Innovating ReFi: SolareumChain

Solareum Inc.

September 24, 2023

https://SolareumL1.com

Contents

1 Solareum (SRM)

1.1 Executive Summary

Large corporations have been seeking sustainable access to blockchain technology, expressing concerns regarding environmental impact, security, scalability, and centralization. At Solareum, we offer a direct solution to these challenges through our innovative dual validation mechanisms, Proof of Generation (PoG) and Proof of Holding (PoH).

1.2 Solareum's Solution

Solareum takes bold strides in reshaping the blockchain landscape by offering a solution that directly tackles pressing environmental concerns and centralization risks through its proprietary dual consensus innovation. We strongly believe Solareum is bringing technology to the industry that will begin a technology transformation and allow much broader adoption.

1.3 Solareum's Value Proposition

Solareum's unparalleled value proposition is rooted in our unwavering commitment to blockchain, sustainability, innovation, and empowerment. We lead the way in the blockchain industry with our proprietary blockchain technology, powered by PoG and PoH. Solareum sets a new gold standard for sustainability in blockchain, demonstrating our dedication to environmental responsibility.

Additionally, we prioritize decentralization and trust through transparent and secure consensus mechanisms, ensuring a level playing field for all participants. Our EVM compatible blockchain empowers sustainable innovation across every sector, allowing a much broader adoption opportunity than ever before. At Solareum, we don't just offer a Layer 1 blockchain; we provide a catalyst for transformative, sustainable, and innovative change across industries.

1.4 Final Thoughts

The Solareum whitepaper is a deeply technical text that embodies our vision for a future where blockchain catalyzes positive change. Solareums dual consensus mechanisms, sustainability commitment, and focus on decentralization pave the way for a greener, more equitable world. Embrace Solareum to be part of this transformative journey towards a

sustainable and decentralized future.

2 What is SolareumChain?

Solareum Inc. pioneers the future of blockchain technology with SolareumChain, a cutting-edge Layer 1 (L1) blockchain system, empowered by our innovative Proof-of-Generation (PoG) consensus validation mechanism. Unlike traditional blockchain networks that rely on energy consumption for validation, SolareumChain redefines the paradigm by anchoring its validation process in renewable energy generation. At its core, renewable energy production serves as the driving force behind SolareumChain's security, with the native token, Solareum (SRM), facilitating transactions and governance.

In an era marked by an escalating commitment to sustainability, decentralized energy ecosystems have taken center stage. These ecosystems are characterized by the localization of energy generation, predominantly harnessing the potential of renewable sources such as solar, wind, and hydro power. In stark contrast to prevailing blockchain validation methodologies that consume vast amounts of energy, our PoG protocol aligns perfectly with the ethos of sustainability. Not only is it inherently eco-friendly, but it also negates the vulnerabilities of centralization and manipulation that plague existing systems.

SolareumChain opens the door for renewable energy producers, including solar farms, wind farms, tidal farms, geothermal installations, and even individual rooftop solar panels, to participate as validators. By continuing their primary function of generating renewable energy, these entities simultaneously fortify the security of Solareum's Layer 1 blockchain. This revolutionary approach extends inclusivity to individual households and businesses that have invested in renewable energy generation installations. As a result, it fosters a decentralized and competitive landscape within the energy marketplace, democratizing the power of renewable energy in the blockchain space.

> **"By embracing a blockchain that is validated by energy generation, rather than consumption, significant strides can be made towards a greener, more sustainable, and equitable future for all. Together, it is possible to revolutionize the way transactions are validated and build a better world for generations to come. Join SolareumChain to be part of this transformative journey!"** -SolareumChain Team

3 Mathematical Analysis of Validators

In the context of SolareumChain, this discipline applies advanced mathematical techniques to scrutinize validators' performance, security, and reliability. Validators are pivotal to maintaining the integrity of SolareumChain's Layer 1 blockchain, ensuring secure and efficient transactions. By subjecting these validators to rigorous mathematical analysis, we aim to optimize their functionality, detect vulnerabilities, and enhance their overall efficiency within the SolareumChain ecosystem. This approach offers a specific and in-depth understanding of validator performance in the context of SolareumChain, ultimately contributing to the network's stability and trustworthiness.

A variety of formulas are provided capturing description of the SolareumChain system. Let

$$\mathcal{X} = \{X_1, ..., X_n\}$$

be a set of sets of validators, namely $\mathcal{X}$ is a set of sets, where each set contained compromises of the validators of distinct type, with $n \in \mathbb{N}$ types. Then, for each distinct type $i \in \mathbb{N}$, with $1 \leq i \leq n$, we have that

$$X_i = \bigcup_{j=1}^{k} X(i)_j$$

where $1 \leq j \leq k$ are indices, with $j, k \in \mathbb{N}$, and $X(i)_j$ being energy generator j of type i, and therefore, that all energy generators acting as validators form the following superset

$$\mathcal{X} = \bigcup_{i=1}^{n} X_i = \bigcup_{i=1}^{n} \bigcup_{j=1}^{k} X(i)_j$$

Combinatorics of energy generation for the above superset of all validators then results in the following given an energy generation function $E : \mathcal{X} \to \mathbb{R}$ with the standard norm acting as a metric,

$$\|\mathcal{X}\| = \left\| \bigcup_{i=1}^{n} X_i \right\| = \left\| \bigcup_{i=1}^{n} \bigcup_{j=1}^{k} X(i)_j \right\| = \sum_{i=1}^{n} \|X_i\| = \sum_{i=1}^{n} \sum_{j=1}^{k} \|X(i)_j\| = \sum_{i=1}^{n} \sum_{j=1}^{k} E(X(i)_j)$$

With the above terminology established, the nature of energy generators as validators as well as application to the Proof of Generation (PoG) consensus mechanism is presented.

4 Solareum Proof of Generation

SolareumChain L1 is ushering in a new era of innovation with Proof of Generation (PoG) at its core. This ground-breaking achievement relies on advanced integrations that precisely track electron flow and correlates it with energy generation. By ensuring local generation aligns with this electron flow, we guarantee the emergence of fresh energy resources.

Data collection is seamless and reliable thanks to our approved third-party hardware solutions, including smart sensors and the FPGA hardware running the Solareum algorithmic software. These components work together to optimize SolareumChain L1 by processing data only after it has undergone meticulous computation and validation.

To bolster the security of our Proof of Generation (PoG) on-chain reports, we will employ the robust BLS12-381 elliptic curve with 128-bit security for zk-SNARK proof reporting. This cryptographic framework substantiates the authenticity of energy generation data, ensuring the utmost trustworthiness in our energy generation records.

4.1 The BLS12-381 Elliptic Curve for zk-SNARK Proofs

In the ever-evolving landscape of digital security, staying one step ahead of potential threats is paramount. Our BLS Key Generation Signature Scheme Security is a cutting-edge solution that promises to revolutionize the way Solareum secures its cryptographic assets. With its robust key generation process, this scheme ensures the highest levels of security for your data and communications.

The BLS Key Generation Signature Scheme Security is designed to address the unique challenges faced by today's blockchain community. It employs advanced mathematical principles to generate keys that are virtually impervious to attacks, providing a rock-solid foundation for securing your digital assets. Whether we're safeguarding sensitive financial transactions, confidential communications, or critical infrastructure, this innovative scheme offers peace of mind like never before and will serve SolareumChain very well on its mission.

Solareum strives to stay ahead of the technical curve and protect what matters most with an innovative solution for some of today's most technical challenges.

SolareumChain outsources computation to private hardware which will provide a zk-SNARK (Zero-Knowledge Succint Non-Interactive Argument of Knowledge) proof of the energy generation required for validation. The elliptic curve BLS12-381 with 128-bit security level will be used with the first curve G1

$$y^2 = x^3 + 4 \mod p$$

as well as the second curve G2 required as defined through bilinear mapping with respect to a pairing $e(P, Q)$ with $P \in G1$ and $Q \in G2$.

4.1.1 FPGA Hardware

The Solareum Field Programmable Gate Array (FPGA) Hardware for L1 validation will be an initial third-party hardware unit capable of Proof of Generation (PoG) by running the SolareumChain algorithmic PoG software. The energy generation function $E : \mathcal{X} \to \mathbb{R}$ would be hardware indexed to align with computational tasks required for validation. To improve multi-scalar multiplications (MSMs) and/or (inverse) Number Theoretic Transform (NTT) computational tasks required for Zero Knowledge Proofs, SolareumChain Field Programmable Gate Array (FPGA) hardware will embed performance upgrades to ensure less computational requirements for SolareumChain.

5 BLS Key Generation Signature Scheme Security

5.1 BLS Key Generation

The key derivation process allows for the derivation of a child key from a set of intermediate Lamport keys. The entropy source for Lamport private keys is the parent node's private key, and hashing into compressed Lamport public keys which are hashed into BLS12-381 private key group.

Define the following conventions:

K = 32 is the digest size (in octets) of the hash function (SHA256),

L = K * 255 is the HKDF output size (in octets),

'' is the empty string,

bytes_split is a function takes in an octet string and splits it into K-byte chunks which are returned as an array

Using the RFC 5869 - HMAC-based Extract-and-Expand Key Derivation Function (HKDF) definition (https://datatracker.ietf.org/doc/html/rfc5869) of Extract and Expand:

5.1.1 Extract

```
HKDF-Extract(salt, IKM) -> PRK
```

```
Options:
   Hash     a hash function; HashLen denotes the length of the hash
             function output in octets

Inputs:
   salt     optional salt value (a non-secret random value);
            if not provided, it is set to a string of HashLen zeros.
   IKM      input keying material

Output:
   PRK      a pseudorandom key (of HashLen octets)

The output PRK is calculated as follows:

PRK = HMAC-Hash(salt, IKM)
```

5.1.2 Expand

```
 HKDF-Expand(PRK, info, L) -> OKM

Options:
   Hash     a hash function; HashLen denotes the length of the hash
             function output in octets

 Inputs:
   PRK      a pseudorandom key of at least HashLen octets
            (usually, the output from the extract step)
   info     optional context and application specific information
            (can be a zero-length string)
   L        length of output keying material in octets
            (<= 255*HashLen)

Output:
   OKM      output keying material (of L octets)

The output OKM is calculated as follows:

N = ceil(L/HashLen)
T = T(1) | T(2) | T(3) | ... | T(N)
OKM = first L octets of T
```

```
   where:
   T(0) = empty string (zero length)
   T(1) = HMAC-Hash(PRK, T(0) | info | 0x01)
   T(2) = HMAC-Hash(PRK, T(1) | info | 0x02)
   T(3) = HMAC-Hash(PRK, T(2) | info | 0x03)
   ...

   (where the constant concatenated to the end of each T(n) is a single octet.)
```

5.1.3 IKM_to_lamport_SK

```
 IKM_to_lamport_SK
 Inputs
IKM, a secret octet string
salt, an octet string
 Outputs
lamport_SK, an array of 255 32-octet strings
```

Procedure

```
0. PRK = HKDF-Extract(salt, IKM)
1. OKM = HKDF-Expand(PRK, "" , L)
2. lamport_SK = bytes_split(OKM, K)
3. return lamport_SK
```

5.1.4 parent_SK_to_lamport_PK

```
parent_SK_to_lamport_PK
 Inputs
parent_SK, the BLS Secret Key of the parent node
index, the index of the desired child node, an integer 0 <= index < 2^32
 Outputs
lamport_PK, the compressed lamport PK, a 32 octet string
 Definitions
I2OSP is as defined in RFC3447 (Big endian decoding)
flip_bits is a function that returns the bitwise negation of its input
"" is the empty string
a | b is the concatenation of a with b
```

Procedure

```
0. salt = I2OSP(index, 4)
1. IKM = I2OSP(parent_SK, 32)
2. lamport_0 = IKM_to_lamport_SK(IKM, salt)
3. not_IKM = flip_bits(IKM)
4. lamport_1 = IKM_to_lamport_SK(not_IKM, salt)
5. lamport_PK = ""
6. for i  in 1, .., 255
       lamport_PK = lamport_PK | SHA256(lamport_0[i])
7. for i  in 1, .., 255
       lamport_PK = lamport_PK | SHA256(lamport_1[i])
8. compressed_lamport_PK = SHA256(lamport_PK)
9. return compressed_lamport_PK
```

5.1.5 HKDF_mod_r

```
hkdf_mod_r() is used to hash 32 random bytes into the subgroup of the
BLS12-381 private keys.

 Inputs
IKM, a secret octet string >= 256 bits in length
key_info, an optional octet string (default="", the empty string)
 Outputs
SK, the corresponding secret key, an integer 0 <= SK < r.
 Definitions
HKDF-Extract is as defined in RFC5869, instantiated with hash H.
HKDF-Expand is as defined in RFC5869, instantiated with hash H.
L is the integer given by ceil((3 * ceil(log2(r))) / 16).(L=48)
"BLS-SIG-KEYGEN-SALT-" is an ASCII string comprising 20 octets.
OS2IP is as defined in RFC3447 (Big endian encoding)
I2OSP is as defined in RFC3447 (Big endian decoding)
r is the order of the BLS 12-381 curve defined in the v4 draft IETF BLS signature scheme
standard r=52435875175126190479447740508185965837690552500527637822603658699938581184513
```

Procedure

```
1. salt = "BLS-SIG-KEYGEN-SALT-"
2. SK = 0
3. while SK == 0:
```

```
4.     salt = H(salt)
5.     PRK = HKDF-Extract(salt, IKM || I2OSP(0, 1))
6.     OKM = HKDF-Expand(PRK, key_info || I2OSP(L, 2), L)
7.     SK = OS2IP(OKM) mod r
8. return SK
```

5.1.6 derive_child_SK

```
     derive_child_SK
The child key derivation function takes in the parent's private key
and the index of the child and returns the child private key.

 Inputs
parent_SK, the secret key of the parent node, a big endian encoded integer
index, the index of the desired child node, an integer 0 <= index < 2^32
 Outputs
child_SK, the secret key of the child node, a big endian encoded integer
```

Procedure

```
0. compressed_lamport_PK = parent_SK_to_lamport_PK(parent_SK, index)
1. SK = HKDF_mod_r(compressed_lamport_PK)
2. return SK
```

5.1.7 derive_master_SK

```
Inputs
seed, the source entropy for the entire tree, a octet string >= 256 bits in length
 Outputs
SK, the secret key of master node within the tree, a big endian encoded integer
```

Procedure

```
0. SK = HKDF_mod_r(seed)
1. return SK
```

5.2 Post-quantum security backup upgrade

SolareumChain is committed to adhering to a robust security strategy, drawing inspiration from the successful implementation of ERC-2333, specifically focusing on BLS12-381 Key Generation (https://eips.ethereum.org/EIPS/eip-2333). We've integrated a cutting-edge approach that involves the use of a Lamport key pair within our key derivation process. This step serves as a crucial intermediate layer, strategically positioned to address potential security concerns in the post-quantum era.

In the event that BLS12-381 becomes vulnerable to the advancements in quantum computing, SolareumChain has proactively designed a seamless transition plan. Our system is primed to swiftly pivot to a new signature scheme, such as Falcon signatures, or adapt to any guidelines established by the National Institute of Standards and Technology (NIST) regarding post-quantum security standards. This ensures that your data remains safeguarded even in the face of rapidly evolving threats in the quantum realm. Trust in SolareumChain to keep your digital assets secure and future-proof.

6 SolareumChain Algorithmic Security

In the ever-evolving landscape of blockchain technology and Renewable Energy, SolareumChain is positioning itself as an industry leader in relation to both innovation as well as sustainability. At the heart of our revolutionary platform lies an intricate web of algorithms we have meticulously crafted to safeguard the decentralized energy ecosystem. Our commitment to algorithmic security goes beyond the ordinary, ensuring that every transaction, every data point, and every interaction within the Solareum ecosystem is fortified with the highest level of protection. With a laser-sharp focus on the technical nuances of security, SolareumChain employs cutting-edge cryptographic techniques, Byzantine fault tolerance, and upcoming Layer 1 contract audits to guarantee the integrity and trustworthiness of our network. As the future of decentralized energy solutions unfolds, trust in security of Solareums underlying technology becomes paramount. SolareumChain stands at the forefront by setting new standards in algorithmic security that redefine the possibilities of a sustainable energy future.

6.1 BLS signature aggregation and Multisig security

6.1.1 BLS Signature Aggregation

Imagine you're sending a package through the mail, and you need several people to sign the delivery confirmation. In the world of blockchain transactions, signatures work similarly. When you make a secure transaction, you often need a digital signature to prove it's really you and that the transaction is valid.

BLS signature aggregation is like having a secure stamp that represents all the signatures you need on that package. Instead of collecting individual signatures from each person, you can combine them into one powerful signature. This is not only significantly faster but also reduces byte size, making things more efficient.

Effectively, Solareum's BLS Signature Aggregation simply means we have found a clever way to make transactions faster, more efficient, and ultra-secure by bundling all the necessary signatures together into one. Therefore, TPS is significantly impacted and Solareum will perform optimally.

6.1.2 Multisig Security

When you want to secure something important online, like your cryptocurrency wallet or sensitive documents, Multisig security lets you use multiple "keys" or signatures to access it. But here's the unique part: you don't need all the keys at once; just a certain number of them. For example, you might need at least two out of three keys to access your digital wallet.

By Solareum emphasizing our use of Multisig security, we're telling you that we take your online security very seriously. We're using a smart system that involves multiple layers of protection, making it incredibly hard for unauthorized people to access your valuable digital assets.

In a nutshell, BLS Signature Aggregation and Multisig security are like the superheroes of blockchain safety, making transactions faster and your digital currencies more secure.

6.1.3 BLS signature aggregation definitions

Consider a bilinear pairing

$$e : \mathbb{G}_0 \times \mathbb{G}_1 \to \mathbb{G}_T$$

which is efficiently computable, non-degenerate, and all three groups have prime order q, and $g_0 \in \mathbb{G}_0$ and $g_1 \in \mathbb{G}_1$ are generators. Let

$$H_0 : \mathcal{M} \to \mathbb{G}_0$$

be a Hash function treated as a random oracle.

Then the BLS signature scheme using the following definitions:

KeyGen(): choose $\alpha \leftarrow \mathbb{Z}_q$ randomly, let $h \leftarrow g_1^\alpha \in \mathbb{G}_1$, output $pk := (h), sk := (\alpha)$.

Sign(sk,m): output $\sigma \leftarrow H_0(m)^\alpha \in \mathbb{G}_0$

Verify(pk,m,σ): if $e(g_1, \sigma) = e(pk, H_0(m))$ output accept, otherwise reject.

With triples (pk_i, m_i, σ_i) for $1 \leq i \leq n$, anyone can aggregate the signatures $\sigma_1, ..., \sigma_n \in \mathbb{G}_0$ into a short convincing aggregate signature σ by computing

$$\sigma \leftarrow \sigma_1 \cdots \sigma_n \in \mathbb{G}_0.$$

Verifying an aggregate signature $\sigma \in \mathbb{G}_0$ is done by checking that the following condition is satisfied:

$$e(g_1, \sigma) = e(pk_1, H_0(m_1)) \cdots e(pk_n, H_0(m_n)).$$

6.2 Proving security definition references

A challenger and an adversary $\mathcal{A}$ are used in a Gedankenexperiment for describing multi-signature scheme security as follows.

6.2.1 Gedankenexperiment Setup

The challenger runs **KeyGen** to generate a key pair (pk, sk) and sends pk to the adversary.

6.2.2 Gedankenexperiment Signature queries

The adversary issues adaptive chosen message queries $m_1, m_2, ... \in \mathcal{M}$ and receives back signatures $\sigma_i = \mathbf{Sign}(sk, m_i)$ for $i = 1, 2, ... \in \mathbb{N}$ from the challenger.

6.2.3 Gedankenexperiment Forgery

Eventually, the adversary outputs a forgery: it outputs public keys $pk_1, ..., pk_n$, a message $m \in \mathcal{M}$, and a multi-signature σ.

The adversary has broken security if it did not issue a signature query for m and

$$\textbf{Verify}(pk, pk_1, ..., pk_n, m, \sigma)$$

outputs accept.

6.2.4 Security and co-CDH Assumption

We use

$$\textbf{SIGadv}[\mathcal{A}, \mathcal{S}; Q_{\text{sig}}, Q_{H_0}, Q_{H_1}]$$

to represent the adversary's advantage in attacking the scheme $\mathcal{S}$, for an adversary that makes at most Q_{sig} signature queries, at most Q_{H_0} queries to H_0, and at most Q_{H_1} queries to H_1. We say that the scheme $\mathcal{S}$ is secure if for all efficient adversaries the advantage is negligible.

The co-CDH assumption is that the security of the scheme $\mathcal{S}$ relies on the standard co-CDH assumption in the bilinear group $(\mathbb{G}_0, \mathbb{G}_1)$. The assumption states that for all efficient algorithms $\mathcal{A}$,

$$\textbf{CDHadv}[(\mathcal{A}, (\mathbb{G}_0, \mathbb{G}_1)] := \textbf{Pr}[\mathcal{A}(g_1^\alpha, g_0^\beta, g_0^\alpha), g_0^{\alpha\beta}] < \epsilon,$$

where ϵ is a neglible quantity and where $\alpha, \beta \leftarrow \mathbb{Z}_q$.

6.3 Adversaries and message query theorems

Our innovative message query theorems redefine the boundaries of data integrity, ensuring that every piece of information exchanged within the Solareum network is not only secure but also transparently verifiable. We believe that in a world increasingly reliant on decentralized solutions, technical excellence in security is non-negotiable.

Theorem 1 *Let $\mathcal{A}$ be an adversary attacking $\mathcal{S}'$ that makes no chosen message queries and at most one query to H_1. Let $\epsilon = \textbf{SIGadv}[\mathcal{A}, \mathcal{S}'; 0, Q_{H_0}, 1]$ be its advantage. Then there exists an adversary $\mathcal{B}$ for computing co-CDH, whose running time is about twice that of $\mathcal{A}$, with advantage $\epsilon' = \textbf{CDHadv}[\mathcal{B}'(\mathbb{G}_0), \mathbb{G}_1]$ such that $\epsilon' \geq \epsilon^2 - \epsilon/N$, where $N = |R|$, is the size of one coordinate in the image of H_1, thus $\epsilon \leq (1/N) + \sqrt{\epsilon'}$.*

Theorem 2 *Let $\mathcal{A}$ be an adversary attacking $\mathcal{S}'$ that makes no chosen message queries but potentially many queries to H_1. Then there exists an adversary $\mathcal{B}$ attacking $\mathcal{S}'$, that makes only a single query to H_1, and whose running time is about the same as $\mathcal{A}$, such that*

$$\boldsymbol{SIGadv}[\mathcal{A}, \mathcal{S}'; 0, Q_{H_0}, Q_{H_1}] \leq Q_{H_1} \cdot \boldsymbol{SIGadv}[\mathcal{B}, \mathcal{S}'; 0, Q_{H_0}, 1]$$

Theorem 3 *Let $\mathcal{A}$ be an adversary attacking $\mathcal{S}'$. Then there exists an adversary $\mathcal{B}$ attacking $\mathcal{S}'$, that makes no chosen message queries and whose running time is about the same as $\mathcal{A}$, such that*

$$\boldsymbol{SIGadv}[\mathcal{A}, \mathcal{S}'; Q_{sig}, Q_{H_0}, Q_{H_1}] \leq (e \cdot Q_{sig}) \cdot \boldsymbol{SIGadv}[\mathcal{B}, \mathcal{S}'; 0, Q_{H_0}, Q_{H_1}]$$

Corollary 1 *For every adversary $\mathcal{A}$ attacking $\mathcal{S}$ there is a co-CDH algorithm $\mathcal{B}$, whose running time is about twice that of $\mathcal{A}$, such that*

$$\boldsymbol{SIGadv}[\mathcal{A}, \mathcal{S}'; Q_{sig}, Q_{H_0}, Q_{H_1}] \leq (e \cdot Q_{sig} \cdot Q_{H_1}) \left(\sqrt{\epsilon} + \frac{1}{N} \right)$$

where $N = |R|$ and $\epsilon = \boldsymbol{CDHadv}[\mathcal{A}, (\mathbb{G}_0, \mathbb{G}_1)]$.

The proofs of which are left as an exercise to the reader.

6.4 Multi-Input Transactions and Transaction Validation Caching

In the dynamic realm of SolareumChain, validators hold the key to a game-changing advancement – the ability to seamlessly combine signatures from multiple transactions. SolareumChain will leverage the BLS signature aggregation mechanism, therefore enabling validators to craft leaner, more efficient blocks. This revolutionary approach paves the way for a streamlined and resource-efficient blockchain experience.

SolareumChain miners can choose to aggregate signatures across different transactions using the standard BLS signature aggregation mechanism which will ensure a smaller block size.

6.4.1 SolareumChain Multi-Input Transactions

For SolareumChain transactions that have multiple inputs, one currently includes all the signatures in the transaction. One can set things up so that all signatures are computed over the same message, namely the transaction data. When using BLS multi-signatures, anyone can aggregate all these signatures into a single multi-signature. If the user does not aggregate, the miner who mines the transaction can do it for them.

6.4.2 SolareumChain Transaction Validation Caching

SolareumChain transaction validation caching is a process whereby a SolareumChain node validates transactions as they are added to the node's mempool and marks them as validated. When a previously validated transaction appears in a new block, the node need not re-validate the transaction. Transaction validation caching is compatible with signature aggregation across multiple transactions in a block. To see why, consider a node that receives a new block containing an aggregate signature aggregated over n transactions in the block. The node can identify all the transactions in this new block that are already marked as validated in its mempool, and divide by the signatures associated with these pre-validated transactions. Effectively, the pre-validated signatures are removed from the aggregate signature. Now the node need only check that the resulting aggregate signature is a valid aggregate signature over the remaining transactions in the block, namely those transactions that are not already in its mempool.

7 SolareumChain ReFi Implementation

7.1 Proof of Hold (PoH)

SolareumChain holders above a discretionary threshold can be considered as part of the Proof of Hold algorithm as a form of auto-staking for consensus. That is, there exists N SRM in rewards as part of Proof of Hold for which of $n \in \mathbb{N}$ holders which meet the threshold of relevancy $k \in \mathbb{N}$ where $\epsilon < k < n$, then the union of all threshold relevant holders is the following time-parameterized set, where $t \in [t_0, t_1]$ provides a time-sampling interval with well-ordering of $t_0 < t_1$,

$$\mathcal{U}(t) = \bigcup_{i=1}^{n} \mathcal{U}_i(t)$$

for which

$$R(\mathcal{U}(t)) = R\left(\bigcup_{i=1}^{n} \mathcal{U}_i(t)\right) = \frac{\int_{t_0}^{t_1} \sum_{i=1}^{k} R(\mathcal{U}_i(t))dt}{\int_{t_0}^{t_1} \sum_{i=1}^{n} R(\mathcal{U}_i(t))dt}$$

and furthermore,

$$\int_{T\in\mathcal{T}} R(\mathcal{U}) = \int_{T\in\mathcal{T}} R\left(\bigcup_{i=1}^{n} \mathcal{U}_i(t)\right) dT = \int_{T\in\mathcal{T}} \left[\frac{\int_{t_0}^{t_1} \sum_{i=1}^{k} R(\mathcal{U}_i(t))dt}{\int_{t_0}^{t_1} \sum_{i=1}^{n} R(\mathcal{U}_i(t))dt}\right] dT$$

Thus, over changing time intervals per block, the Proof of Hold rewarder function will update throughout all intervals where $[t_{l-1}, t_l]$ runs over indices relevant for partitioning $T \in \mathcal{T}$, where $l \in \mathbb{N}$ determines the cardinality of the partition of time intervals.

7.2 SolareumChain Inherited NFT Multipliers

In the realm of Solareum NFT's, a unique evolution in utility, Solareum will allow the harnessing of the unique traits encoded within these ERC-1155 Tokens (the esteemed Tiered Solareum NFTs). These NFT's hold the key to unlocking a world of reward multipliers, revolutionizing the way Solareum approaches blockchain validation rewards.

7.2.1 Tidal Tier

1.1 Multiplier on SolareumChain Rewards

$$\textbf{Tidal}(R(\mathcal{U}(t))) = 1.1 * R(\mathcal{U}(t))$$

7.2.2 Wind Tier

1.15 Multiplier on SolareumChain Rewards

$$\textbf{Wind}(R(\mathcal{U}(t))) = 1.15 * R(\mathcal{U}(t))$$

7.2.3 Solar Tier

1.2 Multiplier on SolareumChain Rewards

$$\textbf{Solar}(R(\mathcal{U}(t))) = 1.2 * R(\mathcal{U}(t))$$

7.2.4 Fusion Tier

1.3 Multiplier on SolareumChain Rewards

$$\textbf{Fusion}(\mathcal{U}(t))) = 1.3 * R(\mathcal{U}(t))$$

8 SolareumChain Architecture and PoG Math

In the dynamic landscape of blockchain technology, the traditional paradigm of PoW validation, characterized by SHA-256 hashes and the global dominance of GPU mining, has undeniably brought innovation to the forefront. However, it's evident that its reign is approaching its twilight as the blockchain industry and society embrace the optimization potential sustainable initiatives like Solareum.

SolareumChain's architecture, where PoG (Proof of Generation) and PoH (Proof of Hold) Mathematics takes center stage, marks the dawn of a sustainable and environmentally responsible era in blockchain validation. This is more than just a technological evolution; it's a revolution that resonates with the most discerning minds in the field. SolareumChain want to contribute its proprietary PoG validation mechanism while ensuring both innovation and environmental responsibility coexist harmoniously.

In traditional blockchain systems such as BTC, electricity consumption from miners running SHA-256 algorithms to solve blocks for their rewards has been the mainstay of crypto. With the transition of PoW to PoS by some systems there is an advancement made by SolareumChain wherein energy generation rather than energy consumption is the basis for validation in Proof of Generation (PoG), a new consensus mechanism wherein algorithmic verification of generation of electricity rather than it's consumption provides the basis for transaction security and decentralized consensus. The blockchain trillema of scalability, decentralization, and security is addressed within this context as all three aspects can be satisfied through energy generation scalability having a positive societal impact and environmental effect rather than energy consumption which is not runaway scalably sustainable.

8.1 Societal Impact of Blockchain Technology

Examples of societal impact regulatory wise for influence of PoW mitigation and a need for a new solution include the January 2022 event of the European Securities and Markets Authority Vice-Chair Erik Thedéen calling on the EU to ban the proof of work model in favor of the proof of stake model due its lower energy emissions. Further, in November 2022 the state of New York enacted a two-year moratorium on cryptocurrency mining that does not completely use renewable energy as a power source. SolareumChain can address these concerns and improve beyond the Proof of Stake (PoS) model with validators ongoing energy generation fueling the consensus algorithm rather than energy consumption by GPUs for mining.

8.2 Energy Generation Analysis and Correlation

It is crucial for Solareum to dissect the lowest level details around renewable energy generation, leveraging state-of-the-art technology to dissect this data and unveil concealed connections. Solareums proprietary algorithms and data analytics will deliver a comprehensive understanding of energy generation dynamics, to then be leveraged by SolareumChain for the purposes of validation and security. We are redefining the boundaries of technology in energy analysis, enabling us to fuel innovation and optimize our blockchain for a more sustainable future.

Let $E_i(t)$ be an energy generation function parameterized by time

$$t \in [t_{i-1}, t_i]$$

corresponding to validator $i \in \mathbb{N}$, where $1 \leq i \leq V(t)$, where $V(t) \in \mathbb{N}$ is the total number of validators at time $t \in [t_{i-1}, t_i]$. Consider the well-ordered time-parameterized sequence of functions

$$\mathcal{E}(t) = \{E_1(t), ..., E_{V(t)}(t)\},$$

determined by an ordering norm wherein,

$$||E_{i-1}(t)|| \leq ||E_i(t)||,$$

and define the maximum energy generation from a validator as

$$E_{\mathbf{max}}(t) := \lim_{i \to V(t)} E_i(t) = \sup_{i \leq V(t)} \mathcal{E}(t) = ||E_{V(t)}(t)||$$

Then across the union of all time intervals

$$\mathcal{T} = \bigcup_{i=1}^{V(t)} [t_{i-1}, t_i] = [t_0, t_{V(t)}]$$

there exists the following inequality upper bounding the total energy generation

$$E_{\mathbf{total}}(t) \leq E_{\mathbf{max}}(t) * V(t)$$

More precisely, the exact total energy generation calculation is

$$E_{\mathbf{total}}(t) = \sum_{i=1}^{V(t)} ||E_{V(t)}(t)|| = \int_0^{V(t)} ||E_{V(t)}(t)|| dt$$

8.3 Energy Correlation Assurance Functions

Solareums innovative technology guarantees precision in energy correlation, enhancing our blockchains reliability and performance. SolareumChain is very well equipped for a future of seamless renewable-energy blockchain management, driven by our very advanced assurance functions.

Let there be an energy correlation assurance function

$$\mathcal{A} : \mathcal{E}(t) \to \{0, 1\}$$

which checks at a time $t \in \left[t_0, t_{V(t)}\right]$ that the energy generation claimed by a validator corresponds to electron flow which was not recycled through an anti-islanding feature of the ongoing flow corresponding to generation. That is, if there were to be a spoofed claim of electricity generation which was in surplus of the energy actually generated, the energy correlation assurance function would then sort the alleged energy validator as rejected if

$$\mathcal{A}(E_i(t)) = 0,$$

whereas it would be accepted if

$$\mathcal{A}(E_i(t)) = 1,$$

thus acting as a characteristic function at time

$$t \in \mathcal{T}_{,t} : [0, V(t)] \to \{0, 1\}$$

which is isomorphic to the energy correlation assurance function $\mathcal{A}$, that is,

$$\mathcal{A} \cong \chi_t,$$

where $\cong$ is an isomorphism in the category of binary output functions, thus allowing for the equivalence condition

$$\mathcal{A}(E_i(t)) = \chi_{t_i}(E(t_i)).$$

All characteristic function applications indexed across all times $t \in \mathcal{T}$ and validators $E(t_i)$ forms a matrix.

Therefore, simplified matrix notation

$$\mathbf{E}_{\text{claimed}}(t) \cdot \chi_t = \mathbf{E}_{\text{verified}}(t),$$

allowing for the verified Energy generators approved through not being zeroed out by the characteristic function and for spoofed Energy generators to be zero. Non-zero characteristic function outputs

$$\mathbf{E}_{\text{verified}} \neq 0$$

corresponding to a verified proof of electron flow which is not double counted. Similarly to the double spend problem solved by BTC, the double counted electron problem is solved as a main architectural basis of SolareumChain Proof of Generation.

8.4 zk-SNARK Validation

A BLS 12-381 signature of a zk-SNARK of verified energy generation is a required submission to have validation proven, that is, an algorithm runs to determine that the characteristic function output of the energy validator claim is non-zero, and if so provides either a 0 or a 1 as attached to the submission which either accepts the transaction as part of the validators or eliminates it from the consensus algorithm. The main hardware task of the FPGA running PoG is in the characteristic function calculation corresponding to the tracking of ensuring electrons are not double spent as calculated over a displaced current whereas recycled current will yield characteristic function outputs of zeros and thus not have weighted input into the PoG algorithm.

8.4.1 Case Study I: Proof of Hold and no Proof of Generation

A SolareumChain user $\mathcal{U}_i$, where $1 \leq i \leq V(t) \in \mathbb{N}$, acting without PoG inputs and only PoH will yield zero contribution to the PoG consensus mechanism, though will receive PoH rewards corresponding to the duration of time under which $\mathcal{U}_i$ does no SolareumChain transactions with the native token.

8.4.2 Case Study II: No Proof of Hold and Proof of Generation

A SolareumChain user $\mathcal{U}_i$, where $1 \leq i \leq V(t) \in \mathbb{N}$, acting without PoH inputs and only PoG will yield non-zero contribution to the PoG consensus mechanism, though will receive no PoH rewards corresponding to the duration of time under which $\mathcal{U}_i$ holds as it is assumed that SolareumChain transactions with the native token will all immediately occur within the same block prior to any elapsed time exceeding an interval partition cardinality. This type of user will JIT-compile send on any SolareumChain native tokens immediately to another SolareumChain address.

8.4.3 Case Study III: Proof of Hold and Proof of Generation

A SolareumChain user $\mathcal{U}_i$, where $1 \leq i \leq V(t) \in \mathbb{N}$, acting with PoG inputs and PoH will yield non-zero contribution to the PoG consensus mechanism, and will receive PoH rewards corresponding to the duration of time under which $\mathcal{U}_i$ does no SolareumChain transactions with the native token.

8.5 SolareumChain Address Generation

As blockchain evolves, one constant is certain: security reigns supreme. SolareumChain is not just committed to safeguarding your assets; we're raising the bar for unbreakable security. Our Address Generation process is incredibly technically sound, fortified with quantum-resistant Falcon signature technology and interim Lamport method security assurances.

Solareums cutting-edge Falcon signature technology, combined with interim Lamport method security assurances, ensures that your private key generation is a fortress against even the most determined quantum hacking attempts. When you use the SolareumChain dapp to generate a new address, you're not just creating an address – you're forging an unbreakable shield around your assets. No brute force from a quantum computer can compromise the sanctity of SolareumChain L1 addresses generated through our robust security measures.

To ensure that secure private key generation corresponding to SolareumChain L1 addresses is secure, and even post-quantum secure without mentioned interim Lamport method security assurances, a Falcon signature runs over generated addresses for private key security. That is, when a user is using the SolareumChain dapp and generates a new address, they must compute a Falcon signature for their private key generation such that not even brute-force from a quantum computer could hack the private keys corresponding to SolareumChain L1 addresses generated.

8.6 SolareumChain Genesis Architecture

After a genesis block creates the initial SolareumChain block, referred to as $\mathbf{B}_0$, which consists of a sole transaction of the first generated Null address executing a Falcon signature for which all SolareumChain native token (SRM) exist as transferred into the next block under which they begin providing the rewards to participants of Proof of Hold (PoH) and Proof of Generation (PoG) as per their respective algorithms. That is, the address 0x000000000000000000 generates a private key through a Falcon signature, for which there is an immediately burned OTP (one-time pad) self-execution that mints all SRM and then destroys access to the null address private key after the $\mathbf{B}_0 \rightarrow \mathbf{B}_1$ transaction mapping occurs, as the first block for which Proof of Hold accrues to be paid out at the end of the first block in confirmation leading to the $\mathbf{B}_1 \rightarrow \mathbf{B}_2$ transaction mapping and requires Proof of Generation occuring with at least three validators solving the Byzantine General problem for minimum 2/3 consensus to progress to the next block as is ongoing required by SolareumChain. That is, energy generation validators which compute the initial history of

$$IN : 0x000000000000000000[X\text{SRM}]$$
$$OUT : 0x000000000000000PoH[X\text{SRM} - \text{PoH}]$$
$$OUT : 0x000000000000000PoG[X\text{SRM} - \text{PoG}]$$

where X - PoH - PoG is the amount of potentially bridgeable SRM (ERC-20) tokens from Ethereum Mainnet.

8.7 Distributed Ledger Technology Energy Sustainability

SolareumChain's cutting-edge PoG/PoH hybrid consensus will revolutionize the blockchain landscape by delivering significant energy savings. Our technology leads the way in sustainable distributed blockchain solutions and will set the new standard for eco-conscious blockchain enthusiasts and enterprises alike.

While Bitcoin's PoW algorithm demands significant energy consumption for each block, SolareumChain's efficient operation during a single block cycle showcases the remarkable difference in energy conservation. Tomorrow's technology, today!

The difference saved from the operation of SolareumChain during one block compared to the energy consumption required by the PoW algorithm of the Bitcoin network provides an initial comparison of the energy savings caused by SolareumChain PoH / PoG hybrid consensus.

$$\Delta E = \text{Bitcoin}_{\text{PoW}} - \text{Solareum}_{\text{PoG}}$$

8.8 SolareumChain Bridge

A SolareumChain Bridge will operate to connect other EVM compatible L2 networks and ETH L1 with SolareumChain through a bridge which can wrap SolareumChain L1 tokens sent to EVM compatible blockchains, and can also allow for unwrapping of ERC-20 wrapped SRM which through an LP removal and pause function will migrate the existing SRM (ERC-20) to SRM (SolareumChain L1) and force users to interact with the SolareumChain Alt L1 as opposed to the Ethereum Mainnet L1. As bridge security is of utmost importance, the verification checks regarding bridged tokens from SolareumChain to other EVM compatible networks or Ethereum Mainnet are sufficient through including a zk-SNARK of the proposed transfer tokens Merkle Tree with a root test of prior transitively verified history. Conversely, bridges tokens from Ethereum Mainnet or other EVM compatible networks requires a checksum on the total remaining non-bridged tokens relative to total supply for a one-way function with speed. That is to say, bridging onto SolareumChain requires less computationally intensive effort than to bridge off of SolareumChain. The possibility for a one-way bridge only onto SolareumChain for which there is no exit may also be considered under alternative security and computational intensity reduction models.

8.9 Sufficiency of Sub 128-bit Security for Pairing-Friendly Curves on SolareumChain

Assurance of the discrete logarithm problem being hard relative to the prime group order r being at least 2*128 bits long as there are algorithms such as Pollard's rho algorithm that have a runtime cost of $\mathcal{O}(\sqrt{128})$ in big-Oh notation. Furthermore, the number field sieve method must not introduce vulnerabilities by ensuring that the extended field $\mathbb{F}_{q^k}$ is sufficiently large. Due to finite field extensions of size 3072, there exist actualized security levels of maximum 117-120 bits, which is deemed to be a perfectly adequate security level as per the NCC Group. That is, there exist within the prime group of order r faster than Pollard's rho algorithm for which there is a security threshold window of

$$||\mathcal{O}(\sqrt{120}) - \mathcal{O}(\sqrt{117})|| = 0$$

wherein there are equivalent Big-oh notation runtime results at the bit security boundary.

9 Conclusion

Through data collection with approved hardware solutions, and an innovative new architecture for ReFi including Proof of Generation and Proof of Hold, SolareumChain has positioned itself at the precipice of an explosion of DeFi adoption with an alt L1 blockchain with a unique selling point of energy generation based validation rather than energy consumption, and the value proposition of sustainability and environmentalism brought to distributed ledger technology.

From analyzing our vision and solution, as well as mathematical analysis of related matters including the BLS12-381 Elliptic Curve and zk-SNARK Proofs, as well as BLS Key Generation Signature Schemes, and cybersecurity as well as future security upgrades possible of the system. With signature aggregatio and multisig signature as well as adversary attacks in the context of explanation of mathematical theorems existing and cited for which further application so as to have multi-input transactions and transaction validation caching. With energy generation analysis and correlation explained, through the use of energy correlation assurance functions, and a unique approach to address generation and genesis architecture, there is sustainability and security brought to the forefront including for the SolareumChain Bridge and at least 117-120 bit security with a sub 128-bit security pairing-friendly curve meeting sufficient metrics prior to other potentially required improvements.

SolareumChain is at the forefront of ReFi, and in general distributed ledger technology, as a new protocol to implement into the world for the first time, a blockchain system which is based at it's core on energy generation rather than energy consumption, which if extrapolated into use with scalable energy validators could lead to improved lessening of carbon impact in global infrastructure for transactions of data and value.