SOLAREUM

Innovating ReFi: SolareumChain

Simplified ...

03/10/2023 info@solareuml1.com www.SolareumL1.com

CONTENTS

SOLAREUM (SRM)

Executive Summary

Big companies want to use blockchain technology, but they're worried about the environment, security, and some other things. At Solareum, we have a solution to these problems. We use two special mechanisms called Proof of Generation (PoG) and Proof of Holding (PoH). Our goal is simple: Be the best blockchain solution available for the renewable energy space while making it attainable and equitable for everyone.

Solareum's Solution

Solareum is doing something big to change how blockchain works. We're addressing the environmental problems and making sure no one has too much control (decentralizing). We believe that Solareum is bringing a new kind of technology to the industry that will make it better for everyone to use.

Solareum's Value Proposition

Solareum's promise to you is that we really care about blockchain, the environment, and making things better overall. We're leading the way in blockchain technology with our special mechanisms, PoG and PoH. We're also making sure that everyone has a fair chance and that things are safe and transparent. Our technology can be used in lots of different areas, not just one, which is a big deal.

WHAT IS SOLAREUMCHAIN?

Solareum Inc. is leading the way in blockchain technology with SolareumChain, a very advanced, green, Layer 1 (L1) blockchain solution. We use our special Proof of Generation (PoG) & Proof of Hold (PoH) mechanisms to make it work. Unlike regular blockchains that use up a lot of energy, SolareumChain does things differently. We leverage renewable energy generated from solar, wind, tidal & geothermal technologies to make it secure. Our own token, Solareum (SRM), will be available to buy/sell as well as being used for governance on SolareumChain.

People are passionate about using clean and green energy nowadays. They want to make power from things like the sun, wind, and water. This is where our PoG technology shines. It's not only good for the environment, but it also stops any one group from having too much power or control by decentralizing.

SolareumChain is open to everyone who makes renewable energy. This means big solar farms, wind farms, and even regular people with solar panels on their rooftops can help make SolareumChain secure. This new way of doing things makes the energy world fairer and more open, giving everyone a chance to be part of the renewable energy & blockchain revolution.

Join us on this journey to create a greener, more sustainable, and fair world. Together, we can change how blockchain works and make a better world for future generations.

MATHEMATICAL ANALYSIS OF VALIDATORS

At SolareumChain, we use advanced math to check how well validators are doing their job, and the validity of the energy source. Validators are critically important because they keep SolareumChain secure and make transactions run smoothly. We use math to optimize validators, find problems, and make SolareumChain run efficiently. This helps SolareumChain stay stable and trustworthy.

We also have some math formulas to describe the SolareumChain system, but we won't get into all the details here. Basically, we will group validators by the type of energy they generate. This helps us understand how well all the validators are performing and allows SolareumChain to run in the most effective & green way possible.

In simple terms, we use math to make sure the energy generators that act as validators on SolareumChain are doing their job correctly. It's part of how our solution works, especially our Proof of Generation (PoG) method.

SOLAREUM PROOF OF GENERATION:

SolareumChain L1 is bringing big innovation with Proof of Generation (PoG) as its heart. This exciting achievement makes sure that the renewable energy generated is verified and validated as an allowable source, which in turn then helps secure the SolareumChain blockchain.

We use reliable hardware like smart sensors and special computer chips (FPGA) to collect green energy data. These parts work together to make SolareumChain L1 better by effectively double-checking the data before allowing it onto the chain.

To keep our blockchain safe & secure, we use strong math called "BLS12-381 elliptic curve" with 128-bit security. This math proves that our validator data is real, making our blockchain very trustworthy.

The BLS12-381 Elliptic Curve for zk-SNARK Proofs

In today's digital world, keeping your information safe is super important. Our BLS Key Generation Signature Scheme Security is a high-tech solution that makes sure Solareum keeps your data and messages super secure.

This system uses fancy math to create keys that are really, really hard for bad guys to crack. It's like a super strong lock for your digital funds, whether it's important money stuff, secret messages, or important systems.

Solareum is always working on smart ways to protect you from high-tech problems, as you partake in securing the worlds greenest blockchain.

At SolareumChain, we use special private hardware to prove that you made the energy you said you did. We use strong math to make sure everything is real and safe. It's like making sure the numbers add up correctly first, then sharing that result with the world.

FPGA Hardware

We're using a special hardware called Solareums Field Programmable Gate Array (FPGA) for L1 validation. It's not made by us but by a third party. This cutting-edge hardware helps us do Proof of Generation (PoG) by running SolareumChain software.

The hardware is set up to do the math needed for validation more efficiently. This makes sure we don't need as much computing power for SolareumChain, leading to a much greener blockchain that any other existing technologies to date.

In simple terms, we're using this hardware to make SolareumChain work better and use less computer power, and be as green as possible.

BLS KEY GENERATION SIGNATURE SCHEME SECURITY

BLS Key Generation

We're using smart math to create secure keys for our system. These keys are like super locks to keep everything safe.

Here are the main steps we follow:

1. We use a process called key derivation to create keys from other keys. This process starts with a parent key, and we use it to make smaller keys.
2. We use a special math function called HMAC-Hash to do this. It helps us make really strong keys.
3. We also have a way to turn a number into a special kind of key called a lamport key. We do this using some clever math tricks to accomplish this.
4. We use these keys to make sure SolareumChain's data stays safe and secure.
5. We also have a way to create child keys from parent keys. This helps organize our keys in a tree structure.

6. We use a secret code called "seed" to start everything. It's like the beginning of our key system.

In the end, all these steps help us create and manage keys to keep our system safe and secure. The most advanced math available is being used to secure SolareumChain that positions us well not just for today, but also the future of quantum computing. We are thinking really far in advance, now.

Post-Quantum security backup upgrade

SolareumChain is serious about security. We've learned from the success of ERC-2333 and are using an advanced method called BLS12-381 Key Generation to keep things safe.

But we're also thinking ahead. If someday, the security method we use becomes weak because of advanced quantum computers, we're ready to switch to a new way of keeping things safe. We'll follow the guidelines from experts to make sure your data stays secure, no matter what new technology comes along.

You can trust SolareumChain to keep your digital stuff safe now and in the future.

SOLAREUMCHAIN ALGORITHMIC SECURITY:

SolareumChain is leading the way in both blockchain technology and renewable energy. We're all about innovation and making sure the blockchain world is eco-friendly.

Our platform is super secure. We've used advanced math and special techniques to protect everything that happens on SolareumChain. This includes every transaction, every piece of data, and every interaction. We're also getting our work checked by leading industry experts to make sure everything is trustworthy.

As we move into the future of renewable energy, you can trust that SolareumChain's technology is super safe. We're setting new standards to make sure the world's first renewable energy blockchain (SolareumChain Layer 1) is sustainable and secure.

BLS signature aggregation and Multisig security

BLS Signature Aggregation

Imagine you're sending a package and need multiple signatures on the delivery confirmation. In the world of blockchain, signatures work the same way. 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 one powerful stamp that represents all the needed signatures. Instead of collecting individual signatures from each person, we combine them into one. This is not only faster but also more efficient.

In simple terms, Solareum's BLS Signature Aggregation means we found a clever way to make transactions faster, more efficient, and super secure by bundling all the necessary signatures into one. This makes Solareum incredibly efficient and fast.

Multisig Security

When you want to secure something online, like your cryptocurrency wallet, Multisig security lets you use multiple "keys" to access it. But 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.

Solareum uses Multisig security to show that we take your online security seriously. We're using a smart system with multiple layers of protection, making it really hard for unauthorized people to access your valuable digital assets.

In short, BLS Signature Aggregation and Multisig security are like the superheroes of blockchain safety. They make transactions faster and your digital assets more secure.

Proving security definition references

We're going to talk about how secure SolareumChain is in a simple way.

Setting Up the Experiment

Imagine we have someone testing our security, called the challenger. They create a key pair (a public key and a secret key) and give the public key to a "bad guy" called the adversary.

Checking for Weakness

The bad guy can ask for signatures on different messages and get them from the challenger. They keep doing this until they think they found a way to break our security.

Finding a Weakness

If the bad guy succeeds in breaking our security without asking for a signature on a specific message, we have a problem.

Security and Assumption

We use a special measure to see how smart the bad guy is at breaking our system. If they can't do it efficiently, we say our system is secure. We also assume that our security relies on a common mathematical problem being hard to solve. This problem involves some numbers and is part of our security.

In simple terms, we're making sure our blockchain is really hard to break, and we assume it's because of a significantly challenging math problem that's tough to solve.

Adversaries and message query theorems

We've created some clever theorems to make sure our data is super secure and easy to check on the Solareum blockchain. Solareum demands and relies on decentralized solutions, we can't compromise on security.

Theorem 1

If someone tries to attack our system without asking for specific messages and only makes one type of query, we can measure how good they are at it. We can then use this to figure out how hard it is to solve a certain math problem. This makes it really hard for anyone to break our security.

Theorem 2

Even if someone asks lots of questions about one part of our system, we can still measure how good they are at breaking it. This helps us keep our security tight.

Theorem 3

When someone tries to attack our system, we can measure how many questions they ask and how good they are at it. This helps us make sure our system is super secure.

Corollary 1: We use the information from these theorems to make sure our system is twice as secure as it needs to be. We don't want anyone to break in easily.

We won't go into all the details here, but trust us, our system is really tough to break and the math supporting it is substantial!

Multi-Input Transactions and Transaction Validation Caching

In the world of SolareumChain, validators have a powerful tool – the ability to combine signatures from many transactions seamlessly. This feature uses something called BLS signature aggregation, making our blockchain more efficient.

SolareumChain Multi-Input Transactions: Sometimes, transactions have multiple inputs, and each input has its own signature. With BLS multi-signatures, all these signatures can be combined into one, making transactions smaller and effectively the transactions per second (TPS) faster. Even if users don't do this, validators can do it when they add the transaction to the blockchain.

SolareumChain Transaction Validation Caching: When SolareumChain checks a transaction and sees that it's valid, it marks it as validated. This way, if the same transaction appears in a new block, the node doesn't need to check it again. This works even if we combine signatures from multiple transactions in a block. Imagine a node receives a block with lots of transactions and one combined signature. It can figure out which transactions it has already validated and remove their signatures from the combined one. Then, it only needs to check the remaining transactions in the block, the ones it hasn't seen before. This makes things faster and much more efficient.

SOLAREUMCHAIN REFI IMPLEMENTATION:

Proof of Hold (PoH)

SolareumChain will reward holders who meet certain criteria through Proof of Hold (PoH). If you have a certain amount of SRM and meet the relevant threshold, you're instantly one of the SolareumChain validators. The rewards are based on the number of L1 SRM you hold. The more you hold, the more you earn.

SolareumChain Inherited NFT Multipliers

In Solareum's NFT world, we have special NFTs called ERC-1155 Tokens. These NFTs (only 151 in existence) have unique traits that give you reward multipliers on SolareumChain L1. These multipliers boost the rewards you earn for validating.

- **Tidal Tier** (x50)**:** If you have an NFT from this tier, you get a 10% boost on your rewards.
- **Wind Tier** (x50)**:** NFTs from this tier give you a 15% boost on your rewards.
- **Solar Tier** (x50)**:** Having an NFT from this tier gets you a 20% boost on your rewards.
- **Fusion Tier** (x1)**:** The NFT in this tier give you a 30% boost on your rewards.

These multipliers make holding these NFTs very rewarding. These NFT's can also be stacked, meaning a single wallet can stack any 2 NFT's together, so long as they are from different tier. This in turn gives additional reward possibilities to holders of the Solareum NFT's.

Solareum NFT's

https://opensea.io/collection/solareumnft

SOLAREUMCHAIN ARCHITECTURE AND POG MATH

In the ever-changing world of blockchain technology, we've seen the traditional way of validating transactions through Proof of Work (PoW) using SHA-256 hashes and GPU mining dominate the scene. It's been innovative, but it's time for a change. SolareumChain is ushering in a new era with a focus on sustainability.

SolareumChain's architecture is a game-changer. It's not just about technological advancement; it's a revolution. We're introducing Proof of Generation (PoG) and Proof of Hold (PoH) Mathematics as the core of our approach, and it's all about being environmentally responsible.

In traditional blockchain systems like Bitcoin (BTC), miners use a lot of electricity to solve complex problems and earn rewards. But SolareumChain is taking a different route. We're shifting from energy consumption to renewable energy generation as the basis for validation. PoG is a new consensus mechanism that verifies the generation of electricity rather than its consumption, making transactions secure and reaching a decentralized agreement.

This approach helps us tackle the blockchain trilemma – scalability, decentralization, and security. We can achieve all three without harming the environment. It's a step towards a more sustainable and responsible blockchain future and Solareum is leading the way.

Societal Impact of Blockchain Technology

Let's look at some real-world examples of why we need a new approach instead of the old Proof of Work (PoW) model in blockchain.

In January 2022, Erik Thedéen, the Vice-Chair of the European Securities and Markets Authority, called for banning the PoW model in the European Union. He wanted to switch to the Proof of Stake (PoS) model because it's more energy efficient. Proof of Generation (PoG) will take this type of legislation to new levels, as it is the greenest solution to date in blockchain technology.

In November 2022, the state of New York took action by putting a two-year pause on cryptocurrency mining. They did this to encourage miners to use renewable energy sources, albeit simply being green washing.

SolareumChain offers a solution to these concerns. Instead of using energy-consuming GPUs for mining like in PoW or relying solely on PoS which does still consume power, we use ongoing energy generation from validators to power our consensus algorithms. It's a more sustainable and efficient way to secure the blockchain and leads to a much greener solution than exists today.

Energy Generation Analysis and Correlation

It's essential for Solareum to dig deep into the details of renewable energy generation. We use cutting-edge technology to analyze this data and find hidden connections. Our special algorithms and data analysis give us a complete picture of how energy is generated. We use this knowledge in SolareumChain to ensure validation and security. We're pushing the boundaries of technology in energy analysis to make our blockchain more sustainable and innovative.

Let's break down some technical terms:

- **Ei(t):** This represents how much energy a validator generates at a certain time.
- **V(t):** It's the total number of validators at a given time.
- **E(t):** This is a sequence of energy generation functions over time.
- **Emax(t):** It's the maximum energy generated by any validator at a specific time.
- **Etotal(t):** This is the total energy generated across all validators at a given time.

In simpler terms, we calculate how much energy all validators produce together, and it's always less than or equal to the maximum energy one validator can produce. This helps us understand and optimize our blockchain for a greener future.

Energy Correlation Assurance Functions

Solareum's innovative technology ensures accurate energy tracking, making our blockchain more reliable and efficient for managing renewable energy sources. SolareumChain is well-prepared for a future of sustainable blockchain management, thanks to our advanced assurance functions.

We have an energy correlation assurance function called "A," which checks if the energy claimed by a validator matches the actual electron flow, ensuring there's no recycling of energy. If someone falsely claims to generate more energy than they actually did or attempts to generate it from a non-renewable source, the function rejects their claim (A(Ei(t)) = 0), but it accepts it if the claim is genuine (A(Ei(t)) = 1). This function acts like a switch, either allowing or rejecting energy claims at any given time.

In simpler terms, this function helps us make sure that energy generation is accurate, valid and not double-counted. It's a crucial part of SolareumChain's Proof of Generation, similar to how Bitcoin solves the double-spending problem.

Zk-SNARK Validation

In simple terms, to validate energy generation on SolareumChain, we require a BLS 12-381 signature, which is like a proof that the claimed energy generation is accurate. This proof goes through a process that checks if the energy validator's claim is legitimate and not zero. If it's valid, the submission gets either a 0 or a 1, which determines whether the transaction is accepted or rejected in the consensus algorithm.

The key task for the hardware (FPGA) running Proof of Generation (PoG) is to calculate the characteristic function. This function ensures that electrons aren't double-spent and tracks their movement. If any electrons are recycled or double-spent, the characteristic function will output zeros, and those transactions won't have any impact on the PoG algorithm.

Case Study I: Holding Without Generating

If a SolareumChain user (Ui) only holds tokens and doesn't participate in energy generation (PoG), their contribution to the PoG consensus is zero. However, they will receive PoH rewards for the time they hold tokens without making transactions.

Case Study II: Generating Without Holding

If a SolareumChain user (Ui) only participates in energy generation (PoG) and doesn't hold tokens, their contribution to the PoG consensus is non-zero. But, they won't receive PoH rewards as it's assumed they'll immediately send any tokens they receive to another SolareumChain address within the same block.

Case Study III: Holding and Generating

A SolareumChain user (Ui) who both participates in energy generation (PoG) and holds tokens will have a non-zero contribution to the PoG consensus. They will receive PoH rewards for the duration they hold tokens without making transactions during the times that PoG is not producing rewards (when renewable energy might not be generating, like Solar during dark periods).

SolareumChain Address Generation

In the ever-evolving world of blockchain, one thing remains constant: the need for top-notch security. SolareumChain is not just committed to protecting your assets; we're setting a new standard for unbreakable security. Our Address Generation process is also backed by cutting-edge Falcon signature technology along with the interim Lamport method security.

With Solareum's advanced Falcon signature technology and interim Lamport method security, your private key generation is like a fortress, impervious to even the most determined quantum hacking attempts. When you use the SolareumChain dapp to create a new address, you're not just making an address – you're building an unbreakable shield around your assets. Quantum computers can't break through the robust security measures protecting SolareumChain L1 addresses.

To ensure the security of private key generation for future SolareumChain L1 addresses, we will use Falcon signatures. When you generate a new address using the SolareumChain dapp, you compute a Falcon signature for your private key. This ensures that even the most powerful quantum computers can't hack your private keys.

SolareumChain Genesis Architecture

After the very first SolareumChain block, known as B0, is created from the genesis block, something important happens. In B0, there's just one transaction, and it involves a special address called the Null address. This address does a Falcon signature, a kind of digital signature, and as a result, all the SolareumChain native tokens (SRM) are moved to the next block. This is where they start being used to reward participants in Proof of Hold (PoH) and Proof of Generation (PoG) based on their respective algorithms.

Here's the key part: The Null address generates a private key using Falcon signature, and right after that, it's permanently locked and cannot be accessed again. This happens as we transition from B0 to B1, which is the first block where Proof of Hold rewards start accumulating. These rewards are paid out at the end of the block when we confirm B1 and move on to B2. But for us to move to the next block, we need Proof of Generation, which requires at least three validators to agree on the transactions. This agreement is essential for SolareumChain to keep moving forward.

In simple terms, energy generation validators play a crucial role in the early history of SolareumChain.

Distributed Ledger Technology Energy Sustainability

SolareumChain is introducing a game-changing hybrid consensus system called PoG/PoH that's all about saving energy. Unlike Bitcoin, which uses a lot of energy for each block, SolareumChain operates efficiently and consumes far less energy. This is a glimpse into the future of technology, available today!

SolareumChain is way more energy-efficient than other blockchains. The energy it saves in just one block cycle sets a new standard for eco-friendly blockchain solutions.

SolareumChain Bridge

SolareumChain is creating a bridge to connect with other blockchain networks, like Ethereum, in a secure way. This bridge will allow SolareumChain tokens to be used on other EVM compatible blockchains and vice versa. To ensure security, we use a special method called zk-SNARK to verify the tokens being transferred.

When tokens move from SolareumChain to other networks, we use a zk-SNARK to ensure their history is correct. But when tokens come from other networks to SolareumChain, we use a simpler and faster method called a checksum to check the total tokens being transferred.

In simple terms, it's easier and faster to bring tokens onto SolareumChain, and we're also exploring the idea of making it a one-way trip to enhance security and reduce computational complexity.

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

On SolareumChain, we ensure strong security against the discrete logarithm problem. This means it's very hard for anyone to figure out the secret values used in cryptographic operations. We do this by making sure that these secret values are at least 256 bits long, which is a high level of security.

We also take extra precautions to prevent vulnerabilities. Our security measures are on par with industry standards and are considered very safe, with a security level of around 117-120 bits. This level of security is more than enough to protect our system against potential attacks.

Solareum is taking significant steps to make sure our blockchain is very secure and that your data and transactions are well-protected.

CONCLUSION

SolareumChain is leading the way in the world of decentralized blockchains with its innovative, proprietary, approach. Instead of using a lot of energy like many other blockchain systems, SolareumChain uses a unique method based on energy generation, making it much more environmentally friendly and sustainable.

We've done a lot of research and analysis to make sure our architecture is secure and efficient. We've looked at, and are implementing, complex mathematical concepts like elliptic curves and cryptographic proofs to ensure our system's safety. We've also developed methods for handling various types of transactions and validating them.

Our system is not only secure but also sustainable. We've designed it to have a minimal impact on the environment, which is crucial in today's world. SolareumChain is on the cutting-edge of blockchain technology, and we're excited to bring our innovative approach to the world.

In summary, SolareumChain is a new and advanced layer 1 blockchain that focuses on energy generation instead of energy consumption. This unique approach makes it eco-friendlier and more efficient, and we're proud to be at the forefront of this technology and be leading the space to a greener and more equitable future for all.

SOLAREUM

Solareum Inc.

Pioneering Proof of Generation (PoG) validation technology on the world’s first sustainable Layer 1 Blockchain.

✉ info@solareuml1.com

🌐 www.solareuml1.com

📍 Dubai, UAE