Salvium ($SAL) /ˈsalviəm/

Noun (from Latin salvus, meaning safe, secure, salvation) A private, layer one protocol with yield generation, staking, and focus on regulatory compliance.

Introduction

Salvium is a cutting-edge proof-of-work private blockchain that seamlessly combines staking, privacy, and DeFi capabilities while navigating crypto regulations. Built on a fork of Monero, it retains Monero's advanced privacy features such as stealth addresses and ring signatures. However, Salvium introduces groundbreaking innovations that significantly alter transaction mechanics, creating a unique solution in the DeFi space.

Innovation

Salvium started as a research project to explore the potential of CryptoNote for private DeFi. The team revisited and prototyped work from Monero researchers, focusing on scalability, extensibility, and multi-chain interoperability. This research also considered global regulatory changes, especially under MiCA, positioning Salvium as an essential evolution of CryptoNote and Monero.

Salvium is taking a 'privacy-first' approach and striving to fully comply with the Markets in Crypto-Assets (MiCA) regulations. The first phases include features such as refundable payments and exchange modes to support compliance. Over the past year, we have made advancements in Conditional Payments (CP), refundable payments, native yield, and staking. Some of these features are ready for launch, while others will be included in future updates.

Salvium introduces unique technological advancements, such as Transactional Imbalances (TI) and Asynchronous Transactions (AT), forming the first native CryptoNote staking and yield system, driving future development, and forming the ecosystem's foundation.

Private DeFi

Building on these technological advancements, Salvium is poised to deliver robust Decentralized Finance (DeFi) features focusing on compliant, programmable privacy.

Programmable privacy: The Salvium base layer inherited exceptional levels of privacy from Monero. In cases where this level of privacy isn’t possible, such as compliant CEX interactions and DeFi applications, Salvium will empower DApp developers to build DApps with differing layers of privacy, which allow their users to select the type of data they share. This results in controllable or programmable privacy, without the typical limitations of traditional privacy coins.

DeFi Future

Salvium already includes features that make it mathematically possible to build DeFi applications on layer 1. This will be developed further in phase 3, where a layer 2 solution may be incorporated, with inherent performance and scalability benefits. In either case, these core innovations will help make DeFi more private.

Conditional payments: CP allows transactions to be conditionally executed based on predefined criteria. This will enable Smart Contracts, unlocking a torrent of potential applications.

Middleware: Salvium will offer middleware for seamless integration with other crypto platforms. This will allow developers to easily adapt applications written in languages like Solidity (Ethereum's primary DApp language) for use on Salvium. As a result, existing DApps can be quickly and efficiently launched on the Salvium network.

Potential DeFi Applications

Once these features are available on Salvium, 3rd parties will quickly build DAAPs, positioning Salvium as a privacy-focused alternative to Ethereum.

This includes Decentralized Exchanges (DEXs), Lending and Borrowing Protocols, Yield Farming, Stablecoins, NFTs, Memecoins, and Gambling.

Why does Crypto need Salvium?

Privacy is a fundamental human right, but this doesn't mean that it should be used for nefarious purposes. Salvium strives to create a decentralized platform that champions ethical usage, safeguarding user confidentiality while remaining compliant with applicable laws and regulations.

The new regulations affecting existing private cryptocurrencies create a pressing need for a novel privacy coin that ensures privacy and compliance. Most DeFi tokens operate on public blockchains, exposing sensitive user data. Salvium will address this issue by allowing users to balance privacy and regulatory compliance.

Achieving compliant privacy

The EU's MiCA regulations require privacy coins to adapt, which is a core focus of the Salvium project. As a first step, regulations will mandate centralized exchanges to unmask transactions involving privacy coins like Monero and ZCash. Privacy coins that fail to comply with these regulations risk delisting.

Regulation 2023/1114 of the European Parliament stipulates:

" The operating rules of the trading platform for crypto-assets shall prevent the admission to trading of crypto-assets that have an inbuilt anonymization function unless the holders of those crypto-assets and their transaction history can be identified by the crypto-asset service providers operating a trading platform for crypto-assets."

Source: https://eur-lex.europa.eu/eli/reg/2023/1114/oj Article 76 paragraph (3)

Key Features for Compliance

To comply with this particular regulation, the protocol will require:

1. **Ability to reject and return transactions:** A compliant protocol must allow exchanges to reject unauthorized transactions from unauthorized wallets. This feature is not typically possible with traditional privacy coins.

2. **Visibility of authorized wallets:** Exchanges require the ability to monitor transactions in authorized wallets used to deposit funds on their platform.

Salvium will meet this requirement by:-

1. Anonymously refundable transactions: a feature that is rare in other privacy coins.
2. A visible wallet (or subaddress) history. Users can provide a full view key that will give exchanges a “view wallet mechanism”, not only the limited view currently provided but complete history as required by the regulators.

Salvium’s approach enables selective transparency allowing users to control their privacy. For example, users can keep their transactions private but share a 'view key' with exchanges to verify their transaction history when required for compliance. This balances privacy and regulatory needs, like the revealing bank statements for tax purposes.

The goal is to maintain a leadership position in compliant privacy as the community proactively monitors and analyzes regulatory developments across various jurisdictions worldwide, particularly emphasizing the United States and the EU’s Markets in Crypto Assets (MiCA) regulation.

Project Phases

Phase 1: *Launch Salvium*

Staking and Yield Generation:

As a demonstration of the enhanced capabilities provided by Salvium’s evolved privacy, and a foundation of the Salvium concept, from launch users can stake their SAL tokens to earn rewards, fostering a secure and engaged network.

Also provided at launch is step one towards full compliance; refundable transactions, which allow for the return of unauthorized or incorrect transactions. Refundable transactions enable the recipient of any transaction to return that precise Input (minus the standard transaction fee) to the original sender without needing to request an address. This feature is trivial on public blockchains, but it is a major step towards compliance for a Monero-based chain.

Phase 2: Additional compliance features

Private Blockchain with Compliance Features:

Salvium will continually develop to meet stringent regulatory requirements, particularly the EU’s MiCA regulations. Phase 2 will mean users can keep their transactions private while providing authorized entities, like exchanges, with a view key to verify their transaction history. This approach ensures user privacy while remaining compliant with regulatory demands.

Salvium's development team is dedicated to advancing the foundational technologies of Monero and CryptoNote. We are committed to contributing to and supporting compliance initiatives, including Full Chain Membership Proofs, SERAPHIS, and JAMTIS, as opportunities arise. This commitment reflects our ongoing effort to enhance privacy, security, and regulatory compatibility within the Salvium ecosystem.

Phase 3: DeFi Support

Smart Contract Functionality and Private Token Issuance:

Leveraging the protocol_tx innovation, Salvium will enable smart contract functionalities, allowing complex DeFi applications to operate securely and privately on its network.

Middleware for Solidity:

To streamline adoption and development, Salvium will offer middleware that enables DApps developed in Solidity, the go-to programming language for Ethereum DApps, to be swiftly adjusted and deployed on its network. This move aims to simplify the transition of existing Ethereum projects to Salvium, effectively lowering the entry barrier for developers.

Fees and Incentives

Staking Rewards

Salvium (SAL) holders who stake their tokens will earn a staking reward. To participate, users must lock their SAL for a predetermined period (21,600 blocks - approx. 30 days). The staking rewards are distributed when the lock period expires. The rewards come from one of two sources depending on the project's phase.

Block Reward Sharing

Stakers will benefit from a 20% share of the block rewards during the project's initial phase. These rewards will be distributed proportionally among all active stakers, incentivizing users to participate in the network and supporting its security.

Long Term - DeFi fees

In the future, staking rewards will transition from a share of the block reward to a fee distribution model based on usage. Stakers and miners will receive system fees, similar to gas fees on other blockchain networks.

Technology

Salvium extends the CryptoNote protocol with several key innovations, including refund addresses, asynchronous transactions, and view keys showing entire wallet balances. These enhancements ensure top-tier anonymity while enabling complex rules and tokenomics for yield generation and the delivery of defi features.

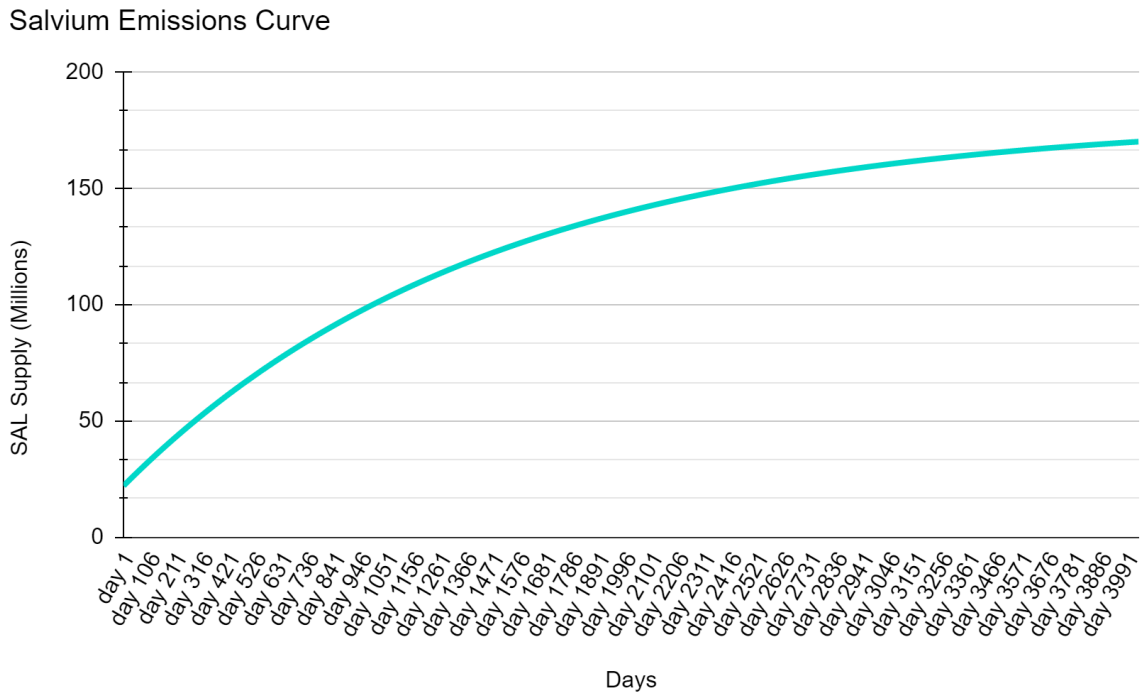
By leveraging advanced privacy technologies like ring signatures, stealth addresses, and zero-knowledge proofs, Salvium maintains privacy while allowing selective transparency for compliance purposes. These features collectively meet the demands for DeFi functionality, transaction privacy, decentralization, and responsible regulation, making Salvium a pioneering solution in digital finance.

Mining

Salvium is a Proof of Work coin that uses the RandomX mining algorithm. Once DeFi features are operational, miners will also receive a share of the System Fees.

Emission Schedule

The emission schedule is based on a modified version of Monero', to promote greater liquidity and adoption through wider distribution. While the block time remains at 120 seconds, the emission per block has been increased fivefold, and the initial supply duration has been doubled. This results in an initial supply, of 184.4 million coins, featuring a flatter and wider emission curve compared to Monero.



Tail Emissions

Like Monero, Salvium integrates a tail emission to ensure long-term mining incentives and network security. Once the maximum supply is reached, the protocol will emit 3 SALs per block.

Transaction Fees

Savlium transaction fees, much like those on Monero, are dynamic and depend on several factors. The calculation can be simplified as:

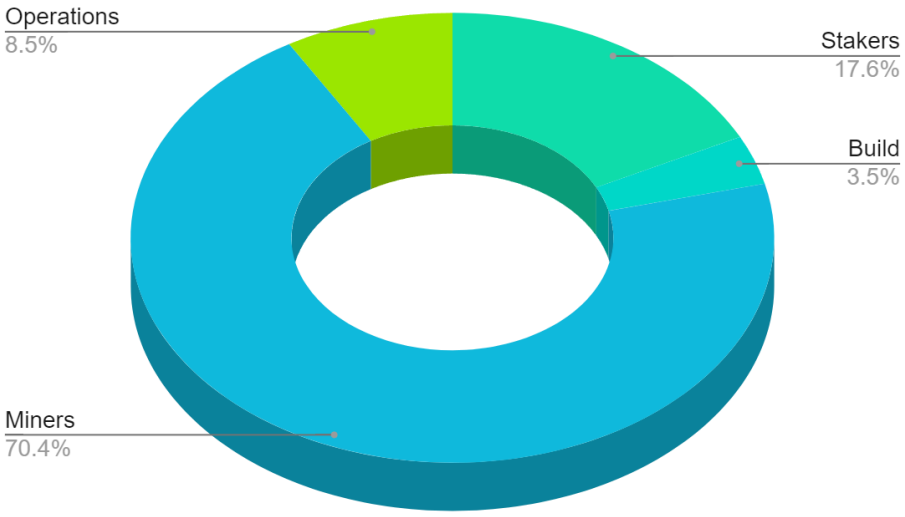
Fee = Base Fee × Transaction Size (kB)

Typical transaction costs will be very low.

Block Reward Structure: Each block mined on the Savlium network includes all the transactions submitted since the last block. The miner who successfully mines a block will receive all the fees from the transactions included in that block, along with any newly minted Savlium coins.

Salvium Token Allocation

The project is funded by a 12.01% pre-mine, which is partially locked. These funds will be allocated to build and operations. Miners and stakers will earn 88% of the total supply, plus tail emissions.



Note: Percentages shown are the proportion of Salvium's 184m coins, excluding tail-emissions.

1. Build - 3.5%

Salvium became a reality in early 2023 thanks to the vision and dedication of its early developers and contributors. 3.53% of the pre-mine will be allocated as incentives for these active team members and suppliers to support the project's launch.

2. Operations - 8.48% (locked)

The long-term success and sustainability of the Salvium protocol rely on continuous development and innovation. To support this, 8.48% of the initial supply is set aside for ongoing enhancements, smart contract integration, and new feature implementation through bounty and grant programs.

These tokens are time-locked in a governance wallet and released over 24 equal monthly installments. By the end of this period, the project aims to be self-sustaining, funded by system fees (gas fees) generated within the ecosystem.

3. Block Rewards - 87.99%

The block reward is initially split between stakers (20%) and miners (80%). Once DeFi features are operational, the miners will receive 100% of the block reward, as stakers will receive a share of system fees.

Independent Audits

Salvium will undergo independent security audits before major upgrades. Audit reports will be made public, demonstrating our commitment to transparency and security. Community feedback and audit findings will guide ongoing protocol improvements.

Pre-Launch Audit by Cypher Stack

The pre-launch audit of Salvium is focused on reviewing the mathematical validity and security of the key technologies that are unique to Salvium, namely:

1. The “transactional imbalance” mechanism. This was designed by the team and utilized to implement the “protocol_tx” technology, and

2. The “Return Address Scheme”, originally proposed by knacc, including the adaptations to support the asynchronous transactions implemented by the “protocol_tx” technology contained within Salvium

The pre-launch audit for Salvium was conducted by Cypher Stack, specialists in Monero security. Cypher Stack's expertise in cryptographic research, development, and consultation ensures that our platform is built on a solid foundation of security and innovation.

Team

The team consists of a broad community and developers. All cryptocurrency enthusiasts are committed and incentivized to act in the project's best interest. They each bring a wealth of experience and a proven track record of success in decentralized finance and private cryptocurrency.

Contact Information

Website: salvium.io

Discord: discord.gg/YJmdGcdtDt

X: x.com/salvium_io

GitHub: github.com/somerandomcryptoguy/salvium

Donate: https://salvium.io/donate/

Appendix 1

Token Distribution and Regulatory Stance

Following the European Union's regulations on crypto-assets, particularly the requirement for a "crypto-asset white paper," we present the following information:

1. Issuer Information: Salvium is developed by a decentralized team of crypto enthusiasts and developers committed to advancing privacy-focused blockchain technology.
2. Project Overview: Salvium aims to create a privacy-centric blockchain that combines the benefits of Monero's privacy features with regulatory compliance and DeFi capabilities.
3. Distribution and Regulatory Status:
    - Salvium (SAL) is not conducting a public offering. The initial distribution of SAL tokens occurs solely through mining.
    - A small portion of the total supply has been pre-mined to support development and operations.
    - As Salvium is not making an offer to the public (ICO) it does not currently fall under the scope of the EU regulation on crypto-assets that requires a crypto-asset white paper for public offerings.
    - While we are not currently subject to these specific regulations, we are committed to maintaining transparency and adhering to best practices in the cryptocurrency space.
4. Rights, Obligations, and Voting: a) Rights:
    - SAL miners participate in network consensus through mining, holders may engage in staking for rewards, and use the token for transactions within the Salvium ecosystem.
5. Obligations:
    - Token holders are obligated to comply with applicable laws and regulations in their jurisdictions.
6. Voting Rights:
    - Holding SAL tokens does not confer any voting rights or governance control over the Salvium project.
    - The project's development and decision-making processes are open and collaborative, with contributions welcomed from the entire Salvium community. While a core group of developers may guide certain aspects of the project, we strive for decentralization in both our technology and our governance.
7. Underlying Technology: Salvium is built on a fork of the Monero codebase, utilizing CryptoNote protocol with additional innovations such as Transactional Imbalances (TI) and Asynchronous Transactions (AT).
8. Related Risks:
    - Regulatory Risk: The cryptocurrency regulatory landscape is rapidly evolving. While Salvium is committed to regulatory compliance, there is no guarantee that we will be able to meet all future regulatory requirements. Changes in regulations could potentially impact Salvium's operations, the use of SAL tokens, or their value. Users should be aware that: a) New regulations may be introduced that could affect Salvium's legal status or operational model. b) Our interpretation of existing regulations may differ from that of regulatory authorities. c) Despite our best efforts, we may not be able to adapt to all regulatory changes promptly. d) Future offerings of Salvium may be subject to different regulatory requirements.
    - Technology Risk: As with all blockchain projects, there's a risk of undiscovered vulnerabilities in the code or underlying cryptographic principles.
    - Market Risk: The value of SAL tokens may be volatile and subject to market conditions.

- Adoption Risk: The success of Salvium depends on community adoption and development.

This information is provided in good faith and represents our current understanding and plans. It should not be considered as financial advice. We encourage all prospective participants to conduct their own research and seek professional advice if needed.