other nodes as possible and cooperate with one another to efficiently route data from/to clients. Mesh routers can route data destined for other devices, while hosts are able to sleep for long periods of time.

7. List of References

[1] P. Kasireddy, “Blockchains don't scale. Not today, at least. But there's hope.,”2017. [On the Internet].
Available at:
https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a
[2] F. Ehrsam, “Blockchain Governance: Programming Our Future,” 2017. [On the Internet].
Available at:
https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74
[3] A. J. Markus Jakobsson, “Proofs of Work and Bread Pudding Protocols (Extended Abstract),” 1999. [On the Internet].
Available at: http://www.hashcash.org/papers/bread-pudding.pdf
[4] V. Buterin, “What Proof of Stake Is And Why It Matters,” 2013. [On the Internet].
Available at:
https://bitcoinmagazine.com/articles/what-proof-of-stake-is-and-why-it-matters-1377531463/
[5] C. L. A. M. M. R. Iddo Bentov, “Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake,” 2014. [On the Internet].
Available at: https://eprint.iacr.org/2014/452.pdf
[6] “CryptoNote Philosophy”. [On the Internet]
Available at: https://cryptonote.org/inside
[7] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. [On the Internet].
Available at: https://bitcoin.org/bitcoin.pdf
[8] Ethereum Foundation, “Ethereum Homestead Documentation,” 2018. [On the Internet].
Available at: http://www.ethdocs.org/en/latest/
[9] IOTA Foundation, “The IOTA Developer Hub,” 2018. [In the Internet]. Available:
https://iota.readme.io/
[10] A. Churyumov, “Byteball: A Decentralized System for Storage and Transfer of Value,” 2016. [On the Internet].
Available at: https://byteball.org/Byteball.pdf.
[11] Universa Corporation LTD, “Universa Blockchain Platform Whitepaper,” 2017. [On the Internet].
Available at: https://universa.io/files/whitepaper.pdf?v=1.3
[12] N. N. T. D. a. M. V. Ethan Heilman, “IOTA Vulnerability Report: Cryptanalysis of the Curl Hash Function Enabling Practical Signature Forgery Attacks on the IOTA Cryptocurrency,” 2017. [On the Internet].
Available at: https://github.com/mit-dci/tangled-curl/blob/master/vuln-iota.md.
[13] A. E. G. E. G. S. R. v. R. Ittay Eyal, “Bitcoin-NG: A Scalable Blockchain Protocol,” 2015. [On the Internet]].
Available at: https://arxiv.org/pdf/1510.02037.pdf
[14] J. Vermeulen, “VisaNet -- handling 100,000 transactions per minute,” 2016.[On the Internet].
Available at:
https://mybroadband.co.za/news/security/190348-visanet-handling-100000-transactions-Per-minute.html

[15] P. Kasireddy, “Fundamental challenges with public blockchains,” 2017. [On the Internet].
Available at:
https://medium.com/@preethikasireddy/fundamental-challenges-with-public-blockchains-253c800e9428
[16] M. B. a. T. C. Nicola Atzei, “A Survey of Attacks on Ethereum Smart Contracts,” 2016. [On the Internet].
Available at: https://eprint.iacr.org/2016/1007.pdf
[17] “Solidity,” 2017. [On the Internet].
Available at: http://solidity.readthedocs.io/en/develop/
[18] J. J, “No SegWit2x Makes Bitcoin Cash Shine Amidst Crypto Bloodbath,” 2017. [On the Internet].
Available at:
https://cointelegraph.com/news/no-segwit2x-makes-bitcoin-cash-shine-amidst-crypto-bloodbath
[19] J. Clifford, “Privacy on the blockchain,” 2017. [On the Internet]. Available:
https://hackernoon.com/privacy-on-the-blockchain-7549b50160ec
[20] “Deep Inference,” 2018. [On the Internet]
Available at: http://alessio.guglielmi.name/res/cos/