



ESPERS

A CryptoCoderz Team Project

White Paper

Written by the CryptoCoderz Team
February 20th 2018 (Version 1.0 Release)

TABLE OF CONTENTS

Abstract	pg 3
Blockchains	pg 4
Consensus and Reward Mechanism	pg 5
Terminal Velocity RateX (VRX)	pg 7
Velocity Blockchain Constraint System	pg 9
Sidechains & Cross-chain Interfacing	pg 11
Secure Messaging	pg 13
Site-On-Chain	pg 14
Lightweight/Mobile Blockchain	pg 16
Chain Apps	pg 16
X-Nodes	pg 17
Project Roadmap	pg 18
Team Structure	pg 19
Disclosure	pg 20



ABSTRACT

With the advent of blockchain technology in the early 2000's the world has been standing by excited to see what becomes of it. Most notably Bitcoin has captured everyone's attention as being a currency that operates on the blockchain and other communities have sprung up in its wake. The need for an advanced blockchain solution to everyday tasks that both the provider and the user would benefit from being secured and decentralized has yet to be fully realized though. Even those currently with specialty features often have a "lone wolf" mentality causing projects to fight amongst themselves and fragment so that communities become diluted and the message of the goal is lost.

Espers is a Proof-Of-Work/Proof-Of-Stake (PoW/PoS) hybrid blockchain that was created to be a solution to the division and lack of usability that is currently attributed to blockchain technology, both unifying and expanding possibilities. Implemented features such as secured messaging, cross-chain interfacing, modular sidechains, websites on the chain, file storage on the chain, to name a few are then joined through a universal interface that any coin project may then participate in. Using ESP (Espers) coins as "fuel" or a catalyst that drives the services that the chain operates further stimulates the interest in contributing to processing blocks for the network. Miners/Stakers are encouraged to participate causing consistent block generation and ensuring a lightning fast network overall. This document is intended to describe in detail the different systems that the Espers project employs and how they operate in unison to provide the end user of any community a seamless and intuitive experience.

BLOCKCHAINS

- **Current Shortcomings**

Much of what is attributed to a blockchain today is simply a single function system with a very specific purpose intended to generate revenue. Bitcoin's creator had hoped to offer a truly unique technology not focusing on revenue, but the vision became muddled as hundreds of blockchains flooded out into the world. Despite what the news and media would like to have you believe blockchains do not have to only carry one functionality. Regrettably the media focuses only losses and gains, as such the average person is put off considerably for any blockchain that deals solely with providing tokens or "coins". Though individually being technological feats little is able to tie Bitcoin based blockchains together, even alternatives such as Ethereum fall short of providing an effortlessly seamless solution.

- **Current Implementation and benefits**

Blockchains can be described as "a digital ledger in which transactions made in Bitcoin or another cryptocurrency are recorded chronologically and publicly" (–Google). Though this is more or less true, stating that a blockchain's digital ledger is used for recording transaction history mentally causes one to restrict what they believe can be done with it. Primarily blockchains are indeed used to widely distribute a decentralized digital ledger that stores recorded transaction data for the entire system, allowing anyone to be able to access their accounts and information securely. With no central point of failure by being decentralized, blockchains such as Bitcoin are very resilient to any kind of form of take down or attack against the system. Distributed ledgers also provide transparency allowing general information to be visible by anyone while keeping more private values and info under the lock of a private key which each user individually has a unique version of. Transaction information is stored in blocks of information conveniently known as "blocks". Blocks are generated by "miners", people either mining or staking which is a form of contributing resources in order to encrypt a block of information and pass it off to the network. As a blockchain generates blocks it can also manipulate their size, easing the possibility to store different data types in large capacities that are then provided to end-users. This negates need to grow the blockchain unless required by the chain parameters. When put together a blockchain is a very capable system in terms of coins, but its versatility doesn't end there.

- **Future possibilities**

A blockchain may be utilized for a plethora software solutions in regards to additional security and reliability offered through a distributed consensus. The limitation is one's own imagination and creativity. Communities talk of operating systems, messaging systems, data storage systems all running on the blockchain, significantly improving our current protocols. Once communities and projects alike begin to move away from monetary focus and lean more towards developing the technological possibilities itself it will create a real streamlining in both security and reliability of our every day tasks.

CONSENSUS AND REWARD MECHANISM

Espers uses a Proof-Of-Work/Proof-Of-Stake (PoW/PoS) hybrid blockchain which directly affects how the system handles block production and stimulates interest in doing so.

Proof-Of-Work or (PoW) as it's often referred to, is the most notable consensus method as it's also the most common among blockchain projects since its use in Bitcoin. PoW functions by having participants contribute computing power in a form known as "hash" or "hashing" in reference to hashing a block of the blockchain. Participants are rewarded for correctly submitted blocks that are accepted by the blockchain/network and then confirmed as the block ages ensuring subsequent generation (mining) of future blocks by keeping participants interested. Furthermore multiple participants typically pool together their resources by using a "mining pool", as apposed to normally competing against each other, service allowing even those with little computing power to be able to receive compensation for what they do provide rather than attempting to beat an entity with considerably more hashing power. This distribution method falls short of perfect though as it is possible to attack the blockchain by controlling what information is in the blocks being mined and submitted. These are known as "bad blocks" which are blocks with invalid information that would normally not be accepted even possibly splitting the blockchain into two versions of itself (forking) that then compete for network validity and acceptance when an entity has the ability to compute with massive amounts of power that the majority do not have access to.

Proof-Of-Stake or (PoS) for short is a newer method of block generation, however arguably one of the more secure methods of distribution though not as readily available to newcomers just climbing on board a community/project. This is because PoS uses the coins that a participant owns and is holding to generate a block, thus owning more coins and staking them provides the participant with a higher possibility of generating the next block. Staking is the act of allowing one's wallet/client to remain online in order to support the network by having randomly selected coins become temporarily unavailable while the wallet/client forges a block and then compensates the participant with an earned interest on the coins used. The longer one has owned their coins the more "weight" they accumulate and the higher their chances of forging the next block, once the block is found the coin's weight is reset to allow for other participants a chance of also mining a block. This method is considered more secure as if properly distributed the participants will invalidate most any form of attack that abuses hashing power in order to gain control of a blockchain, however one must first obtain coins in order to stake which depending on their worth can be costly and overall a deterrent to the project if this is the only method available.

PoW/PoS Hybrid, known typically as just a "hybrid" distribution method, shuffles both PoW and PoS together onto a singular blockchain. Hybrid systems are still relatively new, as few blockchains employ a robust enough difficulty algorithm which adjusts the time span between generated blocks for either PoW or PoS and in this case both in unison. A custom difficulty retarget algorithm known as "VRX" was created for Espers in order to allow for proper shuffling of generated block types within a full hybrid blockchain. By doing so the security of Espers is substantially increased as PoW and PoS complement each other's shortcomings, allowing the blockchain significant edge over one operating singularly on a particular method.

The Consensus and Reward Structure, as of the writing of this document for the Espers project, is defined below:

- **Block Time (Post VRX implementation)**

Minimum enforced spacing:	3.5 minutes per block	
Target spacing:	5 minutes per block	
Max (soft limit) :	7 minutes per block	

- **Proof-of-Work / PoW**

Block 0-10:	0 ESP per block	<i>(Start blocks*)</i>
Block 11-365:	50,000,000 ESP per block	<i>(Reserved blocks*)</i>
Block 366+:	5,000 ESP per block + network fees	<i>(Standard blocks)</i>

- **Proof-of-Stake / PoS**

Block 2125-20,000:	250% annual interest	<i>(2-day miscalculation*)</i>
Block 20,001- 2,000,800:	25% annual interest	<i>(Standard phase)</i>
Block 2,000,801- 3,000,300:	5% annual interest	<i>(Scale down phase-1*)</i>
Block 3,000,300+:	1% annual interest	<i>(Scale down phase-2*)</i>

- **Maximum Espers Coin Supply**

Total of:	50,000,000,000 ESP	<i>(50-Billion ESP*)</i>
-----------	--------------------	--------------------------

Start blocks*: Refers to setting a block reward of “0” so that the first few blocks of the chain may be analyzed while they are mined without generating any reward for the miner.

Reserved blocks*: Initially the Espers project gave away 20% of the total blockchain in what’s known as an “Air-Drop” to anyone who wanted to participate free of charge, while reserving 5% that was split equally amongst the six team members to fund ongoing development. This was done in April of 2016 upon launch and carried over in the blockchain swap that was conducted shortly afterward.

2-day miscalculation*: Upon launch of the PoS system within Espers there was initially a mistaken value input for the annual percentage equation that calculates a user’s stake rewards. This resulted in a 2-day (48 hours) over compensation of stake rewards generated by PoS, but in no way had any major impact on the overall supply/function and was promptly resolved. Twenty thousand blocks were processed as this was prior to VRX implementation and the chain had been rushing block generation during this time.

Scale down phase-1*: Once the standard PoS reward phase ends after approximately 48 billion ESP has been generated.

Scale down phase-2*: Later a final scale down to 1% is conducted fairly close to reaching maximum coin supply.

50-Billion ESP*: The maximum coin supply is estimated to be reached ~30 years after launch (2016-2046 A.D.)

TERMINAL VELOCITY RATEX (VRX)

VRX or Terminal Velocity RateX is a blockchain difficulty retarget system that, using a several block depth scan, quickly adapts the implemented blockchain/altcoin's mining or staking difficulty levels to ensure a narrow window around the desired block time. Allowing of course for some inconsistencies in block spacing due to significant increases or decreases in hashrate/staking depending on whether the blockchain is Proof-Of-Work based, Proof-Of-Stake or Hybrid, the VRX system ensures that blocks are generated at a consistently even pace. Furthermore for Hybrid blockchains the blocks are properly shuffled in a 50/50 ratio allowing both consensus types an even chance.

Simply put VRX indexes a previous set amount of blocks (typical reference implementations are set to the previous six blocks) and then compares each of them against one another in relation to their block times thus determining a set spacing between those blocks. The system then takes the determined block spacing and compares it against desired block spacing in what is called "Check Round". This *check round* is similar to the other retarget systems available but adjusts on a different curve which adapts quickly to large changes in the hashrate of the blockchain, also making sure to not adjust too much so as not to "stall" the blockchain. There is one *check round* per pair of blocks indexed so using a six block count index depth VRX will yield five *check rounds*. After VRX runs through its checks it then determines whether it should change the difficulty either up or down depending whether the desired block time was overshoot or rushed, the severity of which is limited to a maximum of doubling the previous block difficulty or halving it. Finally an average is calculated between the different pair of difficulty changes so that the most logical change in difficulty occurs that best suits the blockchain and is then logged by the Espers system. Please refer to the function diagram in the next page that depicts the actual function.

Late versions of the VRX systems (such as the one used) feature a unique PoW/PoS difficulty swing in which hybrid systems skew the difficulty on a curve in favor of the less often found block type. Doing so ensures that neither one block type can win out over the other one and both miners and stakers can benefit the blockchain equally. VRX was designed to directly interact with Espers' Velocity block constraint system, which is discussed at greater length in the next section. This is because no other difficulty retarget method was compatible with it since the block difficulty plays an important role within the Velocity system itself.

(Function example diagram)

[Fetch Previous-block-1] → [Block time: e.g. 07:00]

- 7 – minute block spacing (mbs1)

[Fetch Previous-block-2] → [Block time: e.g. 07:07]

- 9 – minute block spacing (mbs2)

[Fetch Previous-block-3] → [Block time: e.g. 07:16]

- 8 – minute block spacing (mbs3)

[Fetch Previous-block-4] → [Block time: e.g. 07:24]

- 5 – minute block spacing (mbs4)

[Fetch Previous-block-5] → [Block time: e.g. 07:29]

- 5 – minute block spacing (mbs5)

[Fetch Previous-block-6] → [Block time: e.g. 07:34]

Target spacing = 5 minute block spacing (mbsT)

[Check-round-1] → [mbs1 > mbsT] → [Adjust-down]

[Check-round-2] → [mbs2 > mbsT] → [Adjust-down]

[Check-round-3] → [mbs3 > mbsT] → [Adjust-down]

[Check-round-4] → [mbs4 = mbsT] → [Adjust-none]

[Check-round-5] → [mbs5 = mbsT] → [Adjust-none]

Compare actions then select highest chosen action

Adjust-down = 3

Adjust-none = 2

Adjust-down > Adjust-none

VRX adjusts blockchain mining/generating difficulty down to meet target spacing

VELOCITY BLOCKCHAIN CONSTRAINT SYSTEM

- **Overall Feature Functionality**

Velocity is a rewritten feature originally [found in Frycoin](#) (a now ancient Bitcoin based altcoin). Upon stumbling across this feature it became quickly apparent that although significant sections of code would need to be re-done the feature itself had a good overall premise in both security and chain stability aspects making it very desirable. The feature was successfully rewritten despite a few small setbacks and bugs in earlier versions that do not actually affect chain stability or coin operation in any way other than intended. Later on in development additional systems were created that were never part of the feature's original function for proper overall blockchain operation.

The key role of Velocity is to constrain the chain with the parameters already defined within the code, instead of having block spacing and other properties behave as a reaction to the chain's operation. Other implementations of blockchain technology, a sudden increase in hashrate, which can indicate a possible attack are still a vulnerability despite the best difficulty retarget systems out there being implemented to control block spacing. Network fees, possible invalid balance issues while sending transactions and other portions of the blockchain are enforced with a double check but are still susceptible to an attack whether it be temporary or a double spend that is confirmed and causes users of the network grief and losses which is unacceptable.

The issue of possibly exploiting parameters is resolved by the Velocity system being a "triple check". Even after a block during generation has seemingly met all requirements and is then generated it is now no longer simply accepted. Instead it is checked once more for inconsistencies and possible other exploits. Most notably users will see rejected blocks during the mining or staking phase (or both depending on coin properties). Despite the tendency to assume that there is something wrong with the chain as it is rejecting blocks this is in fact a completely normal and a welcomed operation.

Reasoning is that rapid block times, incorrect fees, insufficient balance and other issues can be manipulated by a talented programmer with malicious intent. To guard from these kinds of situations Velocity checks the generated block against the chain parameters. First it checks the block for proper spacing, if the block was generated too quickly, thus has not met one of the main parameters for the chain and is promptly rejected, staving off possible attacks and any kind of sudden increase in hashrate.

The next step verifies that previously the client that sent a transaction (if it sent one in the previous block) sent a valid transaction by comparing previous balance vs current balance along with fees paid vs minimum fee required to pay of the block waiting to be accepted. If any of these parameters are not met (mind you these are standard chain parameters and nothing outlandish) then the block is rejected despite being generated successfully. Thus this system secures the chain, making it more stable, predictable, and overall reliable, instilling confidence that the blocks that are accepted are indeed blocks that are proper.

This feature is still a prototype system. Its implementation into the Espers blockchain (which is a fully hybrid system using both PoW and PoS simultaneously) caused small glitches with the original retarget system which were addressed by moving to the previously mentioned VRX retargeting system. These glitches consisted of causing the difficulty to bottom out until a proper retargeting system could be used. That being said blocks accepted are now

spaced consistently at a minimum of 3.5 minutes allowing the chain to move forward smoothly. Next the transaction verification and previous balance checks are currently turned off until such a time as the checks become flawless. The implementation for these specific checks are still being developed to properly ascertain those sections of chain parameters.

- **Security Analysis**

Miners may also be able to create automated cutoffs for the system so as to not waste power while blocks are simply not accepted by the chain creating two possible exploits. First that users with advanced mining systems may be able to effectively premine a block during the time that the chain is not accepting blocks and withhold it from submission until the minimum time has elapsed. If the system were to then employ a security check that verifies the block's timestamp to see if a miner had withheld a block for submission another exploit would be to set a withheld block to be created with a valid timestamp as long as the miner knew each valid time window. These two exploits are resolved first by having the previously stated method of the system ensure the block timestamp does not come from outside the allowed block window. This discourages attacks by creating more steps for the attacker to go through before having a chance of success. Next the VRX implementation penalizes minimum block time, making the power required to maintain a possible attack (even with injecting a valid timestamp) increase exponentially until after just a few generated blocks the difficulty is so great that minimum time can no longer be achieved and another miner/staker can simply find the next block. This quickly negates any possible progress in the attack. Of course the Velocity system requires all parameters to be met and not simply just block time in order to accept what appears to be a validly generated block.

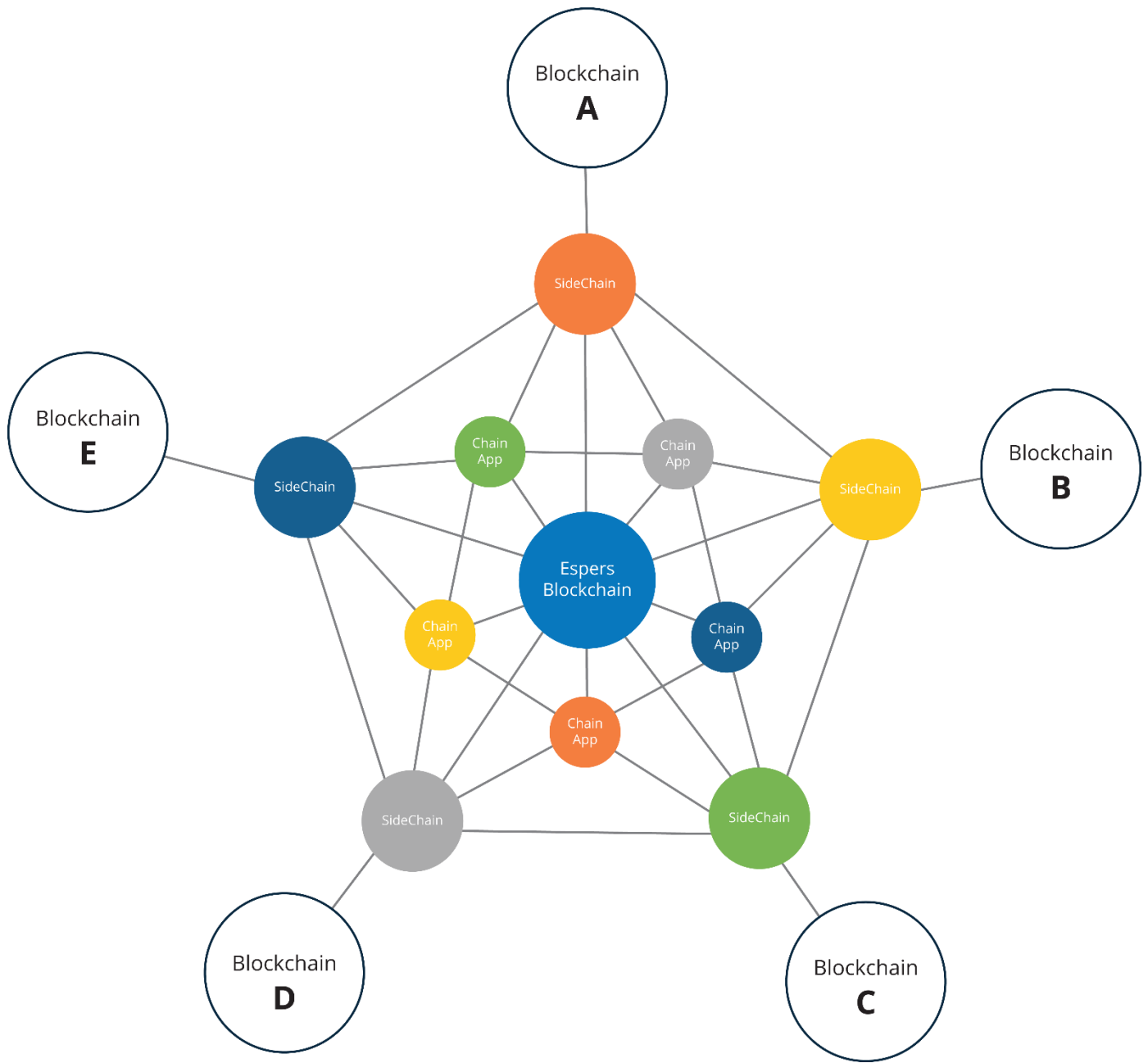
The system can be expanded to include more verification and an even more stringent implementation that may adapt to any kind of features that are added or removed. This makes the Espers system very adaptable and less of a hassle to work with as it can grow with the coin and as it becomes more refined and mature so will this new security feature called Velocity.

SIDECHAINS & CROSS-CHAIN INTERFACING

While a single blockchain is quite capable of processing large amounts of information newer methods have arose where a blockchain system will use smaller blockchains that are reliant on the parent chain that created it, known as *sidechains*, in order to simultaneously process more data while alleviating network load from any particular chain. Some approaches require the main chain to interface with the sidechains directly, having the sidechain fully reliant on the *main chain*. Espers' approach is to have the sidechains remain capable of functioning completely independently. These sidechains once created continue to function without the requirement of the Espers chain existing. Using a cross-chain interface to transmit data from one blockchain to another will allow for each chain to be able to share workloads while remaining completely independent. This independence means that regardless of any failure or issues with a given chain, the rest of the network will remain intact and operational instead of suffering a complete collapse. Employing this system even makes it possible to interface with other projects and communities entirely, allowing multiple projects to tie together and benefit one another if the communities choose to do so.

For example if a project which is capable of encrypted messaging and coin distribution processes only transaction data for a coin with blockchain "A" while processing only message text data with blockchain "B", each blockchain only has to process their respective services. Then, using cross-chain interfacing, products can share data amongst each other, providing end users with a fluid and intuitive system that is fast, secure, and reliable. To elaborate on this example, if blockchain "A" was hypothetically compromised blockchain "B" remains functional and its services would also continue to operate. Allowing users to keep using services that they need even if one or more element may no longer be accessible. This type of system also makes it easier for a blockchain project to break free from only being able to offer a single type of service.

Refer to figure A for a visual illustration of the proposed system.



(Figure A)

SECURE MESSAGING

There have actually been several different attempts to implement –Secure Messaging– into blockchain projects. Regrettably, few if any actually use the chain’s algorithm in order to encrypt the messages. To ensure speedy delivery, the message doesn’t actually affix itself to the blockchain but rather to a private key where the message contents are sent and from which they can be read. Allowing for very fast relays of messages without the need to add load to the blockchain network is a clever solution. However, a proper implementation of secure messaging would need to broadcast the messages across nodes through the blockchain itself, just as a mined block would normally do.

By storing raw text on a block, similar to how Bitcoin’s genesis block contains the text headline of a news article title, the messages can then be more secure than just being encrypted and sent to the recipient. This is due to not only to encrypting the message through an encryption algorithm but also by being able to confirm that the message sent/received is indeed valid. Allowing the message to confirm its validity in the same manner that a transaction confirms its validity within the blockchain ensures that messages received and sent contain only what they were intended to contain. Falsified or even spam messages are significantly reduced or even nullified entirely in some cases.

While the content of the messages remain private, for transparency reasons the blockchain still reports when a message is sent and to what public key. However, the recipient and sender are the only ones privy to the content as publicly there is only a note made onto the chain that there was a message sent, along with the public keys which are already normally available. Transparency is required for any sort of data transference regardless if it is for coins or for another type of service. This is because without transparency it becomes very convoluted to verify that the recipient did indeed receive the intended method of service as the chain fails to properly record actions taken.

Continuing beyond merely including text as the content of a message, Espers’ messaging system is also designed to process and distribute everything from basic images to compressed files and documents allowing its users to go beyond standard text-only limitation. To accomplish the previously mentioned Side-chain system and cross-chain interface is used. With Espers being the catalyst for text data processing its other sidechains then directly interact with the Espers blockchain as well as the other individual sidechains to also be able to process other data simultaneously while keeping the network load light. This is done to remove a central point of failure from the system while allowing for greater flexibility of the services. For example if user “A” sends a message to user “B” on the Espers blockchain that contains stylized text data as well as a few images the message will actually be split up and processed simultaneously in sections.

First the Espers chain itself would process and relay the text message data including the styling code which it will then render client-side upon delivery, keeping data processing lower. Secondly the images that user “A” has sent are then processed into a sidechain that notifies the Espers chain of an image attachment to a sent message. Once the message is confirmed user “B” is then able to view the message contents, the images are rendered across from the sidechain and the message text is natively rendered from the local chain ensuring once again that if some aspect such as the image sidechain failed the message would still be delivered regardless of the state of the rest of



the network. The opposite is also true. If the chain processing text incurred an issue then the chain processing images would still relay and deliver the images to user “B” though the text would not be visible. This creates a far more robust system than attempting to have a single point process such loads of data.

Going beyond the Espers chain, using chain interfacing, the system is also able to interact directly with other projects and their communities, uniting them by allowing users from one community to directly interact with the other. If two users of participating blockchains so desired they are able to send a message from their local wallet/client to the other user’s wallet/client regardless if it is the same chain, community or project. This shatters the separation between communities and allows for a higher possibility of real use from the systems that are currently out there and are still being created. Each chain processes messages with a fee paid to their each respective networks, keeping their communities interested in processing blocks.

A key benefit is how this impacts the goal of the Espers system. Individual entities such as companies are able to conveniently and effectively run standalone blockchains for their own needs such inter-company messaging and data processing that the entity requires to be kept secure/encrypted. This cross-chain communication allows for interaction with another department or an entirely different entity while retaining privacy and individual security.

SITE-ON-CHAIN

Current internet protocols including SSL and TLS still leave us all wanting more. Websites, servers, and even personal computers are compromised almost countless times daily even with the best practices implemented and security protocol followed. This is because much of the traffic that is speeding through the world wide web is not encrypted or secured in any way. More reputable websites and companies make sure to use some sort of encryption for traffic with their website(s) but even then a compromised server or network can cause the whole system to come down potentially jeopardizing client information, business information, and other sensitive data.

In response to this predicament the Espers project proposes that websites and other internet related services be operated/stored/hosted through the blockchain, thus nearly negating any possible attack to websites and other internet services without ever impacting usability. In using the blockchain as an internet protocol you effectively add an almost impenetrable layer of protection to any kind of service operated, especially websites. Going further than merely adding a layer of security, a blockchain operated website has no possibility of suffering from a DDOS attack, as there are no servers or datacenters to compromise, no files to “hack”, no hosting to worry about, no domain headaches, no storage concerns, no data to intercept, and so on. In order to achieve this lofty goal the previously discussed features are all used in unison to bring about a properly rendered website to any user across any participating blockchain/project.



First the hosting party uploads their website through the Espers client which promptly converts the files into raw code and stores it within indexed blocks on the blockchain. Individual sidechains are used to store each type of information so that code types, images, videos and other data does not saturate any given chain. When the hosting party submits their website onto the blockchain they also pay a small network fee to process the data with the blockchain just as one would with paying a transaction fee for sending a transaction. This fee is of a nominal amount, and is simply there in order to retain reasonable compensation to any miner or staker that might have processed the block. Once the data that is processed onto a block, and the block has been confirmed, it becomes available to the entire community using the Espers system and any other participating parties. When browsing for websites the Espers client queries each chain for its predetermined data type and renders it live on the client side for the user to interact with. This means that any type of web browsing is always session based and not visible by another entity or 3rd party. Any information processed between the website and the user is then also secured along with all information viewed by the user with the chain reporting access and other usage variables to be stored for analytical purposes. By doing so a web browsing service such as Google could submit their very own browser that would then crawl the chain for websites that were hosted on it, in a sense offering no transitional difference between our current internet system and what can effectively be called the “internet 3.0” all while maintaining a secure, intuitive, and fluid experience.

By using the cross chain interface system Espers can then be bridged with future like-minded projects so that instead of creating division a user could browse websites stored within another project’s system entirely from the Espers client and blockchain system while effectively remaining completely independent so as not to incur risk from an unrelated project’s chain failure affecting a user’s currently used system. This encourages unity by enabling a standardization, foregoing the need for a proprietary system.

LIGHTWEIGHT/MOBILE BLOCKCHAIN

As a blockchain grows it becomes “heavier” in the sense that it continuously stores information without regard to possible hardware or service limitations to the end user. In order to circumvent such a concern for possible mobile users or users who simply cannot store the entire chain either at that moment/ indefinitely it is important to offer an alternative to what’s known as a “full” client. Standard or “full” clients by general practice store and verify the entire blockchain which allows for significant redundancy and support as community members/users use the system while a “Lightweight” or “Mobile Blockchain” acts as an access portal, querying the blockchain and pulling data from it more like a block browser rather than actually storing the system locally.

By not storing the majority of files locally the Espers system can more readily be used in full scale on a mobile device or by a user with limited network/storage capacities. Though much of what makes this system lightweight is simply crawling the blockchain it also of course has the capability to submit data to the blockchain to be processed in the upcoming block with or without synchronizing the blockchain. Every system should allow for customization by the user that is using it and as such the Lightweight/Mobile Blockchain is also capable of synchronizing either partially or wholly. If the option is selected, the system will synchronize from the last checkpoint and “assume” that previous transactions reported by the chains hosted by nodes are valid. Another option is to have a “quiet” full sync to run where after the semi-sync is completed from the last checkpoint the client then begins synchronizing the rest of the blockchain silently in the background allowing the user to still support the network completely at their discretion.

CHAIN APPS

As the Espers blockchain system is designed to use sidechains and modular features the “Chain Apps” pertains to the project’s ability to plug any kind of blockchain operated application into itself and grow in capabilities. Some of these Chain Apps come from X-Node voted features (discussed further in the next section) while others are from 3rd parties verified prior to implementation into the system. User created chain apps may be submitted at any time via the system’s client and are then promptly processed to be assigned a unique sidechain for it to use.

X-NODES

X-Nodes are not to be mistaken with Masternodes, which is a centralized system where users lock a specific balance in order to participate in additional network features and support them, later rewarding the participant with some of the generated coins from the next block if they qualify. Instead, X-Nodes are completely opt-in meaning that any community member may participate in the system regardless of their current balance or previous experience. This ensures that the decentralization aspect of the Espers project and blockchains in general is not lost once again strengthening the overall network.

The way an X-Node functions is by having a participant register themselves on the network as an additional data processor allowing them to store additional sidechains that are used to provide additional chain features. Similarly to a Masternode, an X-Node requires a persistent internet connection and penalizes any participant that consistently disconnects to avoid inconsistent connections or any possible hang-ups in service provided to end users. The longer that a user participates in the system the higher their chance become of being part of the compensated X-Nodes which are automatically voted on by the network depending on reliability and data processed. A participating user may then also lock any desired amount of their balance which will effectively become frozen as the participant will no longer be able to stake them until they are unlocked from the X-Node and in doing so have the balance act as a multiplier to the compensation rate provided. Of course the multiplier is on a curve and implements several anti-abuse system such as requiring a cool down period for recently locked coins. Until the cool down is complete a participant will not see a multiplier effect. The smaller the amount locked the longer the user must wait for the lock to cool down at an exponential rate. Larger balances require users to wait less time to cool down while having the multiplier on an exponential curve. This negates the usefulness of significantly larger balances ensuring that users are encouraged to lock larger amounts to be rewarded sooner while penalizing possible “dust” locking to such a degree that it becomes impractical.

A locked balance will still be able to find the next block in the chain however any coins created are diverted (after lock cool down) to a participant’s selected feature vote. Voting on the network in this manner is crucial to establishing rapid feature development by the project team and raises community support. Participants may also choose simply not to vote however the multiplier aspect again is penalized as this creates a drop in support for new network features. Any participant may submit a requested feature to be voted on by the network for future development, however when the voting round ends any feature voting that was not selected is pooled together and split into two section that are then used independently. The first half is split into sections that are then trickled back into the network as fees paid allowing miners and stakers alike to receive a slight “bonus” until the balance runs out while the second half is put towards the winning voted upon features. Users may unlock their balance at any time while participating in the X-Node system even if the balance has not completed the cool down period giving users complete control over their experience. Similarly, if a participant opts-out at any given time, just like when they had opted in, the participant will incur another cool down now between deactivation and allowed reactivation time. Furthermore the X-Node system is intuitive and single-click removing possible user-error that often occurs with similar features such as Masternodes and replacing it with user interest/immersion. This also takes a considerable load away from support needs, network inconsistencies, and the overall hassle of operating or participating in the system.



ESPERS

R O A D M A P

Q4
2017

- Website Update
- PoW & PoS Revise
- Wallet Upgrade
- Marketing Campaign (active)

- Whitepaper
- Mobile Wallet
- Lightweight Client

Q1
2018

Q2
2018

- Xnodes
- Sidechains
- Mailing System

- ChainApps
- CrossChain
- SiteOnChain

Q3
2018

DISCLAIMER

This Roadmap is for informational purposes only, and not a binding commitment. Do not rely on this information in purchasing Espers coins/tokens as ultimately the development and timing remains at the sole discretion of the Espers/CryptoCoderz team.



ESPEERS

MEET OUR TEAM

A PERFECT BLEND OF CREATIVITY AND
DEVELOPMENT WIZARDRY.

CRYPTOCODERZ

Jonathan Zaretsky
Lead Project Manager
Developer

ARSONIC

Guillaume Huot
Lead Web Developer
Graphics Designer

MONOXIDE

Assistant Project Manager
Public Relations

BBOBB

Project logistics

CTGIANT

Assistant Developer

ARCADE

Justin Cappellini
Public Relations

BATYSTA

Antonio Batista
Project logistics



DISCLOSURE

This whitepaper (document) is for informational purposes only, and not a binding commitment. Do not rely on this information when interacting with Espers coins as ultimately the development and timing remains at the sole discretion of the Espers/CryptoCoderz team.

We, the Espers/CryptoCoderz team, intend in no way harm of any kind to anyone in any shape or form. There has never been a crowdsale of coins, presale or any other crowd funding method used for the Espers/CryptoCoderz project or its developers. Please understand the risks involved with cryptographic blockchain technology and their respective coins. The Espers/CryptoCoderz team cannot be held responsible for any lost, stolen, or otherwise missing funds of any kind. If you are unsure or have any doubt about this project we urge you to NOT invest or become involved as this is a prototype technology system as stated in numerous areas and to be used at your own risk.

We have no affiliation with the Yobit product called "Easpers". This is a separate product solely operated by Yobit.

CREDITS

Big thank you to all who helped make this project a reality, special thanks goes out to the following community members (usernames) who have contributed to this document's creation and revisions:

Bit010
CafeConTiki
CryptoCarrot
cXplexus
Eugen
Gandalf86
IK
Tekna
Vin
Wolf