DEC, 2018

POSITION PAPER

V.2.2

Open Tomorrow Now

www.enecuum.com

Contents

1. Abstract

Currency means to the economy exactly what language means to the speech: with natural historic competition, borrowed features, and things lost in translation. A language evolves in the direct proportion to the number of its users and with the amount of pronounced/written/read material - “transactions” in it. What keeps it alive and saves it from extinction is its circulation and the Darwinistic ability to adapt to a change. Most traditional currencies developed naturally, similar to most dialects formalizing over time and gradually gaining success through adoption. Constructed languages have failed, in spite of their claim to a global success due to well-planned features and lack of such artifacts as irregular verbs.

Now that we’ve entered the world of cryptocurrencies and the blockchain, it is getting 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 platform 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 of 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 being BUILT TO LIVE ON.

2. Disclaimer

This whitepaper and any other documents published in association with this whitepaper relate to the intended development and use of the Enecuum platform (“Enecuum”). They are for information purposes only and may be subject to change.

- **This whitepaper describes a future project**

This whitepaper contains forward-looking statements that are based on the beliefs of Enecuum HK Limited, a Hong Kong incorporated company (CR: 2562183) (“**Company**”), as well as certain assumptions made by and information available to the Company.

Enecuum as envisaged in this whitepaper is under development and is being constantly updated, including but not limited to key governance and technical features. The ENQ token (“**ENQ**”) involves and relates to the development and use of experimental platforms (software) and technologies that may not come to fruition or achieve the objectives specified in this whitepaper.

If and when Enecuum is completed, it may differ significantly from the network set out in this whitepaper. No representation or warranty is given as to the achievement or reasonableness of any plans, future projections or prospects and nothing in this document is or should be relied upon as a promise or representation as to the future.

- **No offer of regulated products**

ENQ is not intended to represent a security or any other regulated product in any jurisdiction.

This document does not constitute an offer or solicitation of securities or any other regulated product, nor a promotion, invitation or solicitation for investment purposes. The terms of the purchase are not intended to be a financial service offering document or a prospectus of any sort.

ENQ does not represent equity, shares, units, royalties or rights to capital, profit, returns or income in the platform or software or in the Company or any other company or intellectual property associated with the platform or any other public or private enterprise, corporation, foundation or other entity in any jurisdiction.

- **This whitepaper is not advice**

This whitepaper does not constitute advice to purchase ENQ. It must not be relied upon in connection with any contract or purchasing decision.

- **Risk warning**

The purchase of ENQ and participation in Enecuum carries with it significant risks.

Prior to purchasing ENQ, you should carefully assess and take into account the risks, including those listed in any other documentation.

- **Views of the Company**

The views and opinions expressed in this whitepaper are those of Enecuum and do not reflect the official policy or position of any government, quasi-government, authority or public body (including but not limited to any regulatory body of any jurisdiction) in any jurisdiction.

Information contained in this whitepaper is based on sources considered reliable by the Company but there is no assurance as to their accuracy or completeness.

- **English is the authorised language of this whitepaper**

This whitepaper and related materials are issued in English only. Any translation is for reference purposes only and is not certified by the Company or any other person. No assurance can be made as to the accuracy and completeness of any translations. If there is any inconsistency between a translation and the English version of this whitepaper, the English version prevails.

- **No third party affiliation or endorsements**

References in this whitepaper to specific companies and platforms are for illustrative purposes only. The use of any company and/or platform names and trademarks does not imply any affiliation with, or endorsement by, any of those parties.

- **You must obtain all necessary professional advice**

You must consult a lawyer, accountant, tax professional and/or any other professional advisors as necessary prior to determining whether to purchase ENQ or otherwise participate in the Enecuum network.

3. Introduction

Since the Bitcoin's creation in 2009, its underlying blockchain technology has opened up new prospects for evolution of the the world economy. The subsequent emergence of smart contracts , facilitating credible automated transactions on pre-determined conditions, significantly expanded application potential of this technology. We believe that 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 compete to develop the best solutions. The largest banks and corporations are forming consortiums, while governments are looking for ways to create appropriate legal framework to support the technology.

Existing solutions and Ethereum being amongst the most prominent of them, are already providing ampleopportunities for the application of blockchain technology in combination with smart contracts. Nevertheless, for further development and mass popularization of the 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

A disadvantage of a decentralized blockchain system is its limited bandwidth.
In fact, most existing consensus-building mechanisms utilized by distributed ledgers 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 requires more disk space, a stronger Internet connection and higher computational power. All this may result in a 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 can lead to a high degree of mining capacity aggregation in one location: for example, there has been aggregation of bitcoin mining capacity in Mainland 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 a "51% attack".

Another threat to security arises in relation to smart contracts which are more susceptible to vulnerabilities and bugs than the blockchain itself, and have already resulted in millions of dollars' losses for users and inflicted damage to the industry. We expect that the number of smart contracts in use will continue to grow; however, the existing ways of identifying their weak spots are still inadequate.

Another important issue these days is the effect that centralization can have on blockchain direction and control. This may arise where there is power centralization in the hands of a small group of people who can effect modifications to the core protocol [2]. If and when the opinions of these groups contradict the interests of the community, it may lead to a conflict that can completely paralyze the process of system modernization necessary for its stable development. It can lead to a split in the community and the blockchain (cf. 5).

3.3. Privacy

Some blockchain systems strive for transparency of all transactions. However, we believe that this feature limits their commercial attractiveness and infringes individual privacy. While transparency is one of the main advantages of a distributed registry, this property is not always desirable, especially when it comes to transfers between business counterparts, particular financial transactions, and other kinds of transactions that users may legitimately prefer to keep private and confidential.

We believe these issues are being confronted by a large number of developers working on 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 another problem, related to the interoperability of different types of distributed networks – a problem that several cross-chain projects have already been launched to tackle.

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

4. Product Description

Enecuum is designed as a decentralized blockchain platform of the next generation with unique features that have the potential to help implement a large number of secure and well-scalable blockchain services and decentralized applications.

One of Enecuum's key advantages over other platforms is the "HyperDAG" which is a data model for storing and writing transactions, with flexible settings that offer new opportunities for the practical application of blockchain technology. HyperDAG supports the creation of separate branches where the rules can be tailored to solve numerous potential business problems including the ability to handle a large number of transactions cheaply and quickly. Furthermore, this solution allows to integrate the "sharding" technology that is successful in solving the scalability problem.

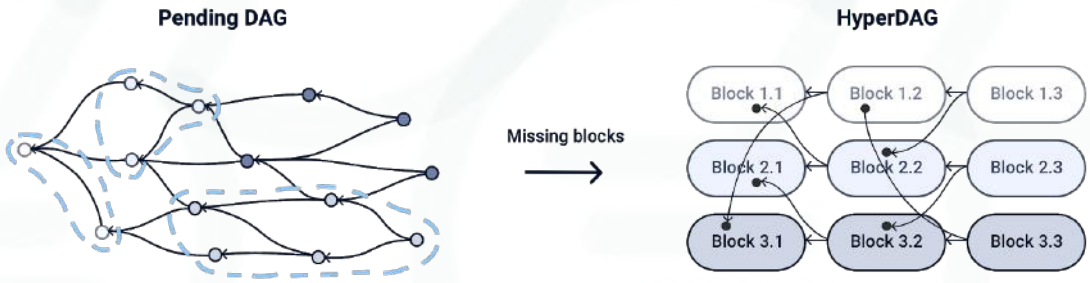

Figure 1. Pending DAG as a part of a HyperDAG

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 as part of its consensus mechanism. *PoA is proposed to be applied for the first time in a real world context through Enecuum.* Utilizing a combination of consensus mechanisms 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 makes Enecuum highly resistant to various types of attacks.

Enecuum has developed "SHARNELL Smart Contracts" [20] to operate on the Enecuum platform. These contracts consist of formulae and business oriented linear logic. SHARNELL Smart Contracts aim to contribute to a high security level within Enecuum.

Linear logic allows for reliable automatic certification of smart contracts prior to their publication to the system, which we believe significantly reduces potential vulnerabilities, misuse, freezes, deadlocks, and other undesirable outcomes in the system.

Another advantage of Enecuum is that it is a highly adaptive system. Users can take part in its development and vote for other participants' proposals for improving system functionality. There are two ways to factor in changes of system parameters:

- to branch the project repository on GitHub 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 ENQ. ENQ is the native cryptographic digital token proposed to operate on Enecuum. Following the test period, the voting algorithm is proposed to be open for the users to present changes to the Enecuum's consensus model. During the test period, the Enecuum team proposes to retain control over the protocol for testing and debugging purposes.

Enecuum has been developed using Haskell, a programming language used due to stability of execution and reduced chances of side effects. A custom version of Cryptonight [6] (Keccak + AES + X11) as the core cryptographic protocol has been chosen because of its high resistance to application-specific integrated circuit ("**ASIC**") devices.

ENQ's are proposed to be generated according to system specific parameters and paid out to miners as a reward for spending their computational power. Primarily, ENQs can be received and sent with no fees. They can also be used as a payment tool for publishing smart contracts to the network, performing complex mathematical computations on a smart contract, creating custom macroblocks, new Tickets, Tokens and branches, and participation in PoS mining.

4.1 Transactions

In our view, there are two broad approaches to storing transactions in distributed registries:

- as blocks (Bitcoin, Ethereum and many others); and
- as directed acyclic graphs ("**DAG**") - (IOTA, Byteball).

The advantage of the former is its high reliability that is achieved through 100% registry duplication among all nodes of the network. However, that approach imposes certain restrictions on the network speed and scalability.

In the latter, DAG, there are no blocks, and every new incoming transaction refers to several previous ones virtually confirming them. As a result, registries of this type can quickly process

large amounts of transactions, but their security level raises certain concerns in the community [12].

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 to apply the sharding technology to increase the network speed and eliminate the need for 100% registry duplication among all the nodes.

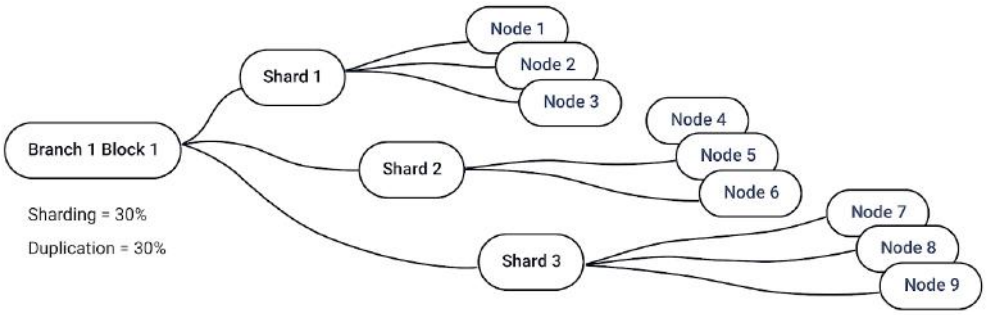

Figure 3. Sharding

4.2 Blocks

In Enecuum, the block size is not proposed to have a fixed value and may vary from 4 KB to 4 MB. Minimum-size blocks can be created to reach the minimum delay in speed per operation while possible, and as the load on the network increases the block size grows. In circumstances where a user needs a block of the size bigger than 4 MB, the system also supports combining any number of blocks into a macroblock, thereby allowing to store large volumes of data on the blockchain.

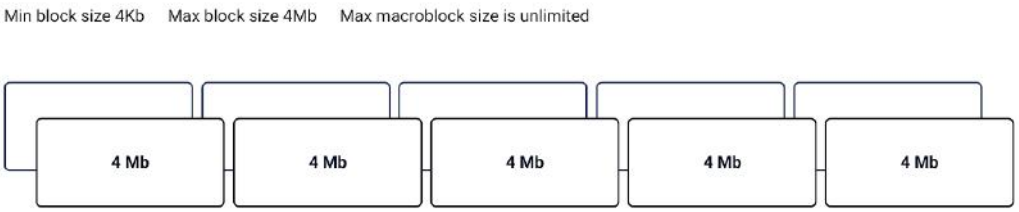

Figure 4. Varying block size

Bitcoin-NG protocol is proposed to be introduced into Enecuum macroblocks [12] to reduce the latency between the creation of blocks, so that each microblock inside a macroblock is created in realtime and adds transactions to the blockchain immediately upon their arrival. So, we do not

have to wait until an entire macroblock is completed, its hash is found, and it is synced between all nodes on the network – small microblocks can be generated concurrently inside it.

The block structure 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 set its own specific rules for creation and confirmation of new blocks. Nodes do not have to duplicate and store all auxiliary Enecuum branches.

The main branches of the system are proposed to be:

1. The Transactional Branch that focuses on storing all ordinary transactions between the users of ENQ.
2. The Statistical Branch that focuses on accumulating and analyzing statistics on the operations in the system. This branch contains data on the overall number of nodes, mining records, block sizes and a multifold of other parameters, including PoA mining reward sizes.

Also, Enecuum proposes to support the creation of other branches described below:

1. Ticket branches that focus on providing opportunities for implementing different scenarios through Tickets. Tickets are intended to allow for the creation of and access to dedicated, private blockchain branches, which we call “ticket branches” (cf. 4.6). If, for instance, a user creates a Ticket and issues Tokens on that Ticket branch, all operations involving this Ticket can be encrypted and stored in this dedicated branch. Moreover, these Ticket branches may have their own rules, for example, 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.

2. Data branches that can act as decentralized repositories. The underlying principles are similar to those of the BitTorrent protocol, however, instead of traditional hashing, Enecuum proposes to offer its own solution - the seamless hash algorithm. It is designed to enable 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.

4.4 Hybrid Consensus Algorithm (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 a high degree of network decentralization, while significantly increasing both the network security level and its speed.

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

Stage 1:

At first stage PoW miners find a proper hash for next block. After a hash satisfying the current complexity requirements is found, a miner translates it to the network.

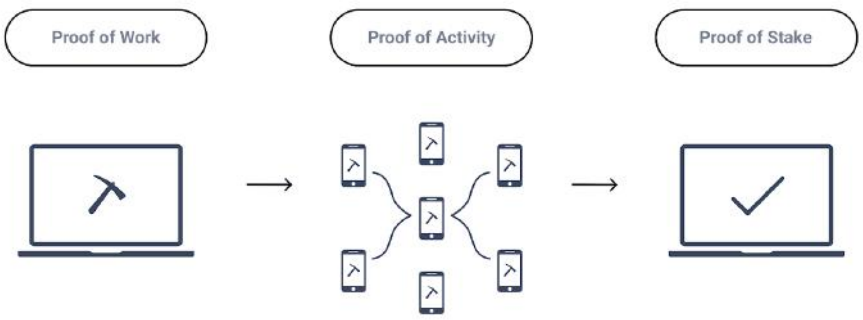

Figure 7. Hybrid consensus algorithm

Stage 2:

During the second stage, PoS miners use ID-based cryptography to obtain publishing key for certain K-block. This key is then split into shares and distributed among certain subset of PoA miners. This subset is defined by K-block.PoA miners then check the hash in the translated block, then create microblocks with transactions, sign them and send them back to the PoS.

Stage 3:

During the third stage, PoS miners collect enough confirmations for microblock from PoA miners, aggregate threshold signature and publish microblock.

By default, the mining reward is distributed between the participants as follows: PoA - 65%, PoW - 10%, PoS - 25%. However, the presence of the 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 to be written in JavaScript and executed on Google's V8 engine.

Smart contracts are to be composed exclusively of mathematical formulae and based on the business-oriented SHARNELL linear logic. Linear logic is completely predictable, hence minimizing the chance of any potential vulnerability.

Logical smart contracts are to consist of a "data card" containing conditions and parameters, and the formula itself which takes into account these conditions and parameters with the possibility of full or partial achievement and actuating. Each condition of a logical contract is to be placed in the data card and assigned a corresponding symbol.

This type of smart contracts is ideal for performing the most common operations and transactions, such as multisig, escrow and so on. They are proposed to be created via a graphical editor in the first version of our system.

5. Problems and Solutions

5.1. Scalability

One of the most important problems facing an open blockchain system is facilitating a large number of transactions cheaply and securely. Scalability is necessary for global scale adoption

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. As the number of cryptocurrency users is growing globally at an enormous speed, the peak times fees for transactions in the current decentralized systems can reach prohibitive levels.

We believe that a simple increase of block size is a partial and temporary solution to the problem, however it will not solve the underlying scalability issue. Currently, the data in the block is stored there permanently and this means the size of a 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, we believe that Enecuum is ideally suited for implementation of the sharding technology that allows 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 thousands of transactions per second without jeopardizing the security of the system. It is intended that the resulting commission for transactions in most cases will be zero or minimal.

In addition, the support of potentially unlimited number of branches in the system makes it possible to create various decentralized business applications, without the need for their own blockchain or more workload on the main Enecuum branch. It is possible that each branch can have a custom ruleset tailored individually to reflect service-specific needs. Furthermore, it is proposed that 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 needs to be upgraded in a certain branch, it is proposed that 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 is intended to support macroblocks of potentially unlimited size - a solution allowing the protocol to scale in parallel with the growing performance of modern CPU's.

5.2. Security

Low Decentralization Problem

First generation blockchain systems used PoW for transaction confirmation. PoW is a reliable algorithm with a proven efficiency in protecting blockchain systems from various types of attacks, such as Denial-of-Service ("**DoS**") and spamming. As the popularity and value of cryptocurrencies increased, PoW mining turned into a large-scale business with hundreds of millions of US dollars invested in mining projects.

Low electricity and labor cost in China led to a massive aggregation of mining capacities in Mainland China. This situation put the relevant blockchain system security at jeopardy due to potential collusion between large pools of miners and an increased “51% attack” possibility. The 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 capacity centralization in the hands of large investors [16].

It is believed that the combination of three types of mining and the use of the Cryptonight cryptographic protocol in Enecuum make it possible to achieve a high degree of decentralization in the system, not only geographically but also in regard to different device types and demographics. We believe that these features will help make Enecuum one of the most secure distributed registries. In addition to that, the presence of the Statistical Branch (cf. 4.3) in the system for collecting and analyzing blockchain status data will further protect Enecuum and its users from potential threats of various types by 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 currently their implementation has many weak points. Once a smart contract is published on 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 many times in various cryptocurrency projects [16].

The existing methods of assessing the security of smart contracts mostly boil down to manual code auditing by the developers in the community. It is submitted that this method of smart contract creation and testing is very inefficient. Especially taking into account that the number of smart contracts being created grows outstrippingly fast and so does their complexity. 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, in our opinion, does not alleviate the problem.

The linear logic, which is to be used in the implementation of SHARNELL Smart Contracts, seeks to take the security of this technology to a new level. It proposes to introduce reliable automatic testing of every smart contract before it is published on the blockchain. This in turn focuses on minimizing chances of any errors and potential vulnerabilities.

In addition, the proposed language of the SHARNELL Smart Contracts will be JavaScript, which is one of the most popular scripting programming languages, so a large number of professionals have a chance to engage in creation of SHARNELL Smart Contracts, which leads a reduced 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 highlight the potential disagreements in the community [18]. Unfortunately, the Bitcoin's architecture is arranged in a way that its miners, developers and ordinary users have

different motives, which shape their views on proposed changes to the protocol [2]. The competing interests have the effect of slowing down adaptation to changing market conditions. It may lead to system obsolescence if not resolved.

Enecuum is to solve this problem by providing users with a fairer opportunity to influence the platform improvement process by conducting on-chain voting for users' proposals on any parameters or new changes. Moreover, the implementation of any changes is to involve a 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. It is also a common belief that, 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].

Enecuum will provide a way to make anonymous payments in ENQ, converted to intermediate form. Emission of custom anonymous tokens also will be available for DApps.

6. Use cases

6.1 Token Emission Platform

The proposed high throughput of the Enecuum blockchain is to allow emit custom tokens, without the risk of a network hang-up. This tokens can be used for payments in DApps infrastructure. Token issuer will use all Enecuum benefits, like high-speed and zero-fee transactions. Since smart contracts in Enecuum are to be implemented in JavaScript, they will be easy to write for any web developer, thus cost of their creation is likely to decrease significantly. In addition, the use of linear logic helps eliminate potential vulnerabilities in smart contract code and helps minimize the risks of hacking.

Token issuers will be responsible for the appropriate design of their Tokens use cases and ensuring that their Tokens comply with all applicable legal and regulatory obligations.

6.2 Distributed computations

Enecuum aims to have the ability to run "heavy" smart contracts in dedicated branches. Enecuum also aims to permit 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 to be made in ENQ 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. If miners agree with the terms provided, 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.

6.3 Decentralized storage

The application of 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 are set to 50%, the effective storage capacity for files is 10 GB. Extrapolating this 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. This means that in the future users may build on top of the Enecuum Blockchain such services as decentralized hostings, cloud data storage services and content delivery networks.

6.4 IoT applications

Enecuum proposes zero transaction fees for a decentralized microtransaction service, and very low fees per transaction in case of a centralized microtransaction services that involve a lot of data from a single device. All generated data can be stored in blocks as transactions’ payload.

We believe this is a perfect use of Enecuum’s functionality in relation to the “Internet of Things”. An implementation of a simple client for PoA mining on various devices could 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 between them.

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/