TECHNOLOGY WHITEPAPER

29.02.2024 v0.1

soloneum.org

CONTENTS

1. INTRODUCTION

The advent of blockchain technology has ushered in a new era of decentralized systems and cryptocurrency networks. The primary goal of Soloneum is to solve the wide-ranging problems found in cryptocurrency projects of poor models of governance, economics and utility, and thereby enable the creation of a large, self-sustaining, decentralised entity that will provide enormous utility and value to the people of the world.

This paper serves as an exploration of Soloneum's technical underpinnings and practical implementation, shedding light on its potential to provide the properties of a robust, decentralised, affordable and high-capacity system that can provide the infrastructure for a new global financial network available to everyone.

2. UTILITY

In the mid to long term, the network must provide real value to people. As much value as possible to as many people as possible in fact. We believe we have not only the governance and economic foundation to do so, but also the technical foundation to build a network that fulfils the original promise of Bitcoin and much more.

2.1. DECENTRALIZED AND UNCENSORABLE

Decentralization stands as a cornerstone in cryptocurrency projects, imbuing them with distinct attributes that differentiate them from traditional centralized financial systems. It confers several advantages, including enhanced security, as the distributed nature of the network makes it more resistant to cyber-attacks and fraud. Decentralization also promotes transparency and trust, as all transactions are publicly verifiable without reliance on a central authority. This aspect is crucial for building confidence in the system, especially in an era where trust in centralized institutions is waning. Furthermore, decentralization ensures that no single entity has overarching control over the network, thus safeguarding against manipulation and censorship.

Decentralization is not just a technical feature, but a foundational principle that guides the ethos and functionality Soloneum, making it essential for its success and long-term sustainability. The maintenance of low operational costs for full nodes is instrumental in preserving the decentralized nature of cryptocurrency networks, which is vital for their security. We aim to keep full node costs affordable for even a hobbyist while achieving a capacity of 20,000 TPS (transactions per second). We believe that this can be achieved by offloading the majority of the compute requirements of a full node off onto new, open-source hardware designed specifically for the purpose of blockchain validation. This will keep the cost and access to operate a full node, even at high TPS, open to a large number of people globally, which will therefore retain the network's decentralised properties.

We also aim to keep bandwidth requirements to running a full node to below what is commonly available on standard residential connections at 20,000 TPS making it a realistic option for people even on residential internet connections. 50Mb/s will provide enough bandwidth for over 20,000 TPS each transaction having an average size of 200 bytes.

2.2. SECURE

2.2.1. COST-EFFICIENT PROOF-OF-WORK SECURITY

The security of the Soloneum network is underpinned by a robust Proof-of-Work (PoW) consensus mechanism, similar to the one successfully employed by Bitcoin. PoW provides a high level of security by requiring participants, known as miners, to solve complex cryptographic puzzles to validate transactions and secure the network. However, to ensure that the PoW security remains cost-efficient and aligned with the network's governance goals, Soloneum implements an innovative approach. The annual adjustment of emissions dedicated to security is a dynamic mechanism that prioritizes cost efficiency over arbitrary fixed emission schedules. This approach optimizes the allocation of resources, ensuring that the energy expended in securing the network remains both economically viable and controlled by those that it impacts financially, the citizens. By continuously evaluating and fine-tuning the emissions dedicated to security, Soloneum aims to strike a balance between network integrity, operational efficiency, and citizen governance.

To provide some examples and comparisons, Bitcoin can handle roughly 100 million transactions per year and spends roughly $200 on electricity and security per transaction via emissions. Ethereum which handles roughly 300 million transactions per year spends roughly $10 on security per transaction via emissions. In contrast to this, Soloneum, which could potentially handle 600 billion transactions per year, could spend $600M per year on security and achieve a security cost per transaction of just $0.001. This is 200,000x less spent on electricity and security per transaction than Bitcoin.

2.2.2. CONTINUOUS IMPROVEMENTS IN SECURITY

At Soloneum, we remain steadfast in our commitment to network security, and we believe in continually exploring new and innovative approaches to enhance the resilience of our ecosystem while optimizing costs. While our foundation is built upon the proven security of the PoW consensus mechanism, we recognize that the blockchain space is dynamic and ever-evolving. Therefore, we pledge to keep our options open, developing and embracing emerging technologies and novel security solutions that align with our mission. We actively seek partnerships and collaborations with the broader blockchain community to harness collective wisdom and pioneer groundbreaking security methods.

2.3. FAST FINALITY

Soloneum adopts the Ethereum GHOST (Greedy Heaviest Observed Subtree) consensus system to achieve swift 15-second block confirmation times. GHOST mitigates the issue of stale blocks by rewarding miners for their contributions, even when their blocks aren't part of the main chain. This approach significantly reduces the chances of stale blocks, ensuring efficient and speedy block confirmations. With GHOST, Soloneum creates a responsive blockchain ecosystem suitable for real-time transactions, dApps, and smart contracts, setting new standards for blockchain performance while prioritizing both security and speed.

Soloneum is dedicated to advancing the forefront of blockchain technology by actively researching and exploring alternative consensus mechanisms to further improve consensus speed and transaction finality. While GHOST has proven effective in achieving rapid block confirmations, we recognize the importance of innovation in the ever-evolving blockchain landscape. By continuously seeking cutting-edge solutions, we aim to optimize the efficiency of our blockchain, offering users even faster transaction finality and an improved user experience.

2.4. GLOBAL CAPACITY

We will develop and implement a number of software and hardware scaling technologies to bring the cost running a global scale full node into the affordability range of a hobbyist. This is key in making the network open to all, at a cost that does create barriers to usage, while still maintaining decentralisation and therefore censorship resistance.

Software

- XEVM: Embarrassingly parallel transaction processing.
- Chainmail: Proof-of-Fee.

Hardware

- RISC-V Supercluster transaction validator.
- ASIC RISC-V Supercore transaction validator.
- FPGA signature accelerator.
- ASIC Signature accelerator.

2.4.1. UTXO VS EVM

The scalability of blockchain networks has emerged as a paramount concern in the rapidly evolving landscape of decentralized systems. While various consensus algorithms and architectural paradigms have been proposed and implemented, one crucial facet that differentiates UTXO (Unspent Transaction Output)-type cryptocurrency networks from their EVM (Ethereum Virtual Machine) counterparts lies in their inherent capacity for parallelism. This has significant implications for transaction processing efficiency and network scalability.

The core tenet of parallelism in UTXO-type networks can be distilled into the simultaneous processing of transactions that are independent of one another. In these networks, transactions are fundamentally comprised of inputs and outputs, represented as UTXOs. Each UTXO encapsulates a discrete unit of value, and the state of the network is inherently distributed across these individual units. This inherent parallelism becomes a salient feature contributing to scalability.

The absence of interdependencies between UTXOs signifies a significant reduction in transaction bottlenecks. Unlike smart contract execution in current EVM-type networks, where computational dependencies often necessitate sequential processing, UTXO systems, by design, circumvent such bottlenecks.

This attribute carries profound ramifications for network resilience. During periods of heightened transactional demand, UTXO-type networks exhibit a heightened degree of resistance to congestion. Transaction processing can proceed in parallel, mitigating the delays and fee escalations witnessed in systems where sequential execution is required.

The hardware-driven parallelism in UTXO-type cryptocurrencies, exemplified by Bitcoin, is fundamentally achieved through the utilization of multiple CPU cores within nodes. Each CPU core is dedicated to processing a distinct transaction or set of transactions concurrently. By leveraging the innate independence of Unspent Transaction Outputs (UTXOs) in each transaction, these CPU cores operate in parallel, executing transaction scripts and cryptographic verifications without interdependencies. This hardware architecture optimally distributes the computational workload, significantly enhancing the network's capacity for concurrent transaction processing.

2.4.2. AN EMBARRASSINGLY PARALLEL EVM: XEVM

2.4.2.1. INTRODUCTION TO XEVM

In the context of Ethereum and other EVM-based systems, transaction processing and scalability have been perennial concerns, that have limited Ethereum to just 14 transactions per second. We describe an innovative approach inspired by the UTXO model, termed **'XEVM'** and is added as an additional constraint to the Soloneum EVM system. XEVM utilizes a DAG structure of transaction ordering to track the state of contract slots and balances of Externally Owned Accounts (EOAs) via chains of **'Keyframes'**. The adoption of Keyframe chains necessitates all transactions to reference these Keyframes, thus facilitating full parallelism akin to the UTXO model.

2.4.2.2. KEYFRAMES

A '**Keyframe chain**' is started when an address receives a payment of Solon for the first time or a contract instance is deployed to the network. Keyframes are generated upon creation or modification of a storage slot or account balance. Upon creation, the 'KeyframeID' is defined as:

Keccak256(Address + SlotID)

The '**Keyframe Nonce**' is set to 0. Upon update, the new keyframeID is defined as:

Keccak256(PrevKeyframeID + txID)

The keyframe nonce is incremented by 1.

This model associates each keyframe with the previous keyframe in a chain and with the data specific to the transaction that created it, making it non-arbitrary. This means that miners cannot extra 'MEV' by inserting their own transactions within the DAG.

Keyframe lengths are limited to first 5 bytes of produced hashes, which provides 40 bits of entropy and 1e12 combinations. This is enough to defend against malicious birthday attacks to insert a transaction within the unconfirmed DAG, and keeps the data requirements low. Keyframe nonces allow nodes to understand if there are missing parts of the DAG when a transaction arrives, and to use this information to decide on whether a transaction should be outright rejected or retained with the expectation that an ancestor transaction will soon arrive, thereby allowing the keyframe chain to be completed and the uncertain transaction to be validated. Keyframe nonces are limited to 1 byte, i.e. a range of 0-256, and overflow back to 0.

2.4.2.3. TRANSACTION POOL

At the heart of the '**transaction pool**', a comprehensive database containing the full set of unconfirmed transactions, including data about the current state Keyframes. Full nodes within the network rely on the transaction pool as a reference point to validate whether a Keyframe, and therefore transaction, referenced by another transaction exists or not. This database serves as a crucial component in the transaction validation process, enabling nodes to discern the authenticity of state references and ensuring the integrity of the parallel processing model.

When a transaction references a particular state Keyframe, the node tasked with validating the transaction checks the transaction pool to see if that Keyframe exists. If the Keyframe does not exist then that transaction is considered currently invalid. If it is determined that a keyframe is an descendent of a transaction that the node is yet to receive, as recognised via the keyframe nonce, then the node may retain that transaction in a ‘waiting pool’, to be process after the missing ‘parent’ of that transaction has arrived. Transactions are added to the transaction pool database after they have been successfully validated.

2.4.2.4. BLOCK BUILDING

As miners build block candidates they will evaluate the transaction pool on their node to determine what sections of the DAG can provide them with the highest amount of fees. Within the unconfirmed DAG there may be transaction conflicts, creating different potential ‘realities’ for the world state. The miner will select between any conflicting sets of realities based on which provides the most fees, and therefore profit.

This is achieved via a fast traverse of the unconfirmed DAG across any areas in which conflicts exist. Where any 'forks' of the DAG exist, the miner must evaluate the fee weight of competing transactions at the base of the fork to determine which side of the fork to have their state changes applied within the block candidate.

Transactions from a conflicting set that are not selected to have their state changes implemented, can still be included into blocks. Transactions that are included but do not have their state changes applied are charged 50% of whatever their fees would have been. This makes sure that users cannot submit transactions that must be processed at a cost to the network, but at zero cost to the sender of the transaction. Their inclusion is charged at 50% of the normal transaction fee to make sure miners have a financial incentive to implement the state changes of the transaction with the highest fee weight.

2.4.2.5. BLOCK VALIDATION

When a block arrives, the transactions in this block are checked against the transaction pool and DAG structure to confirm their existence. Any missing transactions are requested from peers. If the block is confirmed to be valid, all transactions in the block are considered 'confirmed' and any not included in the block are retained in the transaction pool, other than in the specific case for transactions which make use of the COINBASE, TIMESTAMP, and NUMBER virtual machine instructions which are ejected (further details can be found about this below).

2.4.2.6. TYPE-1 TRANSACTIONS

Type-1 transactions put the entire transaction data inside the 'pre-image', therefore all this data, including the access map, is signed by the sender of the transaction. This provides a higher level of protection than Type-0 transactions as it locks the access map of the transaction so that it cannot be changed, preventing MEV and other unwanted activities.

Lite wallets are still able to send Type-1 transactions, but they must communicate with a full-node to provide them with the correct access map to append to their transaction data before they sign the transaction.

2.4.2.7. TYPE-0 TRANSACTIONS

Type-0 transactions are introduced at launch as a method of allowing backwards compatibilities with existing EVM wallet infrastructure. Lite nodes will be able to create and send 'incomplete' transactions that follow the same transaction format on current EVM chains, but the first node that receives these incomplete transactions will 'complete' them by generating the access map and appending it to them before propagating it to the rest of the network.

Type-0 transactions have less protection because the access map is not part of the pre-image and is not signed by the sender. This means that type-0 transactions can still be front-run by miners. Type-0 transactions are not insecure as the actual state changes of the transaction cannot be tampered with, I.e. they have the same protection as transactions on a traditional EVM chain. Type-0 transaction will be made invalid after a hard-fork at some date after launch.

2.4.2.8. CONFLICTING TRANSACTION HANDLING

Transaction conflicts occur when two or more transaction consume the same keyframe. This is very similar to in UTXO systems when a transaction conflict occurs when a two or more transactions spend the same UTXO but have different outputs, which is known as a 'double-spend' and is an indication of some kind of fraud attempt. In the XEVM system, there is no concept of 'double-spend' and in fact, conflicting transactions will happen naturally as a consequence of the model. Contracts that make use of storage variables which have common access to all users and have high-usage, will necessarily generate conflicting transaction as two or more users attempt to access the same piece of state at the same time.

These conflicting transaction are not considered invalid, but only one from a competing set of conflicting transaction will have their state changes applied to the world state.

2.4.2.9. KEYFRAME SELECTION

Keyframe selection is an important component of the XEVM model on Soloneum. Due to the nature of the XEVM system, it is possible for conflicting transactions to exist on the network. In a UTXO chain these are considered double-spends, but on the XEVM network we handle them differently. See the section 'Conflicting Transaction Handling' for further details on this.

When a transaction is built, a valid access map must be generated for it. To generate an access map the relevant keyframes must be chosen for each state ID that is accessed. But due to the potential for multiple valid but conflicting keyframes in existence for any given state ID, the node that builds the access map must have a methodology for choosing one valid keyframe over another.

Keyframes are selected based on the same system that miners are incentivised to use to choose which transactions to be included in blocks. Miners are incentivised to choose the set of transactions that earn them the most money. Front-running is not possible in an XEVM system, so the way miners maximise their extractable value is to choose the set of transactions from a set of conflicting transactions that earn them the most fees. When choosing one transaction from a conflicting set, the miner will not only consider the fees paid by those transactions in that set, but also all transactions that build upon those transactions in the transaction DAG (directed acyclic graph). A transaction and keyframe is therefore selected based on it's 'fee weight' as opposed to just it's fee.

The 'fee weight' is the total fees of a transaction and the fees of all transactions that build upon it in the DAG while these transactions exist in the transaction pool. Therefore when selecting a keyframe when building a transaction, or when selecting a transaction when building a block, the fee weight must be calculated from competing options and the option with the highest weight should be selected. This is not a consensus protocol and is instead based on reinforcing the Schelling point of financial incentives to increase network performance and security properties. The methodology we use for this we call 'Proof-of-fee'. The implications of this system will be discussed within the section 'Chainmail: Proof-of-fee'.

2.4.2.10. SCALABILITY

By embracing the XEVM model, Soloneum unlocks orders of magnitude more scalability. This paradigm permits the concurrent execution of transactions without the need for a highly resourced core for each transaction. Furthermore, it strengthens network resilience, reducing congestion during peak periods and optimizing the allocation of computational resources. Throughput of the network is no longer constrained by the speed of a single CPU core, and can instead be divided up across multiple processing cores of arbitrary quantity.

Each core does not need to have access to the entire world state. Instead, each core only needs access to the state and contracts that is defined upfront by the transaction. This means that when a node receives a 'complete' transaction (as opposed to an 'incomplete' transaction of 'Type-0'), it can read the contracts and states needed for this transaction, and then send only this data to an individual core for processing. This is all the data the core will need to validate that transaction.

If a processing core finds that the transaction requires more contracts or state data than are provided, then the transaction must necessarily be invalid as the transaction must correctly reference *all* contracts and state that it interacts with upfront. The amount of data required to validate a transaction is therefore reduced by many orders of magnitude and can be performed by a core with much less storage resources. This creates a compute situation which is "embarrassingly parallel" and perfect for the development of hardware which contains many processing cores each with minimal resources.

2.4.3. CHAINMAIL: PROOF-OF-FEE

Our XEVM system creates a unique emergent property not found in other cryptocurrency networks, which we call PoF (**Proof-of-Fee**). As discussed in **4.4.2.9 Keyframe Selection**, users and miners must sometimes select transactions from a set of conflicting options. Both users and miners use the same system for selection to remain in sync to reduce wasted effort and financial resources.

Thanks to this keyframe selection mechanism, the highly woven properties of an EVM-based DAG and the large scale of capacity the XEVM system unlocks, we gain an extra emergent security property. In blockchain-based PoW cryptocurrencies, the security principle is based on the cost to extend the chain and the financial incentives to continue to extend that chain as opposed to extending a competing chain. Our PoF property achieves similar properties but applied to the transaction DAG. Each transaction in a DAG extends that DAG forwards and in a non-sequential manner. Given that miners are not able to achieve front-running in our XEVM system, denying a single transaction culls all transactions in the DAG that occur after that transaction in the graph. This means that denying any specific transaction comes at the loss of not only the fees in that single transaction, but also all fees in all transactions in the DAG that occur after that transaction in the graph. This is different to a double-spend 're-org' attack on a blockchain, since in this type of attack a miner still receives all the block rewards and can still include all the transactions that were put into the blocks that have been 're-org'ed' and they can therefore still collect all the transaction fees. Denying a transaction with a high fee weight contrast comes at a direct cost to the miner that does this. This is potentially a non-negligible cost to a miner. This property is also found in all UTXO-based chains, but due to loose connectivity within the DAG and the low usage of all existing networks, this effect is not meaningful. In contrast, in the XEVM system the DAG will become closely woven due to the usage of common state IDs in high usage contracts and the high TPS.

It will be possible to do an assessment of a transaction in the transaction pools, or even in the blockchain, to determine the amount of fee weight it has, and therefore how much PoF security it has. Services can then easily make use of this information to check for extra security assurances to allow them to credit payments more quickly.

To give an example, an exchange might typically wait for 64 blocks of confirmations for a $1000 Ethereum transaction before crediting to a user's account, which would take 16 minutes. On a high usage XEVM system it would be conceivable for a transaction to achieve $1000 worth of fee weight within 15 seconds or less.

2.4.4. HARDWARE ACCELERATION

Our strategy for hardware acceleration is to walk before we can run. We will first maximise network scalability by testing our software on a node with a CPU with 64 cores to determine it's performance on easily accessible consumer hardware at a cost of around $4000. We will then explore the possibility of increasing the number of cores to 256 using off-the-shelf, low-cost RISC-V MCUs at a total cost of around $1000. RISC-V is an open standard instruction set architecture for producing computational circuits, and is the perfect standard to develop hardware for a decentralised cryptocurrency system. After confirming the performance of the RISC-V architecture we will then explore the possibility of implementing these 256 RISC-V cores into a suitable FPGA to reduce the cost down to the order of roughly $250. Finally we may take the final step of moving our 256-core FPGA design into an ASIC and reducing the cost to below $100 per chip. This process will allow us to bring the cost to validate over 20,000 TPS into the price-range of a hobbyist and therefore keep the network open, decentralised and uncensorable.

Another area where we will explore potential performance gains via hardware acceleration is in cryptographic signatures. Cryptographic signatures are well-known as a bottleneck for transaction validation, and therefore this may be another place where it would be valuable to develop specialised hardware to offload a compute-intensive process.

Once final area that can benefit from hardware acceleration is in storage, and we will continue research in this area to maximise our sustained throughput capability.

2.4.5. OTHER SYSTEM BENEFITS

2.4.5.1. RAPID VALIDATION

Thanks to the embarrassingly parallel quality of the XEVM system, and the increasingly large number of cores available in even consumer hardware, transactions can be processed at incredible speed removing this as a bottleneck to scaling to a global capacity. We aim to take advantage of this property even further by creating hardware with massively parallel compute capabilities.

2.4.5.2. NO MINER FRONT-RUNNING & MEV

Thanks to the ordering of transaction occurring in the transaction DAG instead of via the ordering in blocks, miners can no longer 'front-run' transactions. They cannot put their transaction in-between other transactions in the DAG arbitrarily as this would break the DAG graph by invalidating any transactions after the replaced transaction in the DAG.

This provides a significantly improved user experience when using DeFi services, such as constant product market markers, as users can know they can interact with a service without being put at a financial disadvantage by miners whose goal it is to maximise the 'extractable value'.

2.4.5.3. NO BLIND-SIGNING

One problem found in EVMs is that when a user signs a transaction, it is not clear exactly what outcomes to the network state they are agreeing to. On a legacy EVM transaction the user is simply locking the transaction to where the funds and data are initially being sent to, and are not specifying all the world state changes that will occur do that transaction. This leaves open a security risk where a user may believe they are sending a transaction that does one thing, but it instead does something else that may financial harm them. For example it may give someone else access to their assets. This problem is called 'blind-signing'

In Soloneum, Type-1 transactions allow users to lock their transactions to the exact state changes they expect on the blockchain. By doing this, as long as a user checks what they are agreeing to upfront, it is not possible for them to be tricked into agreeing to something they do not want to happen. This makes the network far more secure and predictable for users.

2.4.5.4. CANONICAL TRANSACTION ORDERING & GRAPHENE BLOCK TRANSMISSION

Thanks to the fact that transaction ordering occurs within the DAG and is no longer relevant within blocks, we are therefore able to order transactions in blocks in a way that provides further performance gains. One potential option is to order transactions in blocks using 'canonical ordering'. This would open up the possibility to use a block compression technology called 'Graphene' as developed by UMASS.

Graphene allows blocks to be transmitted between nodes using many orders of magnitude less information than is included in those blocks, and this is achieved due to the fact that nodes will typically have very similar sets of transactions in their transaction pools. This technology is especially beneficial when applied to networks that have large blocks compared to Bitcoin. At 20,000 TPS, we expect Soloneum to have roughly 50-150MB block sizes. Keeping low requirements for bandwidth will allow the network to be accessible to most people who want to run a node.

2.4.6. TRADE-OFFS

2.4.6.1. BANDWIDTH USAGE

Due to the need to communicate the Keyframe and contract information there is a cost to this new system and that is in the form of increased data communicated between nodes. Even for a fairly complex set of contract interactions, such as when making a swap on a Uniswap contract, the size of a transaction including the access map is only 200-250 bytes of data, which is equivalent to that of a simple one input, two output 'pay-to-pub-key-hash' transaction on Bitcoin. Simpler contracts, such as an ERC-20 token transfer, should require roughly 120-150 bytes for a transaction.

As discussed in a previous section, we will offset a large portion of the bandwidth requirement by implementing Canonical Transaction Ordering in blocks and Graphene for block transmission between peers.

2.4.6.2. TRANSACTION CONFLICTS

While the Keyframe system offers significant advantages in terms of scalability and parallelism, it is essential to acknowledge the trade-offs and challenges that can arise, particularly when contract variables experience high write rates and when users face limitations in obtaining required Keyframe information in a timely manner. These trade-offs stem from the dynamic and concurrent nature of the system, and addressing them is crucial to achieving a balanced and efficient blockchain ecosystem.

One notable trade-off emerges when contract variables experience high write rates. In such scenarios, multiple transactions may concurrently attempt to consume the same Keyframe, leading to throughput limitations. The rapid succession of state changes within the contract may result in conflicts as transactions compete for the same Keyframe. Contract authors can mitigate this potential performance limitation and a poor user experience via a number of mechanisms. They can parallelise contract variables which are commonly accessed if they experience a high rate or usage. They can also implement a sequencing system where users of a contract access the contract via an off-chain sequencing service so that no conflicts are possible.

At launch, anyone will be able to submit a type-0 transaction without the Keyframe data included. This transaction format then exactly matches that of current EVMs enabling Soloneum to be immediately compatible with most EVM software and services, such as Metamask. To achieve this we add one extra responsibility for full nodes. Should a node receive an incomplete transaction, i.e. a transaction that does not include the access map, they must validate that transaction in a manner that checks against the entire 'world state' to prepare and append the required access map data to the transaction. The node can then forward the complete transaction to the network. The other nodes in the network therefore no longer need the full world state to validate that transaction. They can simply use the state that is referenced by the Keyframes, given that if a transaction must access any state that is not reference in the transaction, then it is considered invalid.

2.4.6.3. PROTOCOL COMPATIBILITY

There a few places where the Soloneum system is not backwards compatible with existing EVM systems. The Type-1 transaction format is not currently backwards compatible with exist EVM wallet infrastructure (read more about this in the section '**2.4.2.6 Type-1 Transactions**'). We will we work with existing EVM wallet providers to upgrade their wallets to Type-1 transactions for improved properties.

There have also been some changes made to two virtual machine instructions: COINBASE and TIMESTAMP. Instead of taking these values from the current block and applying them to the transactions in that block, we instead take these values from the previous block. If the current block height is 1,000,000 and the miners are searching for a solution to block 1,000,001, the COINBASE instruction will therefore return the coinbase value of block 1,000,000. Similarly, at the same time, if the TIMESTAMP instruction is called in a transaction while block 1,000,001 is being worked on, it will return the timestamp value of block 1,000,000. Based on our research, we believe that this should have a minimal impact on any existing blockchain projects.

2.5. PROGRAMMABLE

2.5.1. FULL EVM COMPATIBILITY WITH SOLIDITY

The integration of a full EVM with Solidity compatibility in a cryptocurrency platform is a strategic move to capitalize on the established network effects of existing EVM-based projects. EVM, as the runtime environment for Ethereum's smart contracts, offers a robust, Turing-complete computational framework. Solidity, as the primary programming language for EVM, underpins a myriad of decentralized applications (DApps) and smart contracts. This compatibility ensures seamless migration and integration of pre-existing DApps, fostering a rich ecosystem. By leveraging the pre-established network effects of EVM-based projects, a cryptocurrency can substantially enhance its adoption rate, user base, and developmental ecosystem. This approach not only minimizes entry barriers for developers accustomed to Solidity and EVM but also ensures a rapid proliferation of applications, contributing to a vibrant and diverse platform ecosystem.

The NUMBER, COINBASE and TIMESTAMP virtual machine instructions all return values about specific blocks. Ordinarily this would also cause a scaling bottleneck as transactions that interact with function of contracts which use these instructions would have to be re-validated every single block until they are included into a block, as their returned data would change for each block. This could be used as a DOS mechanism by submitting many transactions like this with low fees so that nodes have to continually re-validate many transactions even though the transactions are not paying for these resources. The ideal situation is for transactions only to be validated exactly once.

To solve this issue, we introduce a new rule: transactions which interact with contract functions that include the NUMBER, COINBASE and TIMESTAMP instructions, must include the next block number in the relevant place within the transaction format. By doing so, the sender of the transaction is committing to the fact that the transaction is only valid until the next block is found. In effect this means that the transaction can be included in the next block and no other. This removes the need to re-validate these types of transaction for every block produced while the transaction is in the transaction pool, and therefore solves the scaling bottleneck. Any transaction that includes the next block number value, and any transactions that built atop then in the DAG, must be ejected from transaction pool if it is not included in the block with that height specifically.

2.5.2. INTEROPERABILITY THROUGH BRIDGES

Interoperability, facilitated via cross-chain bridges, will be another critical dimension for Soloneum. These bridges enable seamless asset and data transfer across distinct blockchain networks, thereby enhancing liquidity and user reach. Interoperability is quintessential in a fragmented blockchain landscape, where siloed networks often operate in isolation. By implementing interoperable bridges, a cryptocurrency platform can tap into the liquidity pools and user bases of other networks, fostering a more interconnected and efficient ecosystem. This interconnectedness will not only facilitate enhanced liquidity but will also promote a synergetic environment where diverse blockchain ecosystems can coalesce, leading to a more integrated, robust, and versatile blockchain infrastructure.

2.5.3. OFF-CHAIN DATA STORAGE FOR SMART CONTRACTS

Advancing beyond the conventional EVM framework, integrating off-chain data storage solutions for smart contracts offers significant benefits. Off-chain data storage addresses the inherent limitations of on-chain storage, such as scalability and cost. By enabling smart contracts to interact with data stored off-chain, platforms can achieve greater scalability, efficiency, and flexibility. This approach facilitates handling of large datasets, complex computations, and enhances privacy by not overburdening nodes with excessive data.

3. THE IMPLICATIONS OF MASS ADOPTION

We want to provide some hypothetical example numbers to give some insight into what the economic implications could be for a mass adopted Soloneum network by using some real-world economic data from existing cryptocurrencies. These are not predictions or promises, but rather a description of the economic model and its implications if mass adoption were to be achieved.

As of writing, Ethereum processes roughly around 10-14 transactions per second, and users of the network currently spend on average $8 per transaction fee. That works out to around 450 million transactions per year and about $3.8 Billion in transaction fees.

If we manage to keep fees at 1/10 that of Ethereum currently, with an average transaction fee of $0.80, but we achieve an increase in usage of the network to 20,000 TPS, then this generate roughly 500 Billion transactions per year and would generate roughly $400 Billion dollars in transactions fees. If the citizens targeted a miner reward rate that paid $1 Billion per year to secure the chain, and perhaps $5 Billion to develop, maintain and promote the chain, this would leave $394 USD Billion worth of Solon coins to be burnt. This would create a deflationary effect of $394 Billion of Solon coins being removed from the supply each year.

Even if Bitcoin used such a system of removing coins from the supply, it would only achieve a reduction in supply of roughly $75m per year given an average fee of $0.80, and Ethereum would remove roughly $350m. These are many orders of magnitude less than what is possible on a highly scalable layer-1 network such as Soloneum.

Of course, we can neither predict price nor the level of adoption we achieve with the network, but these numbers provide an understanding of the economics and the utility of the system.

4. CONCLUSION

We have provided a comprehensive framework for a global-scale decentralized financial and governance system. Drawing on the principles of Timocracy from the historical figure Solon, Soloneum proposes a unique approach to cryptocurrency governance, economics, utility, and technology.

From a technological standpoint, Soloneum integrates several new and existing protocols and systems. The development and creation of the XEVM protocol underscore a focus on parallel processing and high transaction throughput. Furthermore, initiatives for hardware acceleration are aimed at enhancing the network's capacity to handle large-scale global capacity to enable everyone in the world to use one platform.

Soloneum also emphasizes compatibility and interoperability with existing EVM infrastructure and services, reducing barriers and facilitating cross-chain interactions and asset transfers. This strategic direction aims to broaden the network's reach and utility, enabling rapid growth in use cases and a more interconnected and diverse ecosystem of decentralized applications.

Analyzing the potential impact of Soloneum in a context of widespread adoption reveals a balance between maintaining low transaction costs, achieving high transactional capacity while keeping the network decentralised enough to remain uncensorable. Providing this as a foundation and building millions of financial products a services on top of the network will bring immense wealth to the world