White Paper

As an emerging technology, blockchain 4.0 is a fusion of scalibility, by increasing the speed of transaction per minute, with applicability of blockchain in real world industry 5.0.

Zilionixx technology will revolutionize blockchain as we know it. Zilionixx blockchain will support the improved version of existing products for sectors such as payments, supply chain tracking, healthcare data storage, perfect security solutions and more using the DAG-based aBFT consensus protocol and zk-snarks cryptography.

The convergence with artificial intelligence and equipped with sophisticated algorithms has been proven that blockchain technology of tomorrow adopted by zilionixx technology has made block chain today old-fashioned. Strong ecosystem backed by astonishing marketing policy would set in motion the zilionixx coin to be a market leader of cryptocurrency in the near future.

“ZILIONIXX TOMORROW BLOCKCHAIN TODAY!”

Contents

ZILIONIXX COIN

Blockchain technology has provided a way to maintain consensus across all nodes with no central authority. However the technology faces fundamental issues like a lack of real-time transaction settlement and scalability. Despite improved consensus algorithms, Some blockchain implementations such Bitcoin or Ethereum synchronize one block at a time. This results in slow confirmation times, one of the biggest factors stopping blockchain technology from being widely used across many industries. Although Smart Contract platforms such as Cardano and EOS have started to emerge, public Distributed Ledgers are still not widely used.

To solve these above issues, a new model based on the Directed Acyclic Graph(DAG) was developed. Zilionixx is a new DAG based smart contract platform that intends to solve the scalability issues of existing public distributed ledger technologies. The platform intends to distinguish itself from the traditional block ledger-based storage infrastructure by attempting to employ an improved version of existing DAG based protocol. The Zilionixx platform adopts a new protocol known as the “ZILION Protocol” to maintain consensus. The aim is to allow applications built on top of the Zilionixx Chain to enjoy instant transactions and low transaction costs for all users.

Zilionixx will provide a ZK-SNARKs cryptography to make a transaction as anonymous so that to encrypt all the data as a privacy. This cryptography will be used on several services like as medical/health care service and so on.

VISION/MISSION:

The mission of Zilionixx is to provide compatibility between all blockchains around the world and create an ecosystem which allows real-time transactions and data sharing(for example medical data) with low cost.

“MOST PEOPLE FAIL NOT BECAUSE THEY AIM TOO HIGH AND MISS BUT BECAUSE THEY AIM TOO LOW AND HIT!”

WHY ARE WE MAKING ZILIONIXX

The vision of Zilionixx is to provide compatibility between all blockchains around the world using fast DAG technology that can be deployed at scale in the world, and to create a new infrastructure with high reliability that allows for real-time transaction and data sharing.

Zilionixx has the intention of being used on a large scale in various industry verticals, such as medical service/healthcare, telecommunication, finance, logistics and IOT. The Zilionixx Foundation intends to create the Zilionixx platform along with a new Smart Contract-based ecosystem that can be used all companies and individuals around the world. The Zilionixx will lead the next generation of distributed ledger technology.

The platform intends to be open-source: used and changed by the community, and to provide various application support tools that can be used to create decentralized applications (DApps).

Issues with blockchain

Blockchain is a software innovation for establishing digital trust between users, and facilitates the transfer of value from one entity to another over a network. Its aim is to enable the safe preservation and remittance of capital without the need for a traditional public institution or middleman. Zilionixx believes that in order for blockchain technology to be used in real life with broad applicability, it needs to be easily transferable, irreversible, and the transaction fee must be small or zero. However, existing blockchain technologies have limitations due to slow confirmation times and potentially high transaction fees.

Issues of scalability

In existing blockchains, all nodes verify and store a single block at a time, leading to longer time in creating blocks and limitations in block size. Therefore, no matter how many nodes are connected, the performance will be limited by the speed of each node. The more transactions require processing, the worse the performance due to bottlenecks on the network itself. Thus, Zilionixx believes parallel approach is required.

Fees

The persons who develop applications need the pliability to offer low fee services to the users. The blockchain platform that is absolutely low fee for users will attain more worldwide adoption and then different and monetization strategies can be created by the businesses and developers. Various fees occur when exchanging value using blockchain. Major fees include transaction confirmation fees paid to block miners, and the block reward itself. These fees incentivise consensus participants, and secure the network against attacks such as DDOS and staking attacks. However, Zilionixx believes that these fees are prohibitively expensive for a scalable and enduring blockchain with a thriving ecosystem of users and applications.

Low Latency

An experienced user of any application always demands quick feedback or working of an application with no seconds of time using DAG technology. The applications which make delays while opening or working make the users irritated and they get offended by using these types of applications. This thing makes the applications less competitive. The platforms always support the low latency of transactions so that users always remain comfortable while using the application.

Easy upgrade and bug recovery:

The platforms who work on applications always need flexibility to increase the compatibility of applications with new updates and features. These platforms always support software and smart updates in applications so that users of these applications can get more benefits. All the decidable software subjected to bugs with the most conscientious of formal authentication. The software must be able to solve all the problems and fix the bugs when they suddenly or intentionally occur.

Sequential Performance:

Due to sequential dependent steps, some applications cannot be installed or implemented with smooth algorithms. To handle high volumes, applications such as exchanges need to perform in a sequence. Therefore, the platforms must follow or ensure the fast sequential performance.

Solution offered by Zilionixx

As a means to solve the problems of existing blockchain solutions, Zilionixx aims to develop a new implementation of DAG-based consensus, which intends to create a new platform that improves the scalability and versatility of existing DAGs. Zilionixx's technology is intended to create potentially infinite scalability, and process hundreds of thousands of transactions per second even with large numbers of nodes participating in the network.

The Zilionixx Chain is intended to solve the scalability limitations of existing blockchain with the Zilion Protocol. This is intended to be achieved by adopting a method where a single event block verifies the previous transaction, and transactions are verified and processed

asynchronously without being approved by the miners as in prior blockchains. Thus, increased transactional load will not lead to delayed approval or bottleneck effects. It intends to also manage historical information on its own without being assisted by external databases such as the Oracle Database. Event blocks that store information from transactions that arise include multiple data packages. A data package may include transactions, Smart Contracts, historical information, reputation management, and rewards.

The Zilionixx Chain intends to make the processing infrastructure in our society more transparent and reliable. With fast and safe processing methods based on DAG and independent management of historical information through “Story Data”, the Zilion protocol is intended to be expanded into various industries along with Smart Contracts.

ZILIONIXX TECHNICAL OVERVIEW

The Zilionixx Chain intends to solve the scalability issues of existing blockchain through the rapid processing of blocks on a large scale and to use a high-level functional programming language that compiles to smart contract bytecode on the Zilion Network. Zilionixx initiates a new blockchain planning mapped out to qualify vertical and horizontal going up of scattered applications. This is attained by making an operating system on which applications can be constructed or built. The software gives accounts, verification, databases, non-simultaneous communication and the organizing of applications across many CPU cores or collections. By the same token, distribution and segregation with A1 will make peer-to-peer real time micro lending and nano-insurance.

The authority of each cryptocurrency's coins is provided by a blockchain. A blockchain is a continuously growing list of records, called blocks, which are connected and secured using cryptography. Each block usually contains a hash pointer as a connection to a previous block, a checksum and transaction data. Blockchains are inherently resistant to upgradation of the data if design is to be considered. It is "an open, distributed registry that can record transactions between two parties effectively and in a verified and permanent way". For use as a distributed registry, a blockchain is typically managed by a peer-to-peer network collectively clinging to a protocol for updating new blocks. Once recorded, the data in any given block cannot be changed subsequently

without the changing of all subsequent blocks, which needs complicity of the network majority.

Blockchains are saved by design and are an example of a distributed computing system with high Byzantine fault liberality. Decentralized agreement has therefore been achieved with a blockchain.

The Zilionixx will be implement zk-snarks cryptography to make a transaction as an anonymous and this cryptography will be implemented on smart contract VM so that users can save their private data on blockchain. And this technology will be used on medical technology for the privacy information.

The Zilionixx will be combined with free TON to increase the speed of processing transaction and improve the scalability.

Consensus Algorithm

The Zilionixx blockchain will use a new consensus algorithm known as the Zilion Consensus Algorithm(ZCA), which is intended to significantly improve performance and security using DAG-based distributed ledger technologies. The ZCA intends to be a Byzantine Fault Tolerant (BFT) technology that guarantees a similar level of consensus as existing blockchains. It intends to not only prevents attacks caused by a specific node failure, but also to process up to 100,000 transactions per second. Zilionixx Chain intends to employ cryptographic techniques like as ZK-SNARKS and so on to enhance security when communicating between nodes and uses a functional programming language for full smart contract support.

The ZCA intends to form a “ZILION DAG” based on the DAG-based aBFT. A set of links between event blocks form a DAG, which is a distributed system that stores arbitrary data that cannot be changed. Event blocks contain information such as transactions, smart contracts, Stories (historical information), and the values of previous events. An event is connected to the previous event block with central authority manipulating the structure. Event blocks from the previous rounds achieve more verifications as future events blocks are added.

The ZCA intends to be fully asynchronous and when two identical transactions are requested (i.e. the double-spending issue), only the earliest transaction is validated. The order between transactions is arranged with aid from the Main Chain list

Components

ZCA operates the graph of the Zilion and consists of Events, Clothos, Atropos and the Main Chain.

Event Blocks

The Event Blocks includes Stored Data, Signature and hash values of the previous event block (one or more).

[Stored Data]: transaction, smart contract, history information, reputation management, reward

[Signature]: This is the signature of the user who created the event block.

[Hash Value]: Block Link

Like other Blockchain technologies, where the new event block verifies all previous event blocks (including the transactions inside them), all new Event Blocks will verify only their parent event blocks. A new event block will be connected to its parent event block through hash and all hashes will be derived from parent event blocks, so that it is impossible to modify or delete the previous event blocks. When an event block is connected, another node will build a new event block on top of that event block.

Flag Table

The Flag Table stores the connection data of specific event blocks (Clothos).

[Clotho Index]: Contains index information for each Clotho

[Connectivity]: Contains information about the connection with other Clotho

Clotho

Clotho is an event block that contains the Flag Table, and can see the supra-majority of blocks created in the path of previous event blocks

Atropos

Atropos is a set of special event blocks. It is appointed based on the informa- tion in Clothos and constitutes the Main Chain. It is also utilized in validation of event blocks in a specific stage.

Main Chain

The Main Chain consists of Atropos and related event blocks. The Main Chain intends to be used for the validation of event blocks and to maintain the entire network structure.

Procedure of Algorithm

The Zilion protocol can be represented by a graph where all event blocks are connected. There exists a chain that could be connected through set blocks and it is called the Main Chain. All event blocks can be created asynchronously from nodes and each of these event blocks consists of a set of transactions (payment, remittance, smart contract, story, reputation, rewards). The new event block is connected to the parent event block, which is the most recent previous event block, and the node is intended to generate the block at a high speed through the Zilion protocol.

The Main Chain is a set of event blocks that can validate event blocks created over a period of time. The ZCA can effectively solve various problems such as double-spending issues or malicious attacks by intentionally generating incorrect event blocks while maintaining the Main Chain. The Main Chain has an influence on the ordering between event blocks that

occur asynchronously. The Main Chain helps event blocks that occurred earlier to have a priority in the sequence. At the heart of the Main Chain is Atropos.

```
Zilion Consensus Algorithm
        loop
        parallel func 1
                create a new block on each Node
        parallel func 2
                Find_Atropos(all_blocks, atropos, clotho)
                Main_Chain(MC, atropos, clothos)
end loop

procedure Find_Atropos(all_blocks, atropos, clotho)
        atropos[]
        heap clotho
        heap lookup
        for each clotho c
                traverse flagtable c
                if find atropos_path then
                        atropos[c]++
end procedure

procedure Main_Chain(MC, atropos, clothos)
        heap MC
        heap clotho
        heap MC.last_block
        traverse lookup
        if find MC_path then
                MC append set of list
end procedure
```

Each node can freely create new events asynchronously at the same time. This differs Zilion from other blockchain technologies, in which the consensus requires every node to participate. The Zilion algorithm is intended to allow each node to create blocks in parallel. Each node will make a new event block asynchronously by sending messages to each other. The information will be exchanged to make a new solid chain.

The key factor of the Zilion Algorithm is to maintain the Main Chain which is significant for keeping the block in order. Finding the Atropos and the Clotho in the Zilion Algorithm is intended improve the speed of the Main Chain. The completed Main Chain should make

Zilionixx Chain secure and play a key role in implementing aBFT.

Consensus Algorithm in the future (DAG-based aBFT + TON)

Zilionixx uses the only known scattered agreement algorithm proven capable of meeting the performance parameters of applications on the blockchain. Those who hold tokens on a blockchain adopting the Zilionixx may choose block manufacturers through a continuous approval voting system under this algorithm. Anyone may choose to participate in block production and will be given a chance to produce blocks, provided they can agree token holders to vote for them.

The Zilionixx technology enables blocks to be built exactly every 0.15 second and exactly one producer is allowed to build a block at any given point in time. The block for that time slot is skipped if the block is not built at the given time. There is a 0.15 or more second gap in the blockchain if more than one block is skipped.

A producer is removed from consideration if a producer misses a block and has not produced any block within the last 24 hours unless they inform the blockchain of their reason to start producing blocks again. This makes sure the network operates smoothly by lowering the number of blocks missed by not scheduling producers who are proven to be unrealistic.

ADPOS blockchain does not experience any forks under normal conditions because, instead of competing, the block producers cooperate to produce blocks. In the event there is a fork, agreement will automatically switch to the longest chain. The rate at which blocks are added to a blockchain fork is directly correlated to the percentage of block producers that share the same agreement due to which this method works smoothly. As the fork with more producers will experience fewer missed blocks so that's why a blockchain fork with more producers on it will grow in length faster than one with fewer producers.

Furthermore, no block producer is allowed to produce blocks on two forks at the same time. If a block producer caught doing this will likely be voted out. The evidence of such double production may also be utilized to automatically remove abusers.

Byzantine Fault Tolerance is added to traditional ADPOS by allowing all producers to sign all blocks so long as no producer signs two blocks with the same timestamp or the same block height. Once 30 producers have signed a block the block is then not able to reverse. Any byzantine producer would have to produce cryptographic evidence of their treason by signing two blocks with the same timestamp or block height. The irreversible agreement should be reachable within 0.15 second.

Cryptography Algorithm

Zero Knowledge Proof

The zero-knowledge proof method is a cryptographic theory, which proves what kind of equation is true to the opponent without exposing any information.

A **prover** is the one which tries to prove that any kind of equation is true, and the one which participates in a certification process and exchanges information with a prover is called a **verifier**.

When a prover participates in a zero-knowledge certificate and modifies a protocol with the purpose of cheating the verifier, the prover is **untruthful**, otherwise **truthful**.

The zero-knowledge proofs must satisfy such as the following 3 properties:

1. Completeness: If any kind of equation is true, a truthful prover must be able to prove that the equation is true to a truthful verifier.
2. Soundness: If any kind of equation is false, any untruthful prover must convince an untruthful verifier that the equation is true.
3. Zero-Knowledge: If any kind of equation is true, the verifier must know nothing except for the authenticity of the equation.

The zero-knowledge proofs depend on the probability theory.

The proof method based on the probability theory becomes the Interactive Zero Knowledge Proof.

That is to say, it is an algorithm which judges true and false of the equation as the probability of true and false by carrying out the execution many times.

Such a system causes various problems such as a load on the network.

Then, the concept of non-interactive zero-knowledge came out.

The verification for proof, however, is due to the estimation of the calculation.

Non-interactive zero-knowledge proof is a method to perform verification without interacting with the prover as a type of ZKF.

ZK-SNARK (Zero-Knowledge Succinct Non-interactive Argument of Knowledge) is a concept brought up by non-interactive zero-knowledge proof, and it is also used in the Z cash.

Since there are many publications related to zero-knowledge, please refer to the reference to the specific contents.

ZK-SNARK (Zero-Knowledge Succint Non-interactive Argument of Knowledge) does not exchange any information between the prover and the verifier, however, the prover creates a proof scheme and provides a module that can be varified by the verifier. As an example, in the provider of that proof scheme, there is an algorithm that can be used to inform that it has the Secret Key.

Smart Contract VM(Virtual Machine)

Virtual machines (VMs) used by existing cryptocurrency platforms are mostly stack-based, such as the Ethereum Virtual Machine (EVM) of Ethereum. Stack-based VMs can easily execute instructions using the stack data structure. However, as explained below, stack-based machines have longer code lengths and slower performance speeds in general compared to a register-based machines. As a solution to machine Storage in DAG event blocks are expensive. As code uses such storage, a large number of instructions are expensive. The Zilion Virtual Machine (ZVM) intends to extensively reduce capacity and increase processing speed. Publications5 indicate that register-based virtual machines can reduce OPCODE execution costs by over 50% and improve performance capacity by nearly double.

Stack-based model

The Stack is a basic data structure. A stack-based virtual machine uses the stack to perform operations. Assuming that we are performing a simple addition, four command lines are required to perform additional manipulation using PUSH and POP manipulation. The advantage of a stack-based model is that the operand is implicitly processed by the stack pointer: calling a stack pointer provides the next operand (POP), and there is no need to

explicitly state the operand address.

Register-based model

In storing the operand, a register-based virtual machine models CPU registers. While there is no PUSH or POP instruction, a command must include the name of the pointer, the operand for a command is explicitly stated. For example, when performing an addition on a register-based virtual system, the command may be expressed as follows. You can see that this code is shorter than the earlier stack-based version

Compare Stack/Register

Stack-based model

Load A

Load B

Add

Store C

Register-based model

ADD AX, BX, CX

The Length of the command is different.

The register-based model command length is less than the stack-based model command length.

Recovery from Stolen Keys:

When keys are stolen then the Zilionixx technology allows the users a way to restore control of their account. Any owner key can be used by the account owner that was active in the last 30 days along with approval from their designated account recovery partner to reset the owner key on

their account. The control of account cannot be reset without the help of the owner.

There is nothing for the hacker to achieve by attempting to go through the recovery process because they already "control" the account. Furthermore, the recovery partner would likely ask for identification and multi-factor authentication (phone and email) if they did go through the process. This would likely compromise the hacker or gain the hacker nothing in the process.

This process is also very different from a simple multi-signature arrangement. With a multi signature transaction, another entity is made a party to every transaction that is done. On the other side, with the recovery process the recovery partner is only a party to the recovery process and has no power over the day-to-day money transfer. This dramatically lowers costs and legal responsibilities for everyone included.

Segregated Witness

The concept of segregated witness (SegWit) is that transaction signatures are not efficient after a transaction is immutably involved in the blockchain. The signature data can be trimmed once it is fixed and everyone can still utilize the current state. As signature represents a large percentage of most transactions while SegWit represents a remarkable savings in disk usage and synching time.

This same concept can be used for merkle proofs for inter blockchain communication. If a proof is accepted and logged into the blockchain irreversibly, the 2KB of shard has not been

necessary to derive the proper blockchain state. If we compare the inter-blockchain communication with the normal signatures then the savings are 32x greater in case of inter-blockchain communication.

Performance Of Zilionixx Chain

Using the unique Zilion Protocol algorithm, Zilionixx Chain intends to solve the issue of scalability with the fast processing of blocks. While third-generation blockchain technology might show improved performance compared to previous impliementations of blockchain technology, the speed of creating blocks might be still very slow. Zilionixx Chain intends to ensure high creation and processing performance of up to 300,000 transactions per second. With a high level of reliability and scalability, Zilion believes it is working on a strong third-generation blockchain technology which can be utilized on a large-scale across many domains and industries. Zilion chain intends to not only process large numbers of transactions at scale but also processes Story and historical data that can ensure the reliability of transactions.

ZILIONIXX LAYER

Zilionixx Core

Cryptocurrency

A cryptocurrency, crypto-currency, or crypto is a digital advantage designed to work as a medium of exchange wherein individual coin ownership records are set aside in a registry existing in a form of a computerized database using strong cryptography to save transaction records, to control the generation of additional coins, and to prove the transfer of coin ownership.

It typically does not occur in physical form like paper money and is typically not supplied by a central authority. Cryptocurrencies typically use segregated control as opposite to centralized digital currency and central banking systems. When a cryptocurrency is punched or created prior to supply or issued by a single supplier, it is generally considered unsegregated. When applied with decentralized control, each cryptocurrency works through distributed registry technology, typically a blockchain, that serves as a public financial

transaction database.

Bitcoin, first introduced as open-source software in 2009, is the first segregated cryptocurrency.

Many other cryptocurrencies have been created until the release of bitcoin.

According to Jan Lansky, a cryptocurrency is a system that meets six parameters:

- A central authority is not required by the system; its state is managed through distributed agreements.
- An overview of cryptocurrency units and their ownership is kept by the system. · The system describes whether new cryptocurrency units can be created. If new cryptocurrency units can be created, the system defines the conditions of their origin and how to find out the ownership of these new units.
- Ownership of cryptocurrency units can be proved particularly cryptographically. · The system enables transactions to be performed in which ownership of the cryptographic units is changed. A transaction statement can only be supplied by an organization verifying the current ownership of these units.
- If two different instructions for changing the ownership of the same cryptographic units are entered at the same time, the system performs at most one of them.

A blockchain account can provide functions other than making payments, for example in segregated applications or smart agreements. In this case, the units or coins are sometimes referred to as crypto tokens (or crypto tokens). Cryptocurrencies are typically created by their own blockchain like Bitcoin and Litecoin whereas tokens are usually supplied within a smart agreement running on top of a blockchain such as Etherium.

Decentralized cryptocurrency is produced by the complete cryptocurrency system collectively, at a rate which is defined when the system is generated and which is publicly known. In centralized banking and economic systems such as the Federal Reserve System, corporate boards or governments control the issue of currency by printing units of fiat money or demanding additions to digital banking registries. In the case of segregated cryptocurrency, companies or governments cannot generate new units, and have not so far provided backing

for other firms, banks or corporate organizations which hold advantage value measured in it. The fundamental technical system upon which decentralized cryptocurrencies are based was generated by the group or individual known as Satoshi Nakamoto.

As of May 2018, over 1,800 cryptocurrency identifications existed. Within a cryptocurrency system, the safety, integrity and balance of registries is managed by a community of mutually untrustworthy parties referred to as miners: who use their computers to help update and timestamp transactions, adding them to the registry according to a particular timestamping plan. Most cryptocurrencies are designed to slowly lower the generation of that currency, placing a cap on the total amount of that currency that will ever be in circulation. Compared with ordinary currencies held by financial institutions or kept as cash on hand, cryptocurrencies can be more difficult for takeover by law enforcement.

The Legal Concern of an Unregulated Economy

As the popularity of and demand for online currencies has enhanced since the inclusion of bitcoin in 2009, so have concerns that such an unsuppressed person to person global economy that cryptocurrencies offer may become a danger to the community. Concerns abound that altcoins may become tools for unknown web criminals.

Cryptocurrency networks show a deficiency of regulation that has been degraded as enabling criminals who want to avoid taxes and launder money. Money laundering problems are also present in regular bank transfer, however with bank-to-bank wire transfers for occurence, the account holder must at least supply a verified identity.

Transactions that occur through the use and exchange of these altcoins do not depend on

formal banking systems, and therefore can make tax avoidance simpler for individuals. Since drafting taxable income is based upon what a receiver reports to the income service, it becomes highly difficult to account for transactions made using existing cryptocurrencies, a mode of exchange that is critical enough and difficult to track.

Systems of obscurity that most cryptocurrencies offer can also serve as a simpler means to launder money. Rather than laundering money through a complex net of financial actors and offshore bank accounts, laundering money through altcoins can be achieved through unknown transactions.

Transaction Fees

Transaction fees for cryptocurrency depend mainly on the issue of network space at the time, against the demand from the currency holder for a faster transaction. The currency holder can select a special transaction fee, while network organizations process transactions in order of highest offered fee to lowest. Cryptocurrency exchanges can clarify the procedure for currency holders by offering first concern substitutes and thereby find out which fee will likely cause the transaction to be processed in the scheduled time.

Initial Coin Offerings

An initial coin offering (ICO) is a contentious means of raising funds for a new cryptocurrency set out. An ICO may be used by startups with the goal of avoiding regulation. However, securities regulators in many authorities, including in the U.S., and Canada, have shown that if a coin or

token is an "investment contract" (e.g., under the Howey test, i.e., an investment of money with a reasonable expectation of profit based remarkably on the gumptions or managerial efforts of others), it is a security and is fixed to securities rules and regulations. In an ICO movement, a percentage of the cryptocurrency (usually in the form of "tokens") is sold to early

backers of the project in exchange for legal tender or other cryptocurrencies, often bitcoin or ether.

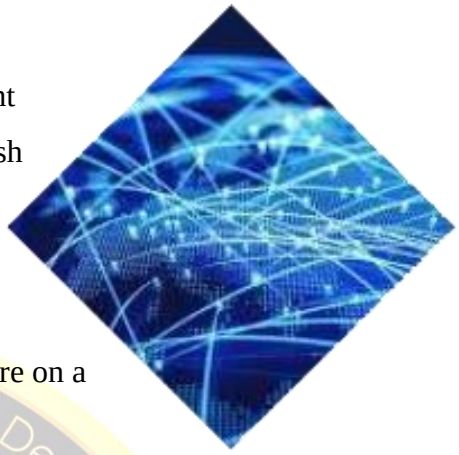
According to PricewaterhouseCoopers, four out of the 10 biggest proposed initial coin offerings have used Switzerland as a base, where they are habitually registered as non-profit organizations. The Swiss regulatory agency FINMA stated that it would take a "balanced approach" to ICO projects and would allow "authorized pioneers to negotiate the regulatory landscape and so launch their projects in a way fulfilled with national laws protecting investors and the respect of the financial system." In response to many requests by industry heads or workers, a judicial ICO working group started to supply legal guidelines in 2018, which are shown to minimize uncertainty from cryptocurrency offerings and to maintain sustainable business practices.

Transaction Confirmation

Typical ADPOS blockchains have 100% block producer participation. After an average of 0.15 seconds from time of broadcast, a transaction can be considered confirmed with 99.9% certainty.

In addition to ADPOS, Zilionixx adds DAG-based asynchronous Byzantine Fault Tolerance (BFT) for faster achievement of irreversibility. The BFT algorithm provides 100% confirmation of irreversibility within 0.1 second.

Transaction as Adaptive Proof of Stake (TaaPoS)



Every transaction to be involved by part of the hash of a recent block header is required by the Zilionixx technology. This hash has two purposes:

1. Prevents a replay of a transaction on forks that do not include the referenced block
2. Signals the network that a particular user and their stake are on a specific fork.

Over time all users end up directly confirming the blockchain which makes it difficult to hammer out counterfeit chains as the counterfeit would not be able to transfer transactions from the legalized chain.

Default Permission Groups

The Zilionixx technology also enables all accounts to have an "owner" group which can do everything, and an "active" group which can do everything except change the owner group. All other permission groups are derived from "active".

Parallel Evaluation of Permissions

The permission evaluation process is "read-only" and changes to permissions made by transactions do not take effect until the end of a block. This means that all keys and permission evaluation for all transactions can be executed in sequence. Furthermore, without starting costly
application logic that would have to be rolled back a rapid validation of permission is possible. At last, it means that transaction permissions can be marked as pending transactions are received and do not need to be re-evaluated as they are applied.

By including all the things we have a conclusion that permission verification represents a significant percentage of the computation required to formalize transactions. Making this a

read only and unimportant parallelizable procedure allows a dramatic enhance in performance.

When replaying the blockchain to rebuild the destined state from the log of Actions there is no need to evaluate the permissions again. The fact that a transaction is included in a known good block is sufficient to skip this step. This dramatically lowers the computational burden linked with replaying an ever growing blockchain.

Actions with Mandatory Delay

Time is a complex component of security. In most cases, it is impossible to know if a private key has been stolen until it has been used. When people have applications that require keys be kept on computers connected to the internet for daily use, then time based security is even more complicated. The Zilionixx technology allows applications to indicate that certain actions must wait a minimum period of time after being included in a block before they can be applied. They can be cancelled during this time.

Users can then receive notification through email or text message when one of these Actions is broadcast. If they did not authorize it, then they can use the account recovery process to recover their account and retract the Action.

The required delay depends upon how sensitive an operation is. For example, paying for a coffee might have no delay and be irreversible in seconds, while buying a house may require a 72 hour clearing period. Transferring a whole account to new control may take up to 30 days. The exact delays are selected by application developers and users

Deterministic Parallel Execution of Applications

Blockchain agreement depends upon destined and reproducible behavior. This means all parallel execution must be free from the use of locking prehistoric. Without locks there must be some way to guarantee that transactions that may be held in parallel do not produce non-destined results.

In Zilionixx technology based blockchain, once parallel operation is enabled, it will be the job of the block producer to organize Action delivery into independent shards so that they can be evaluated in parallel. The schedule is the result of a block producer and will be deterministically held, but the process for creating the schedule need not be destined. This means that block producers can use smooth algorithms to schedule transactions.

Part of parallel implementation means that when a letter builds a new Action it does not get conveyed at the spot, instead it is scheduled to be delivered in the next cycle. The receiver may be actively updating its own state in another shard that is why script is not delivered at the spot.

Minimizing Communication Latency

Latency is defined as the time taken by one account to send an Action to another account and then receiving feedback. The main aim is to allow two accounts to exchange Actions with one another by remaining in a single block without having to wait for 0.1 second. The Zilionixx technology divides each block into cycles to make the latency able to work. Then each cycle is further divided into shards and each shard consists of a list of transactions and then each transaction consists of Actions to be conveyed. This whole system can be taken as a tree where different layers are processed in a sequence and in a smooth way.

Emergency changes

To fix a harmful bug or security exploit that is actively giving harm to users, if a software change is required then the block generators may speed up the process.

Scripts & Virtual Machines

For coordinating the conveying of authorized messages to accounts, the Zilionixx will be the foremost platform surely. The validation of specific details that mostly do not depend on the design of Zilionixx technology are done by the script languages and virtual machines.

Schema Defined Actions

All Actions transferred between accounts are defined by a schema which is the part of blockchain agreement state. This schema enables a smooth conversion of Actions between the accounts.

Schema Defined Database

A similar schema also defines the database state. This makes sure that all the data stored in the applications by the users should be shown in a human readable way and executed with binary efficiency.

Generic Multi Index Database API

A defined database schema is needed to track, store and find data while developing smart contracts. The developers commonly need the same data sorted to maintain smoothness of the indices.

Separating Authentication from Application

To enhance the parallelization opportunities and to lower the computational debt linked with the remaking application state from the transaction log, Zilionixx software separates the validation logic into three forms:

- Validation that an Action is internally consistent
- Validating that all the preconditions are valid
- Updating the application state

Validating an Action is internally consistent or not is just “read-only” and needs no access to blockchain state. This means that it can be done by maximum smoothness. Validating preconditions is also “read-only” and this can also be done by maximum smoothness. Only

updating of applications needs writing access and must be processed in a sequence for each application.

Authentication is the “read-only” procedure of verification of Actions applied. Application actually works. In real, calculations are needed to be worked, however, once a transaction is involved in blockchain then it is not complementary to perform authentication or verification procedures.

Inter Blockchain Communication

Zilionixx software is basically designed to enhance the inter blockchain communication. This is achieved by making it easy to build proof of existence and sequence of Actions. These proofs along with the applications allows the details of inter blockchain communication to enable high level abstractions to be presented to developers.

Merkle Proofs for Light Client Validation (LCV)

If clients do not need to process all the transactions then it is quite easy to integrate with other blockchains. As an exchange does not care about anything but in and out transfer. If the exchange chain could use lightweight merkle proofs of deposits rather than having to trust on its own block developers, then it would be more appropriate. While synchronizing with another blockchain, the blockchain developers would like to keep the smallest possible overhead.

The aim of LCV is to allow the production of relatively light-weight proof of existence that can be verified by anyone tracking a relatively light-weight data set. In this case, it is proved that a particular transaction was involved in a particular block and that the block is involved in authorized history of a particular blockchain.

A valid proof needs about 512 bytes at the rate of 10 transactions per second. This is very appropriate for the blockchains with a 10 minute block interval but not suitable for blockchains with 0.5second block intervals.

After the point in which the transaction was involved, the Zilionixx software allows light-weight proofs for anyone who has any irreversible block header. It is possible to prove the existence of any transaction with the proof of less than 1024 bytes.

There are a wide variety of time, space, bandwidth optimizations that can be made when it comes time to validate proofs on other chains. The proof sizes can be kept small by tracking all the block headers. A tradeoff between minimal long-term storage and proof size can be offered by tracking only recent headers. A lazy evaluation approach can be used by a blockchain intermediate past proof's hashes has to be remembered. New proofs only have to involve links to the known sparse tree. The exact approach executed depends on the percentage of foreign blocks that involve transactions offered by merkle proof.

It becomes more efficient to simply have one chain contain the entire block history of another chain and expel out the needs for proofs altogether. It is efficient to lower the frequency of inter-chain proofs for some performance reasons.

Latency of Interchain Communication

The block producers must wait until 100% certainty of a transaction that has been irreversibly finalized by another blockchain before accepting it as a valid input while communicating with another outside blockchain. If any blockchain developer doesn't wait for 100% certainty of transaction by an outside blockchain, then it will directly influence the blockchain agreement. To provide rapid irreversibility, Zilionixx software uses both ADPOS and aBFT.

Proof of Completeness

When merkle proofs from outside blockchain is used, then there is a clear difference between knowing all the transactions done are valid and knowing that no transactions are skipped or expelled out. It is possible to prove that there have been no gaps in the transaction history but it is impossible to prove that all of the new transactions are known. The Zilionixx software enables
this by giving a sequence number to every Action conveyed to every account. These sequence numbers can be used by a user to prove that all the Actions deliberated for a specific account have been processed and that have been processed in a sequential way.

Zilionixx Wallet

The wallet management component provides services that easily recognize the e-Wallet address of service users through QR code scanning, and instantly enters into transactions once a quantity has been entered. Also, using IOS/ Android Native and Web methods, it should allow external businesses using the e-Wallet service to deploy DApps on various service environments.

Zilionixx Block Explorer

Users can check the blockchain status in Zilionixx block exploer.

Zilionixx dApps

Medical Service

Using smart contract and zk-snarks cryptography, Zilionixx blockchain will support the medical/healthcare service.

Patient will be use medical history smart contract so that all the medical history will be stored on Zilion blockchain. Doctors can check all the medical history of the patient and decide the correct treatment method. All the hospitals are using their own medical history so that, if the patient goes to other hospital then his medical history is nothing. If the medical history stores on the blockchain, then all the hospitals can check all the medical history of a patient.

And also patient can do medical consult with a doctor from any country.

This medical history UI will be implemented on Wallet and Website as a dApp.

DEX Service

We will implement the Decentralized Exchange(DEX) on our Zilionixx blockchain using smart contract. Zilionixx support fast transaction speed so, there is no sniper and arbitrage bot on the DEX. This will be make secure DEX platform for the investers.

ROADMAP

Milestones

First Stage (~October 30th ICO/IDO)

- ZNC Token on pre-sale
- ZNC Token crowd sale
- Zilionixx engine development
- Launch testnet of Zilion blockchain

Second Stage (~4Q, 2021)

- Zilionixx block explorer development
- Zilionixx DEX development
- Zilionixx Medical Service development
- Zilionixx coin service like poocoin
- Launch mainnet of the Zilionixx

Zilionixx Token (ZNX) Distribution

Zilionixx token is an opportunity, BEP-20 token, specifically designed for the Zilionixx platform before our blockchain team finished our own blockchain that adopted blockchain 4.0. BEP-20 tokens allow a smooth and standard set of rules and regulations implementing on how tokens behave and work on the Binance Smart Chain. This is critical for enhanced solidity and the platform strength.

BEP-20 allows for uniform connection with other smart agreements and scattered applications on Binance Smart Chain.

Zilionixx token ZNX is exchangeable to any type of currency but not limited to bitcoin,

bitcoin cash, etherium, USDT, litecoin, dogecoin, ripple and many other cryptocurrency.

Maximum Supply: 88,888,888 tokens

The first release of tokens during the IEO launch will be limited to 20,000,000 tokens with the portion of every 5,000,000 tokens that enable trading on an internal level. The further release of the token's quantity is to protect the first investors and keep the value of the tokens.

Pre-IEO price per token will be found in due date. However, the first mover advantage will make the maximum profit which should be appreciated in values of token prior to IEO.
After launching the mainnet of Zilionixx blockchain, we will have ZSDT as our floating currency and this coin will be listed on our DEX.

Take Off

The investors who invested in the first batch will not only make the profit as early adaptors during the initial selling on an internal level but also will get benefits from the unique nano-franchise system.
There will be unique and outstanding marketing given to early investors with the mechanics of hybrid rewards and group forming which can only occur in the Zilionixx community and ecosystem.
The best reward for the investor is that they can build different streams of incomes that consist of not only token appreciation but also compensation referral.

During the IEO/ICO, Zilionixx will be introduced in the top 5 coin exchanges around the globe. We are very confident that from the very first day of trading, the Zilionixx coin will get its momentum.

Conclusion

The Zilionixx software is designed from experience with demonstrated concepts and best executions, follows the systemized full cycle of blockchain development and represents basic progress in blockchain technology, we named it blockchain 4.0. The software is a part of comprehensive outline for a globally scalable blockchain society in which segregated applications can be easily installed and ruled with speed as one of the most fundamental value postulation, integration and merging with artificial intelligent as well as background novel nano franchise marketing system that enhance the price of coin and it will unavoidable the pre eminence cryptocurrency around the globe in the near future. Considering its wide range of application, Zilionixx coin will furnish the traditional banking old fashioned, discard the financial institution and insurance industry that would benefit zillions of people in the world.