Initial Spec - 1st Draft

Exodium (EXD)
Decentralized, Trustless Cryptocurrency Liquidity

George "Moon" Kushnir

October 13, 2018

Abstract

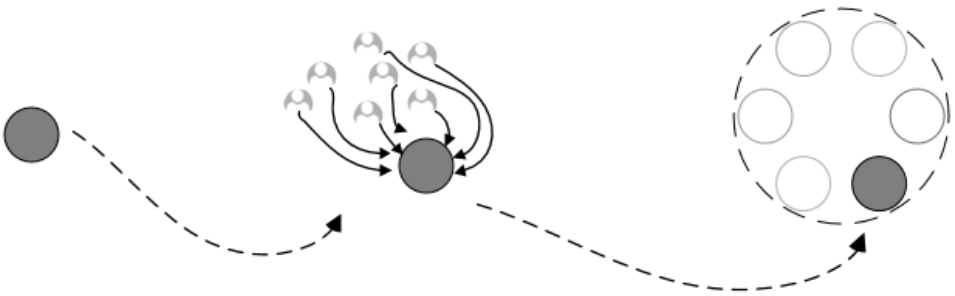
The Exodium Liquidity Network enables decentralized, trustless exchange of any cryptocurrency asset that supports multisignature transactions for any other supported cryptocurrency asset. Through the use of existing blockchain technology, Exodium utilizes the delegated trust model to decentralize and enable such liquidation while simultaneously being invulnerable to fraud and classic 51% attacks on the network through the use of larger than 51% m of n multisignature wallets on supported asset blockchains, controlled by delegated nodes. Delegation is done through the use of on-chain voting to establish the network exchangers.

I. Introduction

While blockchain technology has revolutionized asset ownership and trading across borders while eliminating trust, there exists no real bridge between multiple differing blockchains that specifically enables trustless cross-chain trading. Existing solutions use proxy assets that act as intermediary steps between exchanges, which require redemption for the source asset, or trading is only possible in a decentralized fashion when both assets exist within the same blockchain (such as Ethereum tokens). Atomic swaps solve this problem partially, but require that both assets utilize a common hashing function, as well as support hash time-locked contracts. Exodium allows true decentralized trustless swapping of blockchain assets with no intermediate step and a single requirement, enabling the potential to support trustless trading between the vast majority of cryptocurrency assets. Previously, the two largest cryptocurrency assets, Bitcoin and Ethereum, could not be traded trustlessly with each other. Exodium enables seamless swapping of these assets without relying on a third chain to store proxy assets. Furthermore, these types of trades on intermediary chains require a buyer and seller on both sides, leading to issues in liquidity when intermediary networks go unused.

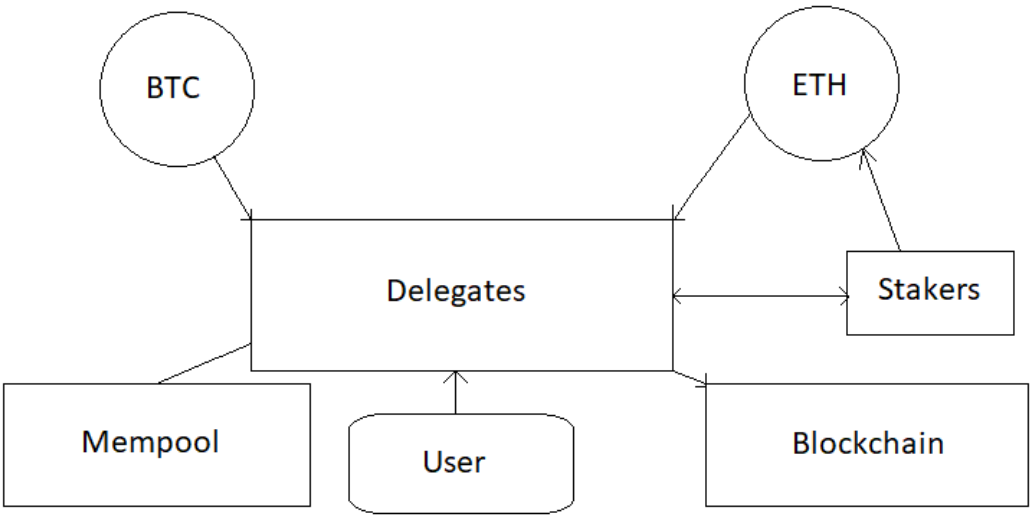
Exodium utilizes a feature inherent to every major cryptocurrency asset – multisignature wallets. Through delegated trust, multisignature wallets secure funds on either side of the transaction, while elected delegates and stakers act as liquidity suppliers that are rewarded for staking their off-chain cryptocurrency assets. Through a combination of the Exodium utility token, the Delegated Proof of Stake system, a multisignature wallet scheme utilizing many signatories matching the elected delegates, and a modified PoS algorithm, we can establish a user-friendly method of exchanging assets without ever requiring direct interaction on the intermediary chain, using the Exodium chain as an invisible pass-through with no requirement to ever own the EXD asset itself (though its value correlates to trades executed on-chain due to it being traded invisibly as a fee token).

II. Distributed Proof of Stake



Exodium's own blockchain functions as a Decentralized Proof of Stake system. Owners of the Exodium asset (EXD) inherently have the ability to vote on the network operators. These network operators are referred to as "delegates" in systems similar to the one employed by Exodium, and will be referred to as such from now on. These delegates operate in a similar capacity to miners on Proof-of-Work blockchains, but instead of work, delegates in Delegated Proof of Stake systems are democratically elected officials, who function as the arbiters of the network, deciding what transactions get processed into blocks and verifying them beforehand. At network creation, 101 "genesis delegates" are created and spawned in order to run the network at launch. As users of the network start voting in other users who register themselves as delegates on the network through a special transaction, they contribute to network consensus indirectly by choosing their network's operators. Network rounds are determined as a list of 101 delegates who have the highest of "voting weight" proportional to the other delegates on the network. Voting weight is defined as the total amount of blockchain assets in the wallets of users who have decided to vote for a delegate using a special transaction. These delegates are required to run software at all times in order to keep the network constantly running, validating transactions and generating blocks.

Unlike the majority of existing Decentralized Proof of Stake blockchains, Exodium functions with a "single asset, single vote" model. In existing DPoS blockchains such as EOS or LISK, owning a single asset allows voting for the entire delegate set with that asset, which encourages the formation of cartel like systems of influence, leading to centralization of authority within these blockchains. Due to the launch structure of these blockchains being Initial Coin Offerings or some form of pre-launch decentralized fund-raising, the assets themselves risk being controlled almost entirely by early investors or by the developers themselves, who hold a large percentage of the initial stake. Thanks to "single asset, multiple votes" systems like these, owning a small portion of the asset would allow large holders to control all of the delegates in these systems. Exodium avoids issues like these using the "single asset, single vote" model, and because of the sensitive nature of the job that delegates perform on a network like Exodium, where custody of off-chain assets is done through a network of decentralized signatures controlled by delegation of trust in 101 operators, avoiding cartels is paramount to implementing proper network security. Security of the network is also taken into consideration when implementing incentive systems throughout Exodium.



III. Trustless Swaps & Interoperability

Interoperability between blockchains has been a major topic of discussions in the last few years in regards to evolution in the blockchain space. Existing solutions are weak at best and at worst are vaporware that don't make it to market. The strongest existing solution is an implementation of Atomic Swaps with an order book, which is just an application of hashed timelock contracts to coins sharing a hashing algorithm, allowing individuals to swap assets trustlessly. This method is functional, and can be automated, but runs into issues when assets do not share hash algorithms, making certain swaps impossible. Blockchain intermediaries exist to solve this issue, but simply end up centralizing the solution, requiring an intermediary chain as a stop-gap, or issuing proxy tokens via contracts on off-chains and redeem them across assets. Exodium's core product relies on a fundamental feature inherent to nearly all modern blockchains; instead utilizing the decentralized voting model combined with multisignature timelocked transactions in order to make swaps across any two tokens possible with the sole prerequisite being multisignature wallets and *recommended but not required* timelocks. By having stakers deposit funds into multisignature timelocked wallets controlled by delegated keys that expire, we can move money across chains without relying on trusting any one authority or having strict requirements across chains.

IV. Multisignatures & Off-chain Liquidity

Bitcoin and its derivatives have had the implementation necessary for a system such as Exodium to exist since December of 2015, with the introduction of `OP_CHECKTIMELOCKVERIFY`. Ethereum and its derivatives can emulate this function in numerous ways with its implementation of smart contracts, and nearly all types of blockchains in existence support some combination of multiple signature redemption and locking of spends until a time in the future.

Users of the Exodium network can exchange their blockchain assets for other blockchain assets without dealing with order books, registration, or revealing any personal information. The network functions as a decentralized exchange with a set price based on market movements and stake settings. Exodium delegates and network stakers provide liquidity off-chain, allowing end users to swap assets trustlessly and (*pseudo*) privately.

V. Proof of Stake & Delegate Staking

The primary source of liquidity for Exodium's network is provided through its users and other crypto asset holders. Delegates are used to manage custody of off-chain assets, but off-chain staking incentives are entirely decoupled from delegation itself. While delegates ultimately control the Exodium blockchain by submitting the necessary proofs, Proof of Stake and potential Sybil flaws are solved in Exodium by utilizing a separate stake system. Providers of liquidity do have a say in consensus of the network, and stakers also run software in order to keep the network secure. While not required, a delegate can individually stake any of their own assets alongside other stakers. Off-chain transactions utilizing just delegates as oracles would be vulnerable to Sybil attacks (as de-anonymizing operators is rather simple), so proofs of off-chain transactions for swap confirmation need to be "voted" on by stakers as well as signed by delegates themselves. Exodium's primary swaps protocol functions in a fashion similar to Bitcoin's Lightning Network, where the majority of transient data is kept in memory and passed around using a communication protocol, but not inserted into blocks except for finalized proofs after a successful swap (*or a published report of staker or delegate fraud*). Aside from normal network operations such as transfers of the Exodium asset itself, the Exodium asset itself will rarely be used as purely a currency, with the exception of being used in order to pay fees for swapping assets on the network.

Since Proof-of-Stake suffers from the "nothing-at-stake" problem all PoS systems have (unlike PoW), Exodium must account for this fraud due to the asset custody aspect of the network. This is mitigated using a method similar to Ethereum's "slasher" concept, where voting on multiple chains as a staker penalizes you by forfeiting your stake to discourage voting on more than a single chain or multiple results. This is implemented by having fraud reported by other network users, who submit proofs of said fraud. If multiple votes by a single staker for a single transaction verification are proven, the stake is forfeit and a bounty is released to the reporter. In order to prevent "false positives" in the case of local chain issues, votes will also reference their most recent block hashes, and must match in order to not be discarded. Staker nodes may also "abstain" from voting in the case that they believe their nodes may not have the most up to date copy of off-chain history, and will not affect their stake (but will consequentially reduce their reward). These stake system implementations, including fraud reports, are autonomous and require no manual intervention at any time, as they are built into the core Exodium system. Thanks to use use of timelocks, transactions can also expire and return to the end user in the case that a transaction cannot be verified in time or in the event of a consensus failure where a result cannot be decided. As all trustless swaps need to be verified by every delegate who in turn trust stakers to vote on validation, this creates a system commonly referred to as "Distributed Byzantine Fault Tolerance".

Stakers of off-chain assets that participate on the network are inherently in control of the off-chain assets, as delegates will collectively use staker votes as consensus for signing off-chain transactions. Staker votes are not equal, and like delegate determination, staker "votes" are proportional to their share of the total stake, with a high threshold required to approve the completion of a swap. This system disincentivizes cartel-like behavior within stakers, and ensures that while delegates essentially retain custody of funds, there is a very low possibility of fraud unless the majority of delegates are compromised. Exodium is safe from traditional 51% attacks, as approval for signing of off-chain transactions will be significantly higher, with current implementation specifications as high as >80%, or 81 of 101 delegate signatures. This implies that if at least 20% of the Exodium network is honest, staker funds cannot be compromised through the use of fraudulent collusion during delegate signing. With an equally high threshold for staker voting and asset forfeiture punishments for committing fraud, collusion between stakers to fool delegates into signing over off-chain assets becomes even less likely, reducing the attack surface.

VI. Network Security & Organic Growth

The distribution of the Exodium asset is paramount to the safety of the assets in custody. As long as a single group does not control over 80% of the Exodium asset itself, it is not possible to attempt theft or compromise consensus using traditional methods of collusive fraud. Due to the nature in which fee incentives are implemented in the Exodium network, the price of Exodium is inextricably tied to the volume of the network, which itself is tied to the assets controlled by the network, which in turn raises its price through organic growth. As overall stake size grows, the fee grows, the price grows, and network security increases. This is a feature unique to Exodium, where market manipulation will be arbitraged away for the security of the network, preventing the price from falling below a point where one group is able to control over 80% of the asset. Software safeguards will be built into all nodes to monitor these thresholds automatically, which serve as checks and balances and create a positive feedback loop promoting both organic growth and total security, and tools will be readily available for all participants to take advantage of opportunity windows for arbitrage within the network itself.

Instead of traditional block rewards, delegates generate a static amount of Exodium once a day in a single block, and distribute the reward with their voters as well as keeping some for themselves. This, on top of fees from swaps, keeps the delegation properly rewarded and the network secure. Because of the lack of height, the "longest chain" is determined by the amount of "slots" passed over the lifetime of the network instead of the height, and each node can verify the amount of slots passed since the creation of the network; This prevents long range attacks one would traditionally perform by exploiting lack of total blocks in a Proof-of-Stake chain. As long as initial distribution is not heavily centralized, a long range attack is nearly impossible, and Exodium's distribution is purposely done in a way that no single entity can control more than a few percent of the initial stake.

VII. Simplified Payment Verification & Light Nodes

Thanks to the ubiquitous implementation of Merkle roots in Proof-of-Work systems, stakers do not need to own a copy of the entire off-chain asset's blockchain in order to vote and decide if an off-chain transaction by an end user was successful. Because "Simplified Payment Verification" can be done simply by having the Merkle branch of a particular transaction, light nodes only need the block headers and that transaction's Merkle branch in order to independently verify that a transaction was successfully completed and vote on its verification within the Exodium network. This is important due to the amount of assets Exodium intends to support, and allows extremely light-weight client implementations to be supported for the vast majority of blockchain verification. Unfortunately, Proof-of-Stake systems do not have this advantage due to the inability to verify transactions trustlessly, and for these assets a full node must be stored on the staker's node.

Despite Exodium being a DPoS chain (which still qualifies as a form of "PoS" itself), light nodes will be able to hold only the block headers in memory as well as the last n blocks. This is done by downloading the entire chain at first boot, and then pruning older blocks upon verification. By default, light nodes hold only 100 blocks in memory, and the majority of stakers are expected to be running these light nodes while delegates run full nodes with off-chain SPV clients for Proof-of-Work asset chains. This ecosystem allows full security, while simultaneously allowing Exodium nodes to be built with a low footprint in mind, and implementing cryptographic shortcuts where available.

VIII. Incentive Systems & The Exodium Asset

In order to secure a trustless network, economic incentives need to be such that the network is in a state of Nash equilibrium at all times, which is just a way of saying that users are incentivized to act in their own best interests and trusting no other user or operator on the network. Altruism cannot be implied, assumed, or accounted for, and game theory shows that incentives must be created in such a way that the network is secure when all users act in their own self interests. Exodium keeps this in mind and uses cryptographic security to enable this trustless nature wherever possible.

When a user initiates a swap, they pay a fee in the Exodium asset. Luckily for end users, they can use the Exodium network software without ever owning any of the Exodium asset. The Exodium software will instead give the users an option to purchase the required Exodium on top of transaction, and the price of their transaction is adjusted in their source asset in order to pay for the Exodium. This fee ends up in the hands of delegates as well as their voters, and other stakers in the network.

The primary incentive for a delegate to operate and validate transactions on the network is some form of economic reimbursement. Traditionally, these are block rewards. Exodium's network does not offer block rewards, instead providing incentives for delegates to participate in transaction swaps and offering a cut of those transaction fees in the form of Exodium asset rewards. Because Exodium is intended to be used primarily for swaps, the footprint of blocks is minimal and blocks are naturally empty except for fees and finalized swaps. Thanks to the exclusion of traditional block rewards, Exodium can opt to "skip" blocks intentionally and only publish blocks that contain finalized swaps or Exodium asset transactions, votes, or delegate registrations.

Stakers of off-chain assets are given proper economic incentive through a unique system where they can earn Exodium assets by staking off-chain assets. This is also a unique feature not available in any other blockchain. In exchange for providing liquidity and offering to sell their assets at a pre-determined agreeable price determined by an external oracle, they are rewarded with the Exodium asset. This creates another positive feedback loop where incentives allow for organic network growth.

By properly providing economic incentives for all facets of the network, we can ensure that delegates on the network can both keep the network secure and safe while simultaneously working in their own best interests by collecting fees on swaps that they help sign off on. Stakers of off-chain assets are likewise incentivized by being rewarded for offering their assets for sale, and get rewarded even if they don't sell. Finally, we have the Exodium asset holders, who stake their Exodium on-chain asset and are indirectly in control of the network through voting. With stakers providing consensus to delegates, delegates signing off on swaps in a distributed group of trust, and voters choosing the operators of their network who help provide value to the asset, we create a fluid system with a positive economic feedback loop.

Because Exodium's asset itself is primarily used for fees, it is possible to make the use of the asset entirely silent to end users, and for investors in the product to be able to trade, vote, and speculate on the asset independently of its network operation. Thanks to the positive feedback loops implemented to encourage organic growth, and the incentive to grow the value of the Exodium asset in conjunction with its network usage, Exodium provides a rather unique situation where a blockchain's economic value is intrinsically tied to its real world usage.

IX. Mempool & Privacy

As previously mentioned, the primary feature of the network is to enable asset swaps trustlessly across many different chains. The majority of the "work" done in order to make this possible is done completely in memory, and only the final proofs are published within the Exodium blockchain itself. While complete privacy is preferred, it is necessary to publish these final proofs publicly in order to be able to verify the integrity of an arbitrary swap performed in the past. This doubles as a way to prove "work" on the Exodium network and to verify that the network state is consistent. Any data not necessary for the verification of a swap itself is not included on-chain, and all negotiations are done through peer to peer node communications. Because stakers themselves sign off on votes which are published to the chain, these votes function as proofs and allow any end user to download and verify the entire blockchain up to an arbitrary point. This process is significantly more complicated due to the nature of the swaps, but is necessary if we want to avoid trusting any part of the network.

Stakers selling assets have the option to improve their privacy and utilize the liquidity on the network to "tumble" their funds arbitrarily by instead submitting an address on supported chains to where they would like their purchased funds to go. While this is not true anonymity, it will allow a staker to avoid revealing their purchased asset wallet, and instead will let them sign receipt of funds without revealing their destination addresses. While blockchain forensics will still not prevent this sort of obscurity from hiding their actions, it will improve privacy in the majority of cases, with a more robust implementation planned in the future for true anonymity.

X. Feature Creep, Arbitrary Oracles, & Virtual Machines

While Exodium's primary launch features are focused exclusively on the ability to swap assets trustlessly across many blockchain platforms, it would be ignorant to not discuss the potential implications of a DPoS-based system that allows for the transfer of arbitrary data across many different chains using delegates as "oracles". Similar to the centralized systems on other blockchains, Exodium can, in the future, be used to "carry over" features of other blockchains and allow anyone to utilize features from one chain to activate events on another. While this sort of feature is potentially an even bigger undertaking than the initial Exodium product specification, it is important to note that there are no immediately obvious technical limitations behind implementing these kinds of features, and allowing cross-blockchain triggers and "true" blockchain interoperability is part of the post-launch road map. These features would come in the form of a Virtual Machine, with larger fees, contracts, and a "gas"-like system similar to Ethereum's, but they are kept in mind when designing the initial spec, even if a VM is still just a fairly distant thought in the development process.

XI. Conclusions

The race to interoperability has been a long one, and many "bandage" solutions and stop-gaps have been implemented thus far to achieve the results Exodium wants to achieve. While not a "decentralized exchange" in the true sense of the word, it is a platform for the instant transfer of value across blockchains. Exodium provides a much needed solution to problems of centralized trust in exchanges, opting to instead tackle the problem with a Delegated Proof of Stake system, along with other checks and balances. The result is an effectively "trustless" network for the masses that functions by taking advantage of one of blockchain's oldest features - multisignature wallets.