Savitri Foundation

Savitri Network White Paper

Savitri Foundation – Andrea Cadamuro

v 1.0.0, March, 01, 2024

Savitri Foundation

The first rule of any technology used in a business is that automation applied to an efficient operation will magnify the efficiency. The second is that automation applied to an inefficient operation will magnify the inefficiency.

Bill Gates

Introduction

The Savitri project emerges at the forefront of the blockchain revolution, proposing a transformative approach to how digital ecosystems are perceived, developed, and interacted with. At the heart of Savitri lies a vision to harness the power of blockchain technology not just as a foundation for cryptocurrencies but as a bedrock for a decentralized future where digital interactions are secure, efficient, and accessible to everyone, regardless of their technical expertise or geographic location.

Savitri is built upon the innovative Proof of Unity (PoU) consensus mechanism, a novel approach designed to address the perennial challenges faced by existing blockchain technologies—scalability, security, and environmental sustainability. By moving away from the competitive nature of traditional consensus mechanisms, PoU fosters a collaborative environment where nodes work together to secure the network and process transactions. This paradigm shift not only facilitates faster transaction speeds and lowers costs but also ensures a more democratic and inclusive blockchain ecosystem.

What sets Savitri apart is its unwavering commitment to integrating blockchain technology seamlessly into daily life. The project goes beyond the technical intricacies to democratize access to blockchain, making it a tool not just for financial transactions but for a myriad of applications that can benefit from its underlying principles of transparency and immutability. Through initiatives like the Savitri Foundation, the project endeavors to break down barriers to blockchain adoption, offering educational resources, development support, and intuitive tools to empower users and developers alike.

Savitri's vision is underpinned by a commitment to sustainability and decentralization. The network's design supports smart contracts, IoT integration, and automated operations, laying the foundation for a future where digital services and applications are not only secure and transparent but also equitable and free from centralized control. This commitment extends to fostering a collaborative ecosystem, inviting developers, entrepreneurs, and visionaries to contribute towards a decentralized digital revolution.

As the digital world continues to expand at an unprecedented rate, the need for a blockchain solution that is secure, scalable, and accessible becomes increasingly apparent. The Savitri project represents a bold stride towards meeting this need, offering a beacon of hope for a future where blockchain technology fulfills its revolutionary potential. By championing innovation, collaboration, and inclusivity, Savitri is not just a blockchain project but a movement towards a more secure, decentralized, and equitable digital future.

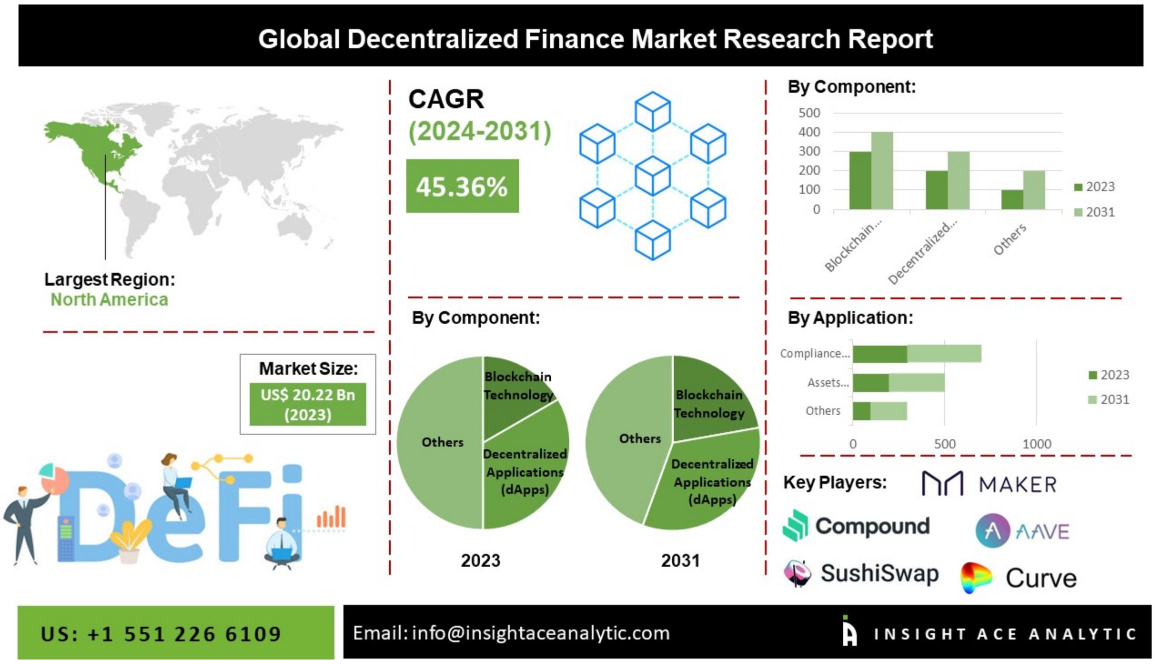
Contents

1. Market Overview

In the rapidly evolving landscape of blockchain technology, the market is ripe with opportunities and challenges. As of now, blockchain technology is not just a buzzword but a critical infrastructure for numerous industries, offering solutions for secure, transparent, and efficient transactions. The global blockchain market, growing at an unprecedented rate, is projected to reach billions of dollars in value within the next few years. This growth is fueled by the increasing adoption of blockchain in finance, supply chain, healthcare, and more, highlighting its potential to revolutionize traditional business models.

However, the path to widespread adoption is not without obstacles. Issues such as scalability, security, and user accessibility continue to hamper the full potential of blockchain technologies. Additionally, the environmental impact of certain consensus mechanisms, like Proof of Work, has raised significant concerns.

In this dynamic market, Savitri positions itself as a game-changer. By addressing these challenges head-on with its innovative Proof of Unity (PoU) consensus mechanism, Savitri offers a more secure, scalable, and environmentally friendly blockchain solution. With its focus on accessibility and integration into everyday life, Savitri is poised to drive blockchain technology beyond its current financial applications, making it a foundational element for a wide range of digital solutions.an inclusive community through active engagement on social media, forums, and blockchain events. Offering incentives for community contributions, such as development, testing, and content creation, can further encourage participation..



1.1. Market Strategy

To capitalize on the burgeoning blockchain market and navigate its complexities, a comprehensive and reliable market strategy is essential, especially for a non-profit foundation like Savitri. Here's how Savitri plans to make its mark:

1. **Educational Initiatives:** Increasing blockchain awareness and understanding is crucial for adoption. Savitri will launch educational programs and workshops targeting both developers and the general public to demystify blockchain technology and highlight its potential beyond cryptocurrencies.
2. **Partnerships and Collaborations:** Establishing strategic partnerships with key industry players across various sectors, including finance, healthcare, and supply chain, can showcase the practical applications of Savitri's blockchain. Collaborating with academic institutions for research and development can also enhance the network's credibility and utility.
3. **Community Engagement:** Building a strong, engaged community is vital for the success of any blockchain project. Savitri plans to foster an inclusive community through active engagement on social media, forums, and blockchain events. Offering incentives for community contributions, such as development, testing, and content creation, can further encourage participation.
4. **Sustainability Focus:** With environmental concerns becoming increasingly important, Savitri's eco-friendly PoU mechanism provides a competitive advantage. Highlighting this aspect in all communications will appeal to eco-conscious investors and users.
5. **Innovation and Development** Grants: Offering grants and funding to developers for innovative applications built on the Savitri blockchain can stimulate creativity and utility, driving the network's growth and adoption.
6. **Open-Source Development:** Emphasizing the open-source nature of Savitri encourages collaboration and transparency, attracting developers and ensuring the continuous improvement of the platform.
7. **Market** Positioning and Branding: Clearly articulating Savitri's unique value propositions, such as its democratic consensus mechanism, scalability, and integration capabilities, is essential. A strong branding strategy that resonates with both technical and non-technical audiences will help Savitri stand out in a crowded market.

37

of the most important project blockchain layer 1

2. *Problem Overview*

In the current blockchain ecosystem, a range of critical issues hampers the full realization of its revolutionary potential. These challenges, encompassing centralization and security, scalability and transaction costs, accessibility, adoption, and environmental sustainability, demand innovative solutions. Savitri's vision proposes transformative approaches to tackle these issues, positioning itself as a pioneer in the next generation of blockchain technology tools to broaden user adoption.

,.

2.1. Decentralized blockchains, face a series of inherent challenges

Scalability: One of the primary issues with decentralized blockchains is their limited ability to process a high volume of transactions quickly and efficiently compared to centralized systems. As the number of users and transactions grows, the network can become congested, leading to slower transaction times and higher fees.

- **Energy Consumption:** Certain consensus mechanisms, like Proof of Work (used by Bitcoin), require substantial computational power and energy consumption. This has raised environmental concerns and sparked a debate on the sustainability of such blockchain networks.

- **Security:** While decentralized blockchains are generally secure, they are not immune to attacks. For instance, a 51% attack, where a single entity gains control of the majority of the network's mining power, can threaten the network's integrity. There's also the risk of smart contract vulnerabilities.

- **Interoperability:** Many blockchain networks operate in silos and lack the ability to communicate with one another. This limits the potential for widespread adoption of blockchain technology, as seamless interaction between different blockchains is crucial for many applications.

- **Regulation and Legal Challenges:** The decentralized nature of blockchain poses regulatory challenges. Jurisdictions around the world are still figuring out how to regulate cryptocurrencies and blockchain technology, leading to a landscape of legal uncertainty for users and developers.

- **Usability and Accessibility:** For many users, blockchain and cryptocurrency technologies remain complex and difficult to understand. This usability barrier hinders adoption among the general public, who may benefit from blockchain technology's offerings.

- **Centralization Tendencies:** Despite the decentralized ideal, there is a trend towards centralization in certain aspects of blockchain ecosystems, such as mining pools in Proof of Work blockchains or the concentration of wealth and voting power in Proof of Stake systems. This can lead to unequal power dynamics within supposedly decentralized networks.

- **Data Privacy:** Public blockchains are transparent, meaning transactions are visible to everyone. This poses privacy concerns for users who may not want their financial transactions or interactions to be publicly accessible.

2.2. Savitri is the solution of challenges of blockchain market

Savitri tackles key challenges facing today's blockchain technology with innovative solutions. Central to its strategy is the Proof of Unity (PoU) consensus mechanism, designed to combat the trend towards centralization by fairly distributing authority across all nodes, enhancing network security and promoting inclusive governance. By optimizing transaction processing. Savitri addresses scalability and transaction cost issues, enabling faster speeds and lower costs without compromising on security or decentralization. The project also focuses on making blockchain technology more accessible and user-friendly, through initiatives like the Savitri Foundation, which provides educational resources and intuitive tools to broaden user adoption.

Furthermore, Savitri is committed to environmental sustainability, with its PoU mechanism requiring significantly less energy than traditional Proof of Work systems. This reflects a broader vision for blockchain as a foundation for new applications, from decentralized finance to secure data management, aiming to make blockchain as integral to digital services as the internet today. With an emphasis on inclusivity and sustainability, Savitri aspires to leverage blockchain for global challenges like financial inclusion and a low-carbon economy. Savitri's layer-1, open-source, decentralized network, powered by PoU, stands out as faster, cheaper, more democratic, and eco-friendly, marking a significant step towards a secure, scalable, and sustainable digital future.

3. *Why Savitri*

Savitri stands as a beacon in the blockchain technology landscape, promising a revolution in the world of decentralized networks. This white paper highlights why Savitri is the cornerstone choice for developers, investors, and users seeking innovative, secure, and democratic solutions in the realm of cryptocurrencies and blockchain technology. Savitri is more than a blockchain; it's a movement towards a decentralized digital revolution, inviting developers, entrepreneurs, and visionaries to contribute to shaping a future where technology enhances freedom, security, and community. Through collaborative effort and innovative solutions, Savitri aims to redefine the landscape of blockchain technology, making it a tool for positive change in the digital age.

In conclusion, Savitri represents not just a response to the current challenges of blockchain technologies but also a bridge to a future where blockchain and cryptocurrencies play a central role in technological innovation, digital security, and global economic empowerment. Choosing Savitri means embracing a vision of the future where blockchain technology serves humanity, making the digital world a safer, fairer, and more inclusive place.

3.1. How did it start?

Savitri was born in 2021, rooted in an idea and a dream that had been nurtured through years of research: to create a truly decentralized network capable of solving today's persistent issues. Currently, many blockchains that started with decentralization in mind are increasingly moving towards becoming federated systems, or in some cases, centralized. This shift is largely due to the prohibitive costs for ordinary individuals to become active members and the minuscule rewards they receive. These challenges are leading to greater centralization in the hands of large investors, whether through mechanisms like Proof of Stake (PoS), Proof of Work (PoW), or other models.

For this reason, we developed Savitri, a network and a consensus mechanism called Proof of Unity (PoU) designed to change the paradigm from a completely competitive system to a collaborative one. In our network, nodes are not meant to compete but to collaborate in order to reach consensus. Moreover, we have also shifted the paradigm regarding the creation of fees. We do not believe in centralization, fixed fees, or percentages, as the value can vary significantly over the long term. Hence, we have introduced a different logic: a fee management system based on the agreement among all network nodes, which will have the right to vote once a month to define the fees.

This model is aimed at addressing the centralization issues faced by current blockchain technologies, promoting a more inclusive and equitable framework. By emphasizing collaboration over competition and introducing a democratic fee system, Savitri is poised to redefine the landscape of blockchain networks. Our commitment to innovation and decentralization reflects our vision for a more accessible and balanced digital future. Join us in this journey towards creating a truly decentralized network that solves the challenges of today's blockchain technologies.

4. *System architecture*

4.1. Network Layer

The Savitri blockchain operates through a network of interconnected nodes, including the Savitri-node and masternode. This software is versatile, functioning as a core block producer, a relay, or a local access point to the network. The node is comprised of various interconnected components, ensuring seamless operation and connectivity within the Savitri ecosystem.

- **The settlement layer:** The settlement layer is primarily concerned with the ownership and transfer of assets over the blockchain. It's where are defined the rules of Savitri

- **The data layer:** in a blockchain refers to the foundational level that handles how data is structured and stored across the network. It's one of several layers that make up the architecture of blockchain technology, each with its own distinct functions and responsibilities.

- **The consensus layer:** in a blockchain is crucial for ensuring that all participants in the network agree on a single, truthful version of the ledger without the need for a central authority. It's what makes Savitri technology so revolutionary for creating trust in a decentralized system.

- **The Execution Layer:** in a blockchain refers to the component responsible for executing transactions and smart contracts according to the rules and logic defined within them. This layer processes the instructions contained in each transaction, ensuring they are carried out correctly on the blockchain.

4.2. Savitri's components

Node:

In the dynamic landscape of the Savitri blockchain ecosystem, a node represents a fundamental building block, serving as the backbone of the network's decentralized architecture. Nodes are individual computers or servers that connect to the Savitri blockchain network, playing a crucial role in maintaining the network's integrity, security, and accessibility. Each node possesses a complete or partial copy of the blockchain, ensuring redundancy and resilience against data loss or manipulation.

Operating a node on the Savitri blockchain is both a privilege and a responsibility, allowing participants to contribute directly to the network's operation. It represents a commitment to the principles of decentralization, transparency, and security that are foundational to blockchain technology. Node operators, through their dedication and collective effort, enable the Savitri blockchain to function as a secure, scalable, and decentralized platform, ready to support a wide array of applications and innovations.

Masternode:

Within the Savitri blockchain ecosystem, a Masternode is a key infrastructure component that plays a crucial role in enhancing network functionality, security, and governance. Unlike standard nodes that primarily support basic transaction verification and block propagation, Masternodes are empowered with additional responsibilities and capabilities, making them pivotal to the network's overall performance and resilience.

Masternodes are highly trusted and resource-committed nodes that require a significant stake in the network's native token to operate. This staking mechanism serves a dual purpose: it incentivizes the provision of high-quality services by the Masternode operators and secures the network against malicious actors. The elevated requirements and responsibilities of Masternodes ensure that only dedicated and invested participants contribute to critical network operations.

Proof of unity

Proof of Unity (PoU) is an innovative consensus mechanism employed in the Savitri blockchain, designed to tackle the challenges of security and centralization plaguing traditional blockchain networks. Unlike competitive models like Proof of Work (PoW) or Proof of Stake (PoS), PoU fosters a collaborative environment where network nodes work together to ensure security, streamline operations, and minimize environmental impact.

The mechanism is based on the equitable distribution of authority and participation across all nodes, democratizing access and governance of the network. This approach not only speeds up transaction processing and reduces associated costs but also encourages broader participation in the network, ensuring it remains open and accessible to everyone.

PoU is crucial for achieving true decentralization, addressing the issue of power concentration in the hands of a few entities or individuals that could compromise network security. Moreover, PoU's design aims at a balance between energy efficiency and performance, positioning Savitri as an eco-sustainable blockchain solution.

In summary, Proof of Unity represents a significant advancement in blockchain consensus mechanisms, offering a more secure, fair, and sustainable platform for decentralized applications.

Block:

In the Savitri blockchain, a "Block" is a fundamental component that represents a set of recorded transactions and data, securely linked together in a chronological chain. Each block contains a comprehensive record of multiple transactions that have occurred within the network at a given time, along with a reference to the previous block, thereby forming an immutable sequence known as the blockchain.

The structure of a block in Savitri is meticulously designed to ensure the integrity, security, and traceability of data. It comprises the block header, which includes essential metadata such as the cryptographic hash of the previous block, a timestamp, and the block's own hash value. This ensures each block is uniquely identifiable and securely anchored within the blockchain's history, preventing unauthorized alterations.

Moreover, blocks in Savitri are created through a consensus mechanism known as Proof of Unity (PoU), which emphasizes collaboration over competition among network participants. This innovative approach not only enhances the efficiency and scalability of transaction processing but also significantly reduces the environmental impact associated with traditional blockchain consensus models.

In essence, a block within the Savitri blockchain is more than just a data container; it is a cornerstone of digital trust, enabling transparent, secure, and decentralized transactions across the network. This design facilitates a wide range of applications, from financial transactions to complex smart contracts, making Savitri a versatile platform for the next generation of blockchain technology.

Monolith Block

In the Savitri blockchain ecosystem, the Monolith Block stands as a pioneering architectural element designed to streamline network efficiency and accessibility. Unlike traditional blocks that contain transactional data or smart contract executions, the Monolith Block serves a specialized function by encapsulating a comprehensive snapshot of the network's state at regular intervals. This includes an updated registry of active nodes and masternodes, ensuring that participants have immediate access to the most current network configuration.

Created daily, the Monolith Block facilitates a seamless entry for new nodes, enabling them to quickly synchronize with the network's current state without the need to process the entirety of the blockchain's history. This is particularly beneficial for maintaining high levels of network scalability and performance, as it significantly reduces the bandwidth and storage requirements for nodes joining the network.

The structure of the Monolith Block is meticulously engineered to include only the essential information required for network synchronization, making it remarkably lightweight compared to standard blocks. This design choice not only expedites the onboarding process for new nodes but also minimizes the computational load on the network, contributing to the overall sustainability and efficiency of the Savitri blockchain.

By incorporating the Monolith Block into its architecture, the Savitri blockchain addresses common challenges associated with blockchain scalability and node synchronization. This innovative approach underscores Savitri's commitment to fostering an accessible, efficient, and scalable blockchain ecosystem, paving the way for a more inclusive and dynamic digital future.

4.2.1. Node

Node Registration Simplified:
In our network, while anyone can run a node and join the network, only a select group of nodes has reached the highest score in the round can create blocks and receive Savi Coin. The process for a node to become registered or to be removed from the registry is governed entirely by the network's rules, without any single user or authority having control over these decisions. This approach is designed with three main goals in mind:

- **Enhancing Security:** To safeguard against the theft of private keys and to prevent attackers from compromising the network by taking control of a majority of nodes.

- **Maintaining Network Integrity:** To ensure that only productive nodes, or those not exploiting the network in unforeseen ways, remain active and eligible for rewards.

- **Regulating Node Participation:** To manage how new nodes join the network and to remove inactive or non-contributing nodes efficiently.

Here's how we address each goal:

- **Separating Private Keys:** Unlike systems where block creation requires the node operator's private key to be on the node itself, potentially exposing it to theft or attack, we keep the private key separate from the block creation process. This minimizes the risk of key theft from online nodes, especially those hosted on virtual private servers (VPS), where data center operators might otherwise access the keys.

- **Controlling Node Registration:** To prevent an attacker from overwhelming the network by registering a multitude of nodes simultaneously, our protocol limits the number of new nodes that can join the registry within a certain period. This control helps to prevent a single entity from gaining a majority control of the network.

- **Removing Inactive Nodes:** Through a scoring system, our Proof of Unity algorithm identifies and removes nodes that are offline or not actively participating. Nodes with a zero score are automatically ejected from the registry but can rejoin once they become active again.

Field	**Description**
Public Key	*The public key corresponds to the node's configured private key. When blocks or Proof of Unity messages are produced by a node, the signatures can be validated against this key.*
Account Address	*The account address of the node owner's account. This account may legally change or remove the node registration, and any participation rewards earned by the node are credited to this account.*
Locked Balance	*An amount of funds that the node's owner has put up as collateral to compete for a spot in the registry, and to incentivize her to maintain the security of her node's private key.*
Participation Score	*A score tracked for this node over time by the Proof of Unity algorithm. A higher score increases the number of rewards received, while falling to zero will cause the node to be ejected from the registry.*

The Node's Public Key and Security

Each node in the Savitri network maintains a private key to sign blocks, ensuring transactions and messages are authentically from the node. This private key, ideally stored securely on the node's device, can also be managed through a separate hardware device for enhanced security. This measure is crucial because if a node's private key is compromised, it risks impersonation and potential loss of locked funds by attackers.

Locked Balance for Registry Maintenance

To be part of the registry, a node owner locks a certain amount of Savitri tokens. These funds are deducted from the owner's account and held by the network as a security deposit. If a node is removed or voluntarily exits the registry, these funds are fully returned. The size of the locked balance plays a role in prioritizing the node's position in the registration queue, serving as a deterrent against Sybil attacks without relying solely on Proof of Stake principles.

The Registration Queue

Nodes awaiting registry entry are placed in a registration queue, ordered by the amount of their locked funds. Admissions from the queue to the registry occur at regular intervals, with the pace adjusted based on the registry's size to maintain network security.

Registering a Node

Registration involves submitting a transaction with the node's public key, a proof of ownership (a special message signed by the node's private key), and the locked fund amount. This transaction, higher in fee to prevent abuse, locks the specified funds and adds the node to the queue.

Claiming a Node

In case a node's private key is lost or compromised, the node can be claimed to recover locked funds, though this action removes the node from the registry. This mechanism aims to balance security concerns, ensuring that while nodes are safeguarded against unauthorized control, owners are incentivized to maintain strict security practices.

Ejection and Re-Entry

Nodes may be ejected from the registry if they become inactive but can re-enter the queue without additional fees, provided they re-establish activity. This process ensures that only actively participating nodes remain in the registry, supporting the network's integrity.

Simplified Management with Savitri

Savitri simplifies this entire process, from registration to management and security of nodes, ensuring that participants can easily maintain their nodes with minimal technical expertise. Through the use of a user-friendly wallet application, node owners can effortlessly manage their registrations and secure their contributions to the network's Proof of Unity, a novel approach replacing the traditional Proof of Participation to ensure a more unified and secure network operation.

4.2.2. Master Node

The masternode in the Savitri blockchain network plays a critical role by providing enhanced capabilities beyond those of standard nodes. Its primary functions include storing the entire blockchain history and creating what is referred to as a "monolith block." This special type of block is designed to simplify access to the network for new nodes, which only need to download the headers of the blocks to verify transactions. Initially, the functionality of masternodes to confirm transactions is being utilized within the DevNet, highlighting their importance in maintaining network efficiency and security.

Enhanced Capabilities: Masternodes are distinguished from standard nodes by their ability to perform additional tasks that are crucial for the network's functionality:

- **Creation of Monolith Blocks**: Masternodes generate a daily 'monolith block' that acts as a comprehensive ledger, listing all network participants, including nodes and Masternodes. This feature significantly enhances the functionality of Masternodes within the Savitri ecosystem.

Registration and Activation: Becoming a Masternode involves a registration process similar to that of standard nodes. Users must install the necessary software on their device and complete a registration transaction that involves sending a specified amount to the network to secure their Masternode status.

- **Activation:** After registration, the Masternode enters a queue until it is approved by the existing Masternode network. Once activated, Masternodes earn rewards based on their staked amount, duration of activity, and quality of performance. Rewards are distributed twice daily to those active for at least two weeks, with factors such as the token amount, hours processed, and a daily performance score influencing the reward size.

- **Monolith Block: A Network Overview:** The monolith block offers a verifiable snapshot of the network's structure and participants, which is crucial for maintaining transparency and accountability. Its generation ensures that the state of the network is accurately recorded, aiding in the review and verification processes.

- **Strategic Importance:** Masternodes play a pivotal role in the Savitri blockchain beyond just facilitating transactions and governance. They safeguard the network's integrity and historical record, which is essential for keeping the blockchain secure, transparent, and well-managed.

- **Removal of Masternodes:** Masternodes may be removed due to reasons such as inactivity, a self-request, or by other Masternodes for poor performance or malicious activity. Depending on the reason for removal, the staked amount may be returned or, in cases of malicious actions, distributed among all network participants as rewards.

In summary, Masternodes are integral to the functionality, security, and efficiency of the Savitri blockchain network, offering advanced features that support the overall stability and integrity of the digital ecosystem.

4.2.3. Mechanism of consensus : Proof of Unity (PoU)

Proof of Unity (PoU) represents an innovative concept in the blockchain world, aiming to optimize the transmission of data such as blocks and transactions through a peer-to-peer (P2P) system among nodes. This method stands out for its ability to facilitate timely communication between numerous nodes without the need for a central tracking entity. Instead, it uses a temporary ledger present in each node to track transactions automatically and randomly upon their reception.

Our goal with this method is to improve network reliability by encouraging the constant availability of nodes; we wanted to change the paradigm from a system in which nodes compete to a new system in which nodes cooperate, the scope is to create a distribute network where the responsibility of maintaining the blockchain’s history more broadly across various participants, and to fairly reward all contributing nodes. Furthermore, this strategy incentivizes the network’s registered nodes to self-organize into an efficient structure, reducing the path data needs to travel for widespread dissemination.This approach promotes a robust, equitable, and high-performing network, ensuring that participation is both incentivized and essential for the ecosystem's health and growth.

Transmission and Tracking Mechanism

In the Proof of Uunity (PoU) framework, whenever a node receives a transaction, it starts a communication procedure with other nodes, which are randomly chosen from its internal list. This process involves forwarding the transaction to a selected node and then awaiting a confirmation response. This confirmation is provided in the form of a receipt, which not only acknowledges that the transaction was received but also provides a score that indicates the success level of the transaction transmission. If the transaction is not approved, the receipt will serve as evidence of this rejection.

Commitments and Transmission Proofs

To ensure the system's integrity, nodes are required to regularly publish "commitments" documenting their transmission activity. This ensures that transmission records are pre-existing and cannot be fabricated on the spot. When a sample of past transmission activity is requested, the node must demonstrate that such records were included in the commitments already published on the blockchain, making it impossible to create them retroactively.

Transmission Receipts and Commitments

Every transmission within the Savitri network generates a digital receipt, signed by the recipient, uniquely identifying the participants and the moment of transmission. These receipts include a commitment in the form of a Merkle root, which in turn aggregates other receipts previously collected. The inclusion of these receipts in a block allows for an objective validation of the node's transmission activity, influencing its participation score.

Age Filter and Network Topology

The system imposes an age filter on receipts, determining their expiration after a certain number of blocks to emphasize recent network activity. This expiration time varies based on the number of active nodes, adjusting to the average time between block creations. Furthermore, the Savitri network periodically updates its topology to determine from which peers a node can receive and publish receipts, ensuring an equitable distribution of participation opportunities among all nodes.

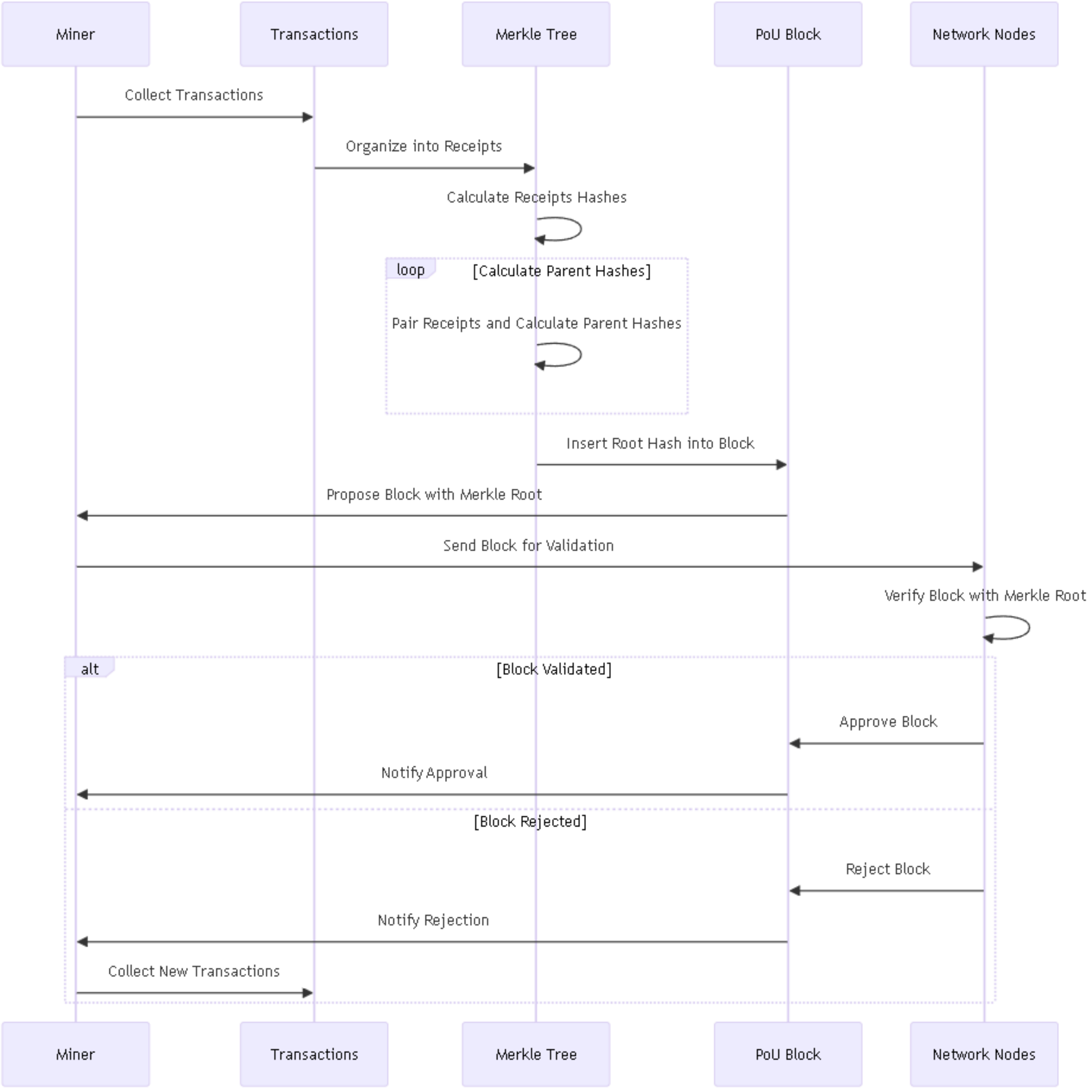


Figure 1 Sequence Merkle tree on Proof of Unity

4.2.3.1. The Receipt

Generating and collecting receipts

In the Savitri network, when one node sends data like a transaction or block to another, the receiver, upon verifying the data, generates a receipt to acknowledge the transfer. This process is done even if the data was previously received from a different source, provided it is valid.

Here's a simplified breakdown of how it works:

• Generating Receipts: After receiving and validating data, the receiving node creates a receipt. This receipt includes:

- **The sender's public key (who sent the data).**
- **The receiver's public key (its own).**
- **The type of data (block, transaction, etc.).**
- **The hash of the data.**

- **The current block height and hash from the receiver's perspective.**
- **The vote from different parameters**

Merkle Root Inclusion:

The receiver adds a Merkle root from its batch table to the receipt. While other nodes can't directly check this, it's crucial for the receiver to accurately include this for future validations of data transmissions.

Signing and Returning:

The receiver signs the receipt with its private key to certify its creation and sends it back to the sender. If a node consistently fails to return valid receipts, it risks being blacklisted.

Organizing Receipts:

When nodes send data, they collect receipts from those who receive them. These receipts are grouped into batches and each batch has a Merkle root representing the combined evidence of those transactions.

Batch limits:

There is a limit to the number of receipts that can be included in a single Merkle root, encouraging nodes to discard receipts that will not be useful for future proofs, such as those that do not align with peer filters.

Scoring: In Proof of Unity, scoring is the key aspect of block allocation, this together with the lottery will incentivise teamwork. The score is calculated according to several parameters some examples are:

- **Amount of coins blocked**
- **Amount of time the node has participated in the network**
- **Quality of data**
- **Timeliness of transmission**
- **Volume of data transmitted**
- **Contribution with votes for network choices**

Database storage and finalisation:

Receipts are stored in memory until the node is ready to finalise a batch. The node calculates the Merkle root for the batch and stores this information in the database, linking it to the block height in which it was created. Each receipt within the batch is also saved, labelled with the Merkle root of the batch and its sequence number in the batch.

This method allows nodes to keep track of their interactions within the network, preparing them to prove their active participation and support the network's Proof of Unity. This process ensures a transparent and accountable network, promoting efficiency and integrity in data propagation.

In the Savitri network, nodes share data as transactions or blocks and confirm these transmissions through receiving objects. This is how the process is simplified and made secure:

Receipt production:

When one node sends data to another, the recipient, after confirming its validity, generates a receipt. This receipt includes details such as the public keys of the sender and receiver, the data type, the hash of the data, the height of the reference block and the hash of that block. It also contains a Merkle root related to the data batch, which helps in subsequent validations.

Receipt Management:

The nodes collect these receipts in batches, calculating a Merkle root for each one to aid future verification processes. Receipts that are unlikely to be needed for future verification can be discarded, optimising storage and focusing on relevant data exchanges.

Remove old receipts:

Receipts expire after a certain period, depending on the block height indicated within them. Nodes periodically remove these expired receipts to maintain a lean and efficient database, ensuring that the system's memory footprint remains constant.

4.2.4. Block

In contrast to centralized systems where client requests are processed in a sequential manner, decentralized systems, like peer-to-peer networks, allow users to submit data through any node, leading to transactions being received in varying orders by different nodes.

Blockchain technology addresses the challenge of establishing a consistent order for all transactions disseminated across the network. Through a pseudo-random selection process, nodes are tasked with adding groups of transactions, known as blocks, to the collective transaction history of the network. Each block, containing transactions and additional data, is securely linked to the preceding block using cryptographic hashes in its metadata, forming a chain — hence the term "blockchain." This linkage means altering any block's data would necessitate the reconstruction of all following blocks, ensuring the integrity of the transaction history.

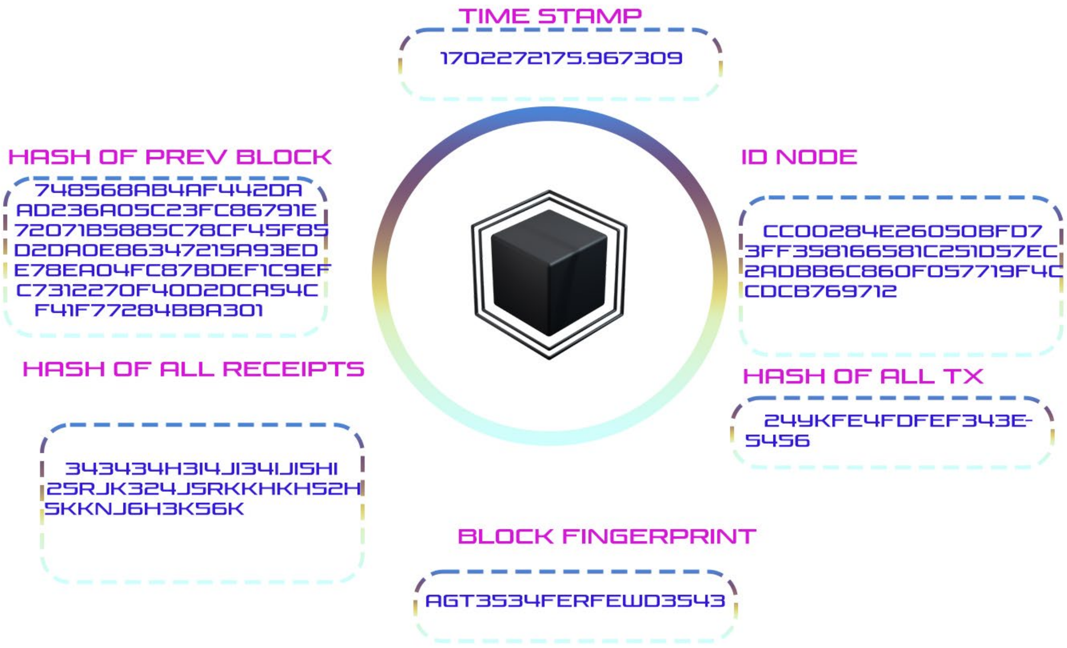


Figure 2Block's Components

Structure of a block

Unlike centralized systems where tasks are done one by one, decentralized systems, such as peer-to-peer networks, let users send information through any of the system's parts. This means that transactions can arrive in different orders at different places.

Blockchain technology solves the problem of how to put all these transactions in a specific order across the whole network. It does this by selecting nodes in a sort of random way to group transactions into blocks. These blocks, which hold transactions and some extra information, are then linked together in order. Each block is connected to the one before it by special codes called cryptographic hashes, creating a chain — that's why it's called "blockchain." If you wanted to change information in one block, you'd have to change all the blocks that come after it, which helps keep all the transaction records safe and unchanged.

Block creation and protection from modification.

In the context of the Savitri blockchain, the process of block creation and its protection from undue modification are key aspects in ensuring the security and integrity of the network. The creation of a block in a blockchain is an operation that, if not properly controlled, could leave room for manipulation by block creators, thus compromising the entire system.

Hash Function and Entropy

The hash function plays a crucial role in block creation, producing a unique hash value from a set of input data. This function is designed to generate output that appears as uniformly distributed random numbers, independent of the input data. Although a block hash may seem like a good source of entropy, i.e. randomness, exploiting it in such a way can be dangerous. An attacker, having the possibility of altering certain elements of the block such as transaction order, timestamp or other data, could repeatedly attempt to modify the block until a 'favourable' hash is obtained that would allow him to manipulate the blockchain.

4.2.5. Monolith Block

The Savitri blockchain incorporates a unique feature known as monolith blocks, designed to streamline the process of accessing the blockchain's history. These special blocks are created once daily and are linked sequentially to the previous monolith block, forming a chain that allows nodes to leapfrog over regular blocks from the genesis block to the current moment. This system facilitates rapid access to any point in the blockchain's history, making it a lightweight and efficient way to maintain an updated ledger of node registry changes.

Monolith blocks are generated on average once a day and primarily record significant updates to the node registry, such as the addition or departure of nodes, along with other metadata. Importantly, they do not contain transaction data, resulting in a very light set of blocks for download. This design ensures that a node needs to download only a minimal amount of data for each day of the blockchain's existence, providing an always up-to-date list of nodes in the registry at any historical moment. Consequently, this allows nodes to verify if the next monolith block was created by a legitimate node and make informed decisions in the event of a fork.

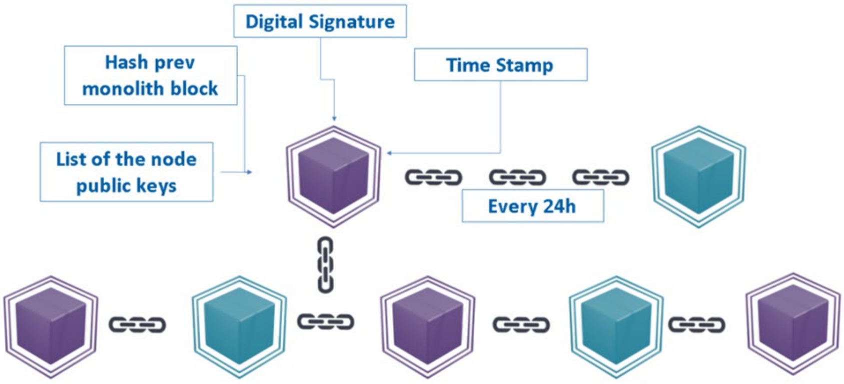


Figure 3 Monolith Block

Bootstrapping a New Node

The initial step for a new node involves downloading all monolith blocks from the genesis block, choosing the set of blocks with the highest cumulative difficulty in the event of a fork, until it reaches the latest available monolith block. The node then uses the hash of the most recent blockchain snapshot found in a spine block to identify and download a snapshot of the blockchain from network peers. This process enables a new node to quickly update itself with the blockchain's current state within minutes, significantly reducing the time and resources needed to become a fully participating member of the network.

This innovative approach to blockchain architecture not only enhances the efficiency of accessing historical data but also simplifies the process for new nodes to join and synchronize with the network, ensuring the Savitri network remains robust, secure, and accessible.

4.2.6. Introduction of the Block fingerprint

The calculation of the block fingerprint is done through a formula that guarantees its unpredictability and uniqueness:

new_block_seedH=hash(creator_signatureH(hash(block_fingeprintH-1+block_metadataH)))

Where:

– **new_block_fingerprintH** is the seed of the current block we are calculating.

– **creator_signatureH** is the digital signature of the creator of the current block, applied to the combination of the hash of the previous block's seed and the current block's metadata.

– **block_fingerprintH-1** is the seed of the previous block.

– **block_metadataH** includes additional data of the current block, such as the block number, timestamp, and hash of the current block's header, thus increasing the entropy of the seed.

Process Description

- Data Combination: Instead of directly signing the seed hash of the previous block, the block creator combines this hash with the metadata of the current block. This step introduces an additional layer of unique data that makes the seed more unpredictabApplication of the
- Digital Signature: The block creator applies its digital signature to the combination of the seed hash of the previous block and the metadata of the current block, ensuring that the seed cannot be generated without the creator's private key.
- Calculation of the Final Hash: Finally, the hash of the signature result provides the new seed of the block. This step ensures that the final seed is a fixed hash value

that is independent of the length of the signature, uniformly distributed and difficult to predict without knowing the signature and the initial data.

Use of the Digital Signature Algorithm Ed25519

Savitri adopts the **Ed25519** digital signature algorithm for creating block seeds, known for its efficiency and security. A key advantage of Ed25519 is that there is only one possible signature per message and per private key. This eliminates the possibility for the block creator to choose between several potential signatures, forcing him to accept the block seed generated by the protocol without the possibility of alteration.

Block creation:

Within the context of “node registration,” where the complete set of potential block creators is known, Savitri employs a method that, following each block, pseudo-randomly generates a priority-ordered list of nodes tasked with creating the next block. If a node fails to produce a block when it’s their turn (due to being offline, network issues, or voluntary omission), its participation score is decreased. In such cases, the network waits for a block from the next node in the randomly ordered list.

Alternative algorithm for block creator selection:

To make the block creator selection process more resilient and distributed, an algorithm based on “weighted voting” and “commitment” concepts could be considered. In this scenario, every node in the network can participate in the selection of the block creator through a voting mechanism that accounts for not only the presence of the node but also its reliability and contribution to the network.

Algorithm Definition:

Commitment Weight Calculation (CWC): Each node commits a certain amount of resources (e.g., computing power, storage, bandwidth) for a specified period. This commitment is measurable and is used to calculate a “Commitment Weight” for each node.

NodeWeight = f(resourceCommitment)

Where f is a function that maps resource commitment into a numerical weight.

Weighted Voting: When it’s time to select the block creator, every node participates in a voting process. The vote of each node is weighted based on its Commitment Weight, with nodes that have committed more resources having more weight in the decision.

Block Creator Selection:

- A unique hash value for the last confirmed block is calculated, serving as the seed for the pseudo-random selection.
- Using the seed, the block creator is selected based on the weighted distribution of votes.

blockCreator = pseudoRandomSelection(hash(lastBlock), weightedDistribution)

Failure to Create Handling: If the selected node fails to create the block within a predetermined time, its Commitment Weight is reduced, affecting its future selection capability. The selection process is then repeated excluding the failed node.

This algorithm aims to incentivize nodes to maintain a high level of commitment and reliability, as their ability to influence the block creator selection and earn rewards is directly proportional to their commitment to the network.

5. Transactions

Every action executed on the Savitri blockchain by a user is encoded in a transaction that specifies the action the nodes should take, the action parameters and and data payload, and has all this digitally signed using the sender's private key. A transaction may be as simple as transferring tokens from one account to another but could have unlimited complexity, so long as its core application logic satisfies the properties that both the transaction validation and its execution are purely deterministic operations which only read from, and write to, the portion of each node's database managed by the consensus algorithm.

When a transaction is first received from a peer or from a wallet software, the node will first confirm that the transaction is legal. This includes validating that the transaction is closed by a valid digital signature for its sending account address and that the parameters of the transaction are valid according to the transaction type's rules and the current state of the database (such as having enough balance to send funds).

If the transaction received is valid, the node will propagate the transaction by transmitting it to other connected peers, as well as store the transaction in its local mempool. In this way, valid transactions are echoed across the peer-to-peer network until they are retained in the mempool of the majority of nodes. Upon receiving a valid transaction, each node will also return a special object we call a receipt to the sender. Receipts are used in the Proof of Unity algorithm described below.

5.1. Transaction Application

When a node receives and validates a new block (described in the section on "blocks" below), it will contain an ordered list of zero or more transactions, which the node will then apply in sequence.

For a node, applying a transaction means executing the rules associated with the transaction's type to update its local database from an old state to a new state. In the simplest example, this can mean deducting the balance from one account and adding it to another.

5.1.1. Transactions Attachments

In future versions of Savitri, transactions will be allowed to specify large attachments to be stored in a distributed file system by the network. While the transaction itself must be propagated to all nodes, the attachment may only need to be propagated to a few nodes responsible for storing the file for others to download. More details on this are given in the section below on File Distribution.

5.1.2. Transactions Escrow

When two parties must swap goods online, it is often useful to have a trusted third party keep the goods in escrow, such that the swap is only executed when both parties have committed their assets. Traditionally, this trusted third party holds both of the assets, and if they are not in fact so trustworthy, they may abscond with both. Therefore, it is useful to have a system in which the trusted third party may only approve or reject the transfers between parties, but in no case becomes the owner of the assets.

To facilitate this use case, Savitri users may optionally include in the transaction the account address of an approver, which may either accept or reject the application of the transaction. Transactions which require approval are kept in an "escrowed" state by the blockchain, such that the funds or other assets they confer ownership of cannot be used by either the sender or the receiver until the explicit approval or rejection is completed, or the timeout returns control of the assets to the sender.

The transaction may also specify:

- **a custom timeout:** the number of blocks until, or the date/time at which, the transaction is automatically rejected (by default 1 day). The maximum timeout is 1 month;

- **commission:** an amount of tokens which will be paid to the approver if he accepts/rejects the transaction before the timeout, by default, the cost of a transaction;

- **instructions for the approver:** in binary or a JSON format if the approver is an application on a server, or in a human language if the approver is a regular user of Savitri;

- **the behavior for when the transaction timeout**: automatically approve or reject.

In the case that the timeout is reached before the approver sends an approval or rejection, the transaction is automatically approved or rejected and the commission is returned to the sender.

In order to approve or reject an escrowed transaction, the specified approver must broadcast an approval transaction, referencing the hash of the pending escrowed transaction and specifying whether he approves or rejects it. While the approval transaction can be submitted automatically by centralized services, when a user needs to manually submit the approval for a transaction, the technical complexities are hidden by the wallet UI.

One use case of such an escrow mechanism would be to configure a centralized server which manages an approver account and which is programmed to automatically approve transactions only when certain conditions have been met. For example, an escrowed transaction may specify that it should only be approved once 10 Ethereum have been transferred to a particular ETH account and set the approver to be a server which will monitor the Ethereum network to determine whether to release the funds.

Alternatively, any account may be configured to require explicit approval to accept any transaction addressed to it. In this case, if an approver account is not specified, the recipient account automatically becomes the approver. The rest of the mechanics defined above apply in exactly the same way, with the receiver of the transaction functioning as the approver.

To achieve the current normal behavior of blockchain transactions, any transaction which does not specify an approver account, and for which the receiver is not configured to require approval to accept transactions, is applied immediately upon its acceptance in a block.

The owner of an account may at any time enable or disable this mandatory approval behavior on the account by broadcasting the desired account property setting with a required approval transaction and specifying whether mandatory approval is enabled (default is “no”).

5.1.3. Fee transaction

Transaction fees in blockchain and cryptocurrencies are costs paid to validators for processing transactions. Usually these fees vary based on network congestion, transaction complexity, and confirmation speed. Every transaction in Savitri requires the payment of a fee in SAVI coin. This practice serves to cover the costs of executing transactions on the network and to protect the blockchain from potential spam attacks, making it economically impractical to overload the network with an excessive volume of transactions.

5.1.4. Distribution of Rewards

The fees collected, along with the new Savi coins issued for each block, are shared among the network’s registered nodes. This system not only rewards nodes for their network contributions but also encourages block creators to include as many transactions as possible to maximize the overall reward.

Each Masternode receives a reward from the network for every block it stores. This allocation is made randomly, but Masternodes with higher scores and longer network activity times are given a greater chance of receiving rewards. This method motivates nodes to improve both the quality and quantity of their work to increase their chances of earning rewards from the network.

5.1.5. Calculating the Minimum Fee

The minimum fee for each transaction depends on the type of transaction being processed. To determine this fee, a specific formula is used that considers both the transaction type and a scaling constant. This scaling constant is adjustable and may be periodically updated to mirror the current state of the network, ensuring that fees remain fair and reflect network demand.

Transactions that pay a fee higher than the minimum requirement are often processed more quickly. This is particularly true during times of high network congestion, where the incentive for faster processing increases with higher fees. Essentially, by offering to pay more than the minimum fee, users can prioritize their transactions, allowing them to be confirmed more swiftly in busy periods.

This fee structure serves multiple purposes: it helps regulate the flow of transactions through the network, preventing spam and ensuring that resources are allocated efficiently. Moreover, it provides a mechanism for users to expedite their transactions when needed, offering flexibility and improved user experience in times of high demand.

Here’s our algotithm for calculate the base fee:

min_fee(TxA) = base_fee(TxTypeA) + congestion_fee(NetworkStatus) + urgency_fee(TxUrgency)

Where:

- **base_fee(TxTypeA):** A base fee determined by the type of transaction A.
- **congestion_fee(NetworkStatus):** An additional fee that varies with the current level of network congestion. This is calculated as a percentage of the base fee or a fixed amount that increases as the network becomes more congested.
- **urgency_fee(TxUrgency):** An optional fee that users can add to their transaction to prioritize it over others. This is a fixed fee or scale with the level of prioritization requested.

5.2. Introduction to Transaction Fee Calibration

In the realm of decentralized systems, determining transaction fees poses a significant challenge. On one end, a centralized approach where a trusted third party sets the fee based on new information against a pre-agreed public key of the entire blockchain could be considered. However, this method contradicts the principles of decentralized systems, as it can be manipulated by a single actor beyond accountability. On the opposite end, nodes independently sourcing public data, such as the token’s value from exchanges to align transaction fees with a stable currency value, risks causing forks due to inconsistency in external data when queried by different nodes at various times.

5.2.1. The Challenge of External Consensus

Achieving a secure consensus on external data, such as a token’s value relative to other currencies, is inherently complex within a blockchain framework. Automatic resolution of such consensus cannot be realized due to the decentralized nature and the variability of external data sources. This presents a dilemma for maintaining transaction fees consistent with a stable currency value amidst the fluctuating value of the blockchain’s principal token.

A Node-Operated Voting System for Fee Scale Adjustment

To address this issue, we propose a system where registered node operators on the network can regularly vote on the appropriate multiplier, which we term the “fee scale,” for minimum transaction fees. This system aims to maintain the transaction fee value constant relative to a stable currency, even as the main token’s value varies. Entrusting such a critical network parameter to node operators is potentially risky, and a more comprehensive discussion of this risk is intended for future work. However, we favor this approach over the inherent risks associated with imposing a static minimum fee for the reasons outlined above.

5.2.2. Balancing Node Operator Incentives

We believe the risk associated with the node-operated voting system can be mitigated by balancing two opposing incentives that should limit each other. On a small scale, a node operator desires to maximize transaction fees collected in each block by pushing the network fee scale higher. However, on a larger scale, high network fees may deter users from conducting transactions on the blockchain, affecting usability and potentially reflecting on the token’s price. This, in turn, influences the real value a node operator can earn, incentivizing them to lower the network fee scale.

5.2.3. Implementing the Fee Scale Adjustment Mechanism

The fee scale adjustment based on voting is realized through three mechanisms: node operators commit to their votes, reveal votes they previously committed, and employ a calculation of the mean to determine the new network fee scale. This process ensures a democratic and balanced approach to adjusting transaction fees, aligning with the decentralized ethos of blockchain systems while addressing the practical need for stable transaction costs.

5.2.4. Voting Phases for Fee Scale Adjustment

The process of adjusting the fee scale within a decentralized network involves a structured voting mechanism. This mechanism is divided into two main phases: the Commitment Phase and the Revelation Phase. Each phase plays a crucial role in ensuring the integrity and security of the voting process.

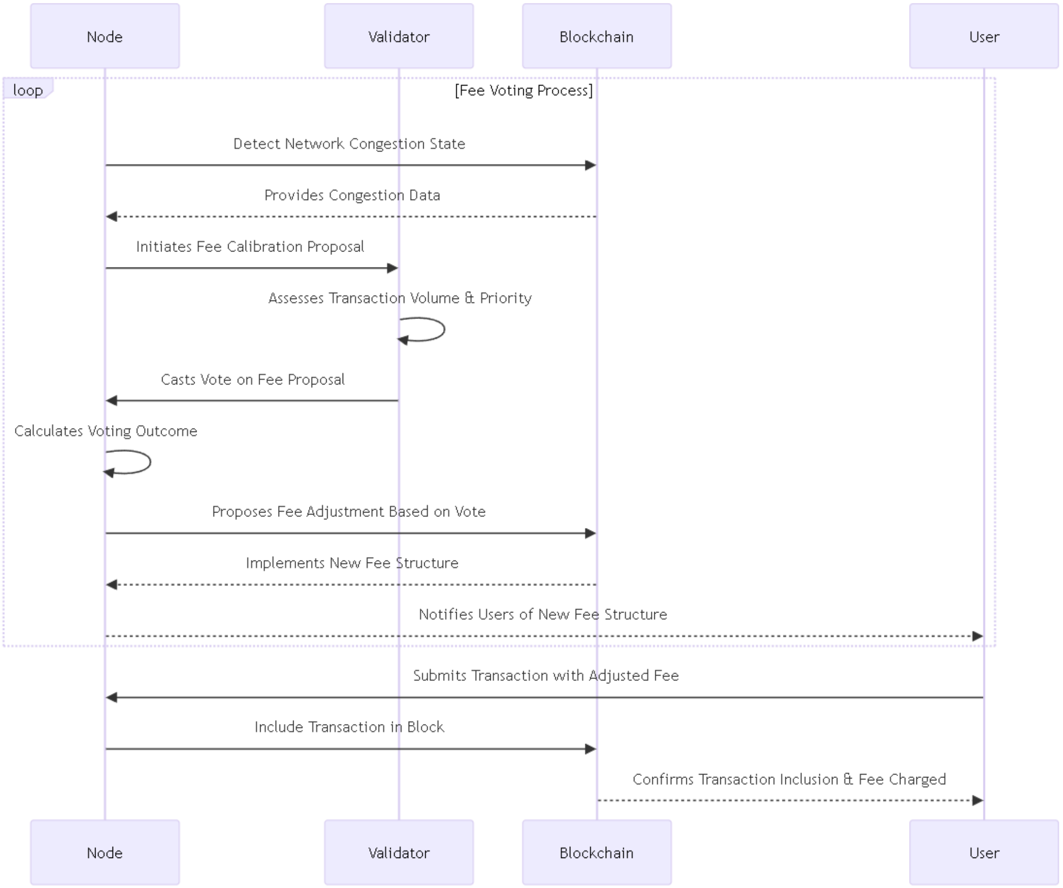
5.2.5. Commitment Phase

During the Commitment Phase, node operators submit their votes on how the network’s fee scale should be adjusted, if at all. This is done through a commitment vote transaction, which creates a fee vote object. This object contains a recent block hash, the corresponding block height, the user’s vote on the new network fee scale, and the digital signature of the account over these pieces of information. Including additional details in the fee vote object (such as the block hash and account signature) is crucial for making the vote object’s hash resistant to attacks where an attacker might guess the fee scale a user is voting for.

5.2.6. Revelation Phase

Following the Commitment Phase is the Revelation Phase, where votes are recorded on the blockchain and tallied. In this phase, registered node operators are allowed to send a revelation vote transaction. This transaction includes the full content of the fee vote object previously committed by the user. The transaction must be signed and sent to the network, and for nodes to accept it as a valid transaction, the hash of the submitted fee vote object must match the commitment hash previously sent by the user during the Commitment Phase.

This two-phase voting process ensures that votes are cast securely and anonymously in the initial phase, with integrity verified in the subsequent phase. It’s designed to prevent manipulation and ensure that each vote genuinely reflects the operator’s intentions regarding the network fee scale adjustments.


Node
Validator
Blockchain
User
loop
[Fee Voting Process]
Detect Network Congestion State
Provides Congestion Data
Initiates Fee Calibration Proposal
Assesses Transaction Volume & Priority
Casts Vote on Fee Proposal
Calculates Voting Outcome
Proposes Fee Adjustment Based on Vote
Implements New Fee Structure
Notifies Users of New Fee Structure
Submits Transaction with Adjusted Fee
Include Transaction in Block
Confirms Transaction Inclusion & Fee Charged
Node
Validator
Blockchain
User

5.2.7. Reward Schedule

The Savitri network is proud to introduce a cutting-edge approach to reward distribution, meticulously designed to transcend the limitations of traditional block reward halving mechanisms. Our strategy ensures a smooth and predictable decrease in rewards over a 50-year timeline, fostering equitable distribution among all network participants. This premier solution is tailored to maintain network health and encourage continuous engagement.

5.2.8. Core Principles of the Reward Mechanism

Our reward distribution model is elegantly simple yet profoundly effective, utilizing a linearly decreasing reward system over five decades. This method guarantees a steady reduction in rewards, enabling participants to forecast their potential earnings with high accuracy, thus ensuring stability and predictability in the network's economy.

5.2.9. Linear Reward Distribution Formula

The heart of our reward mechanism is encapsulated in the following formula:

RewardH=InitialReward−((InitialReward/TotalBlocksIn50Years)×H)

This formula demonstrates our commitment to a transparent and fair approach, where:

- InitialReward represents the reward for the initial block.
- TotalBlocksIn50Years estimates the total blocks produced over the span of 50 years.
- H indicates the height of the current block.

5.2.10. Innovative Selection of Reward Recipients

To democratize the reward process, we've devised a system that judiciously balances each node's contribution to the network with an element of randomness. This dual-factor selection process ensures that every node, regardless of its tenure, has a fair opportunity to be rewarded, thus promoting network growth and vitality.

The Selection Formula

We employ a distinctive formula to calculate each node's score for reward eligibility:

ScoreN=RandomFactor+[1/(1+ActivityLevelN)]

Nodes with the lowest scores are prioritized for rewards, ensuring a fair and inclusive system that values contribution and participation equally.

Implementation and Impact

- The linear reward calculation ensures the minting of tokens is aligned with the target supply, avoiding excess and promoting long-term sustainability.
- Our selection mechanism for reward recipients is crafted to encourage consistent participation while also drawing new nodes to the network, striking a perfect balance between rewarding loyalty and fostering growth.

5.3. Multi Sign on Savitri

When managing valuable digital assets, it's risky to rely on a single individual holding the account key, as it might be lost or compromised. To enhance security, we use multi-signature (multisig) features. This allows the creation of accounts that need a certain number of signatures from a group to authorize transactions. For instance, in a group of 10 people, any 4 can sign to approve a transaction.

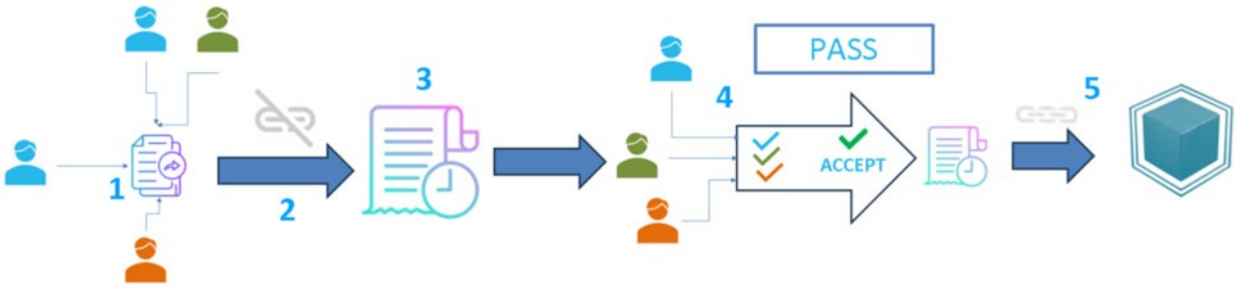


Figure 4 Multi-sign transaction

5.3.1. Multisig Addresses

These are special addresses created from a hash of details, known as multisig info, defining who can sign transactions. This setup keeps signer identities private until needed.

5.3.2. Multisig Info Object

MinSigs: Minimum signatures required to execute a transaction.

Nonce ("Access Code"): A unique number to differentiate multisig addresses with the same participants.

Addresses: A list of account addresses authorized to sign, sorted alphabetically. These can also be multisig addresses, allowing for a hierarchy.

5.3.3. Multisig Transaction Type

Savitri handles multisig through a single transaction type, accommodating both on-chain and off-chain behaviors without revealing signer identities prematurely. The transaction includes optional components: multisig info, the transaction details (or its hash), and signatures from co-signers.

Nodes manage multisig operations using three tables: multisig info, pending transactions, and pending signatures. Transactions are executed once all necessary components are present and valid, maintaining anonymity until execution.

5.3.3.1. Use Cases

- **Off-Chain Multisig:** Similar to traditional multisig, where a transaction prepared off-chain is broadcast for immediate network validation.
- **On-Chain Multisig**: Allows for sequential on-chain signature collection, useful when not all signers can coordinate off-chain.
- **Anonymizing Multisig** Addresses: Keeps asset controllers anonymous until action is needed, with the option for many to submit signatures for plausible deniability.
- **Concealing Pending Transactions:** Protects transaction details until enough support is gathered, enhancing privacy.
- **Hierarchical Multisig:** Supports complex organizational decision-making structures, allowing for multiple layers of multisig requirements.

This simplified approach ensures asset security and flexibility in transaction authorization, catering to various operational needs while preserving privacy and integrity.

5.4. Liquid Payment

In the modern era of web services, the necessity for automated payment systems for salaries or allowances is increasingly becoming a critical requirement. Traditional blockchain transactions have a significant limitation: each transaction must be manually initiated and confirmed via a digital signature. This manual approach is perceived by our foundation as a constraint that diminishes the blockchain's application potential. To address this issue, we are pioneering a technology that facilitates automatic payments through the use of smart contracts.

5.4.1. Revolutionizing Payments with Smart Contracts

Our innovative approach leverages smart contracts to automate the payment process without locking funds within the wallet. This technology allows for the configuration of automatic payment orders contingent upon the availability of sufficient funds in the user's wallet. Unlike traditional methods, this system provides flexibility and control to the user, who can halt payments at any moment. Upon the suspension of a payment, the smart contract will automatically notify the recipient about the payment block.

5.4.2. Ensuring Liquidity and Operational Continuity

One of the paramount features of our technology is its ability to seamlessly handle liquidity issues. Should the wallet lack the necessary funds for the automated payment, the smart contract is designed to automatically terminate the payment order. This feature ensures operational continuity and financial stability without requiring manual intervention, thereby streamlining the payment process.

5.4.3. Integration with External Applications

Furthermore, our solution is designed to complement, not overhaul, the existing operational models of external applications. By merely adapting to communicate with smart contracts, external applications can easily integrate with our automated payment system. This compatibility allows for a smooth transition and adoption of blockchain technology for automated transactions, eliminating the need for significant changes to their current operational procedures.

6. IoT integration

The Savitri Network project emphasizes the seamless integration of IoT (Internet of Things) devices into the network, allowing these devices to directly transmit data to the network without intermediaries. Addressing this challenge involves two potential solutions: treating each IoT device as a distinct network node capable of creating digitally signed transactions, or alternatively, establishing a direct connection with the blockchain.

6.1. Solution 1: IoT Devices as Network Nodes

The first solution involves registering each IoT device as a separate node within the network. By doing so, IoT devices are empowered to actively participate in network operations, generating and dispatching digitally signed transactions akin to any other node. This approach leverages the network's existing security protocols to authenticate and log data sent from IoT devices, ensuring secure and verifiable communication.

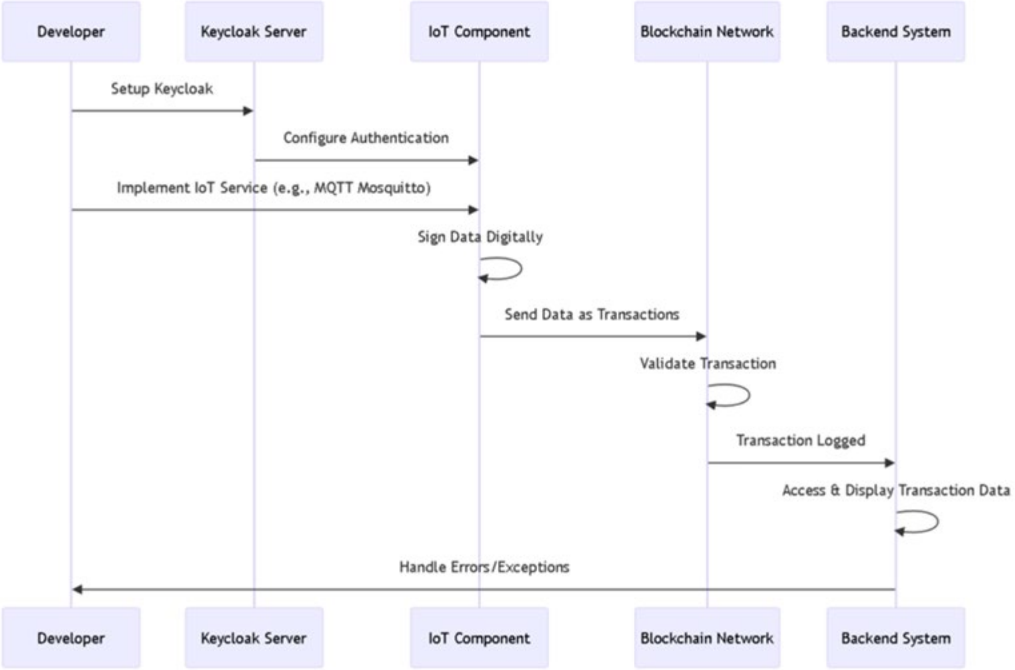


Figure 5 Scheme 1st Solution

1. ***Creating a Digital Authentication Server:*** Utilize an open-source service such as Keycloak to establish a digital authentication server. This server will manage access and identity for users and devices interacting with the blockchain.

Integration with Keycloak

2. ***Keycloak*** Integration: a. Configure Keycloak to interface with the data submission component to the blockchain. This may involve leveraging authentication and authorization protocols like OAuth 2.0 to facilitate secure communication between Keycloak and the blockchain data submission component.

Implementing a Custom IoT Component or Service

3. ***Custom Component or IoT Service Implementation:*** Implement a customized component or an IoT service (e.g., MQTT Mosquitto) that facilitates the interaction between IoT devices and the blockchain network.

IoT Node Functionality

4. ***Functionality of the IoT-Connected Node:*** Ensure that the node connected to the IoT service is capable of: a. Digitally signing data to maintain integrity. b. Associating data with a wallet, a public key, and the address of the smart contract representing its identity on the blockchain. c. Sending data to the blockchain through transactions. d. Upon submission, the blockchain recognizes and validates the transaction.

Monitoring and Management

5. ***Monitoring and Management:*** a. The backend connected to the network accesses transactions via the master-node and identifies the device that initiated the transaction. If the device is linked to a smart contract, the results will be displayed on the corresponding page. b. Manage any errors or exceptional situations that may arise during the data submission process to the blockchain.

This streamlined process provides a clear and straightforward guide for developers and blockchain experts looking to integrate IoT devices with blockchain technology. By leveraging Keycloak for authentication and implementing a custom IoT component, this approach ensures secure and efficient data handling and submission to the blockchain.

6.2. Solution 2: Direct Blockchain Connection

Alternatively, the second solution proposes a direct connection between IoT devices and the blockchain. This method allows for direct interactions between IoT devices and the blockchain, bypassing the need for these devices to operate as traditional network nodes. This simplification aids in the integration process by eliminating the requirement for individual device registration as nodes, while still providing a secure and efficient pathway for data transmission to the blockchain.

Both strategies are designed to facilitate the integration of IoT devices into the Savitri Network, ensuring the secure, direct, and efficient transfer of data to the blockchain. Developers and blockchain experts involved in the Savitri Network can select the most appropriate solution based on the specific requirements and constraints of their IoT devices and the overarching network architecture.

The integration of IoT devices into the Savitri Network involves a series of steps designed to ensure secure and efficient data transmission from the devices to the blockchain. Below is the streamlined process:

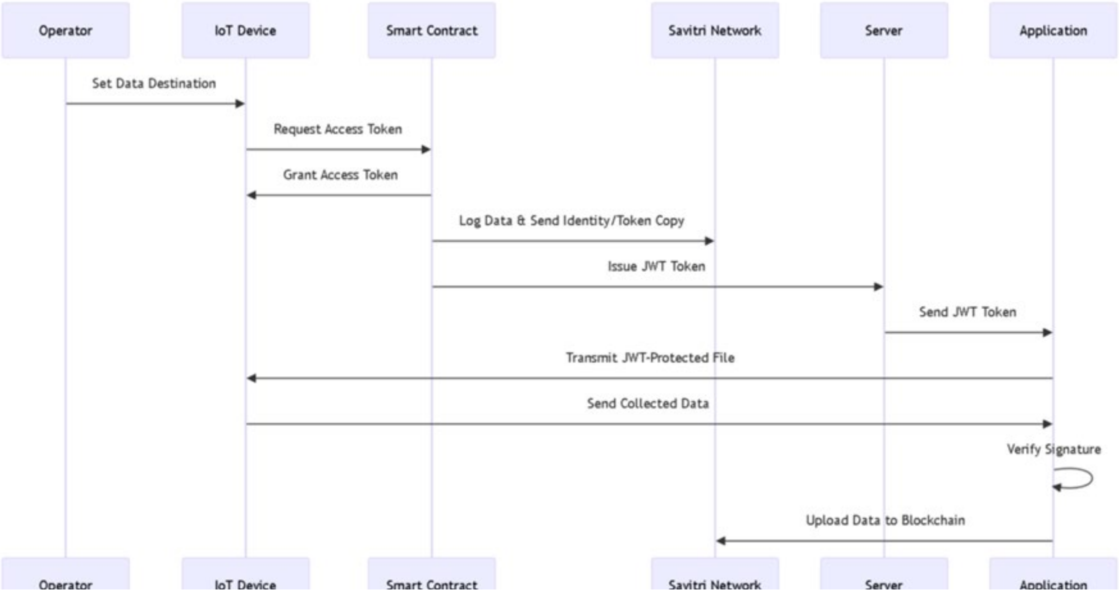


Figure 6 Scheme 2nd solution

1. ***Setting the Data Destination:*** The operator specifies the destination for the data within the IoT system, determining where the data collected by the IoT device should be directed.
2. ***Access Token Acquisition:*** The IoT device requests and obtains an access token from a smart contract deployed on the blockchain. This token is crucial for authorizing the device to interact with the network.
3. ***Data Logging and Identity Verification:*** Upon receiving the access token, the smart contract logs the data and sends a copy of the identity and token back to the Savitri Network. This step is vital for verifying the device's identity and ensuring that the data transmission is authorized.
4. ***JWT Token Dispatch:*** After the device is successfully registered, the smart contract issues a JSON Web Token (JWT) to the server. This token is used for the secure dispatch of files between the network and the IoT device.
5. ***Token Reception and File Transmission:*** The application associated with the IoT device receives the JWT token and uses it to transmit the JWT-protected file to the IoT device. This ensures that the file transmission is secure and authenticated.
6. ***Data Transmission to Application:*** The IoT device then sends the collected data to the application. This step is crucial for aggregating and processing the data before it's uploaded to the blockchain.
7. ***Signature Confirmation and Data Upload:*** Finally, the application verifies the digital signature of the data to confirm its integrity and authenticity. Upon successful verification, the data is uploaded to the blockchain.

This process ensures that data from IoT devices is securely integrated into the Savitri Network, leveraging smart contracts for authentication and using JWT for secure data transmission. This method not only enhances the security of the data transfer but also streamlines the process for a seamless integration of IoT devices into the blockchain ecosystem.

7. *Savitri Tokenomics: An In-Depth Look at SAVI*

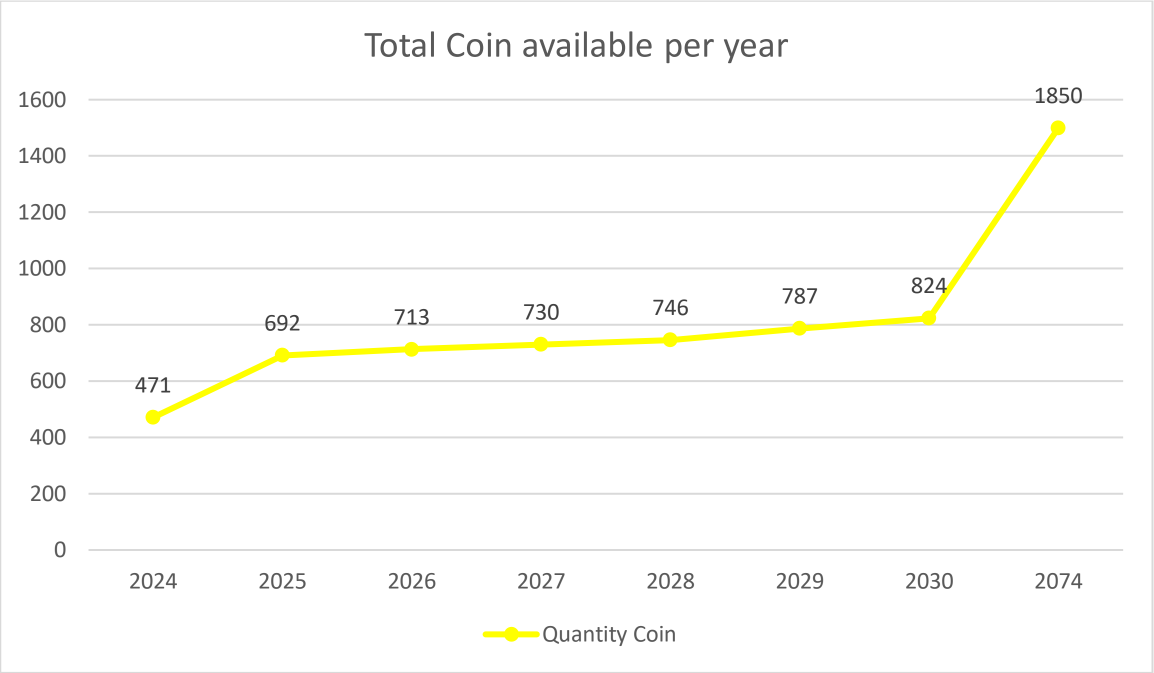
Within the cutting-edge ecosystem of Savitri, the SAVI coin stands as a central element designed to power user engagement, incentivize innovation, and support sustainable growth. With a total supply of 2 billion coins, SAVI is not just a currency but a means through which Savitri aims to revolutionize user interaction with blockchain technology.

7.1. Detailed Distribution of SAVI

- *Rewards for User Participation (52%):* Aimed at rewarding those who actively contribute to maintaining and growing the network, 52% of SAVI coins are set to be gradually released as rewards to users over 50 years. This long-term reward mechanism is designed to encourage consistent and meaningful participation, ensuring the network's vitality and security over time.
- *Company Reserves (10%):* This portion is strategic to ensure financial stability and the ability of Savitri to support ongoing development, future innovations, and necessary infrastructure expansions.
- *Team (5%):* Acknowledging the effort and expertise of the team behind Savitri, 5% is allocated as an incentive for those who have tirelessly worked to bring the project to fruition and will continue to push its boundaries.
- *Business Development and Partnerships (5%):* Allocating 5% to this category underscores the importance of strategic collaborations and the development of new business opportunities to expand and strengthen the Savitri ecosystem.

- *Marketing (5%):* Essential for growth and expansion, this fund will support targeted marketing initiatives to increase Savitri's visibility, attract new users, and solidify its position in the cryptocurrency market.
- *Liquidity and Listing (7.5%):* Crucial for the visibility and accessibility of SAVI, this allocation supports the creation of solid market liquidity and facilitates listing on major cryptocurrency exchanges, improving access for investors.
- *Coin Sale (15%):* The initial sale of SAVI is intended to generate capital to support the early stages of network development and expansion, simultaneously offering investors the opportunity to directly support the Savitri project and participate in its growth potential.

DESCRIPTION	QUANTITY IN %	QUANTITY IN COIN
Ecosystem	52%	1,050,000,000
Company reserve	10%	200,000,000
Team	5%	100,000,000
BD and partnership	5%	100,000,000
Marketing	5%	100,000,000
Liquidity and listing	7,5%	150,000,000
Seed Sale	5%	100,000,000
Private sale 1	5%	100,000,000
Private sale 2	2,5%	50,000,000
Public sale	2,5%	50,000,000
Total coins	100%	2,000,000,000



7.2. Enhancing Token Value and Supply Control in Savitri: The Strategic Burning Mechanism

In the Savitri blockchain, the consensus mechanism incorporates a unique feature to enhance the token's value and regulate the currency's supply within the network. For every transaction fee collected, a portion ranging from 0.1% to 0.5%, up to a maximum of 1%, is systematically "burned" or removed from circulation. This burning process is strategically designed to incrementally increase demand for the token while simultaneously reducing its overall supply.

This deliberate reduction of the available currency supply through the burning of transaction fees serves multiple purposes. Firstly, it acts as an anti-inflationary measure, ensuring that the value of the token remains stable or potentially increases over time by curtailing the total supply. Secondly, it aligns the interests of the token holders and the network's overall health, as reducing the supply tends to incentivize holding, contributing to a more robust and stable economic ecosystem.

The decision to burn a specific percentage of transaction fees is carefully calibrated within the Savitri consensus algorithm, balancing the need to remove tokens from circulation with the necessity to maintain an efficient and user-friendly transaction fee structure. This approach reflects Savitri's commitment to creating a sustainable and growth-oriented economic model that benefits all participants in the network.

By integrating this token burning mechanism directly into the consensus process, Savitri ensures that every transaction contributes to the long-term viability and value appreciation of the network's currency. This innovative feature underscores Savitri's dedication to pioneering economic models that promote scarcity, value preservation, and the long-term success of the blockchain ecosystem.aces entotatur? Ati dolupiet pa dessi te cone es quo od molut dolorectur, cus sum idestiumque rem quide nos sit ut most quiduciis persper sperio (Table 1). Et rem quisquiatur sam eos a voluptam voluptatis ius aut veleste voluptatus sitint mo eossi core con experitem eictiorior aut optaquam, soluptatiost exerferum et liquisto doluptatium vent et et ut volenec turiatis et facerum (Figure 2) et undae sit molora et volorem lior aut optaquam, m faccuptatest aut aut aboreped quate anihiliam qui ullabor sa vendit, nem sendissi officid ut haruptatur, sit a qui cus.

8. *Market Strategy: Positioning Savitri for Global Success*

Savitri's market strategy is crafted to secure a prominent place in the blockchain sector. It's not just about launching a new technology but creating a movement that brings blockchain into mainstream use. Here's how Savitri plans to execute this ambitious strategy:

8.1. Educational Outreach and Platform Knowledge

Understanding that blockchain's complexity often deters widespread adoption, Savitri will embark on an extensive educational campaign. This includes:

- *Online Learning Platforms:* Developing a comprehensive suite of online courses, webinars, and tutorials tailored to various expertise levels, from blockchain beginners to advanced developers.

- *Workshops and Hackathons:* Organizing hands-on workshops and hackathons globally to foster innovation on the Savitri platform and encourage practical learning and experimentation.

- *Partnerships with Educational Institutions:* Collaborating with universities and tech schools to integrate blockchain studies into their curriculum, emphasizing the innovative solutions Savitri brings to real-world problems.

8.2. Strategic Collaborations for Ecosystem Expansion

Savitri aims to weave its technology into the fabric of multiple industries by:

- *Industry Partnerships:* Establishing collaborations with key players in finance, healthcare, supply chain, and IoT to integrate Savitri's blockchain solutions into their operations, demonstrating the versatility and efficiency of the platform.

- *Startup Accelerators:* Partnering with startup accelerators and incubators to provide resources and mentorship to emerging companies building on the Savitri platform, encouraging innovation and growth within the Savitri ecosystem.

- *Government and Regulatory Bodies Engagement:* Working closely with government entities to ensure compliance and explore opportunities for blockchain to enhance public services and infrastructure.

8.3. Comprehensive Marketing and Brand Positioning

To build a strong, recognizable brand, Savitri will:

- *Targeted Advertising Campaigns:* Deploying digital marketing campaigns across social media, search engines, and relevant online forums to reach potential users and investors, utilizing analytics to refine and target messaging effectively.

- *Community Building and Engagement:* Leveraging platforms like Reddit, Twitter, and Telegram to engage with the community, gather feedback, and foster a sense of ownership and involvement among early adopters and enthusiasts.

- *Success Stories and Use Cases:* Showcasing real-world applications and successes of the Savitri platform to illustrate its potential, encouraging adoption by demonstrating tangible benefits and solved problems.

8.4. Developer Support and Network Growth

Recognizing that developers are key to the ecosystem's growth, Savitri will:

- *Developer Grants and Incentives:* Offering financial grants, resources, and support to developers creating innovative applications on Savitri, aiming to lower barriers to entry and encourage experimentation and development.

- *Comprehensive* Documentation and Tools: Providing well-documented APIs, SDKs, and development tools alongside responsive support channels to facilitate easy development of applications on the Savitri network.

- *Open-Source Community* Engagement: Actively contributing to and engaging with the open-source community to drive innovation, improve the platform, and maintain transparency and trust with developers.

8.5. Fostering Global Adoption and User Accessibility

To ensure Savitri's technology reaches a broad audience, the strategy includes:

- *Multi-Language Support:* Offering platform documentation, tutorials, and support in multiple languages to cater to a global audience, breaking down language barriers that often hinder technology adoption.

- *User-Friendly Interfaces:* Developing intuitive user interfaces for both developers and end-users, making it simpler to interact with the blockchain, whether it's for building applications or conducting transactions.

- *Global Outreach Programs:* Implementing regional outreach programs tailored to address local needs and challenges, facilitating global adoption by making blockchain technology relevant and accessible to diverse populations.

- *Through these strategic pillars*, Savitri aims not just to introduce a new blockchain solution but to foster a thriving, global ecosystem that leverages blockchain technology for innovation, efficiency, and problem-solving across industries. This detailed market strategy is designed to ensure that Savitri becomes synonymous with accessible, scalable, and sustainable blockchain technology.

9. *Examples of Savitri's Use Cases.*

Here is possible to find some examples of use cases , how Savitri's network can be used and the advantages.

9.1. Use Case 1: Decentralized Finance (DeFi) Platform

Existing Problems:

- High transaction fees and slow processing times in current DeFi platforms due to network congestion.
- Limited accessibility for users in underbanked regions, restricting participation in global finance.

Solutions with Savitri:

- Low Transaction Costs and High Speed: Utilizing Savitri's Proof of Unity (PoU) consensus mechanism ensures faster transaction processing with significantly lower fees, making DeFi more accessible and economically viable for all users.
- Global Accessibility: Savitri's focus on seamless integration and democratized access makes financial services available even in underbanked regions, leveraging mobile connectivity for wider adoption.

Execution:

- Develop a DeFi application on Savitri's layer-1 blockchain that offers lending, borrowing, and yield farming services.
- Implement a user-friendly interface with multilingual support to ensure global accessibility.
- Utilize Savitri's low-cost transaction model to enable micro-transactions, appealing to users in economies of varying scales.

9.2. Use Case 2: Supply Chain Transparency

Existing Problems:

- Lack of transparency and traceability in supply chains, leading to inefficiencies and fraud.
- Difficulty in verifying the authenticity of products, which affects consumer trust.

Solutions with Savitri:

- Immutable Ledger: Savitri's blockchain provides a transparent and unchangeable record of every transaction and product movement, enhancing traceability.
- Smart Contracts for Automation: Automate supply chain processes like payments and verifications, reducing human error and increasing efficiency.

Execution:

- Partner with manufacturers and distributors to implement Savitri's blockchain for real-time tracking of product movements.
- Develop smart contracts that trigger automatic payments upon the fulfillment of specific conditions, streamlining the supply chain.
- Offer consumers access to a transparent history of their purchased products, from production to delivery, via a simple scan of a QR code.

9.3. Use Case 3: Secure IoT Network

Existing Problems:

- Security vulnerabilities in IoT devices lead to data breaches and unauthorized access.
- Difficulty in managing and authenticating vast numbers of devices within the IoT ecosystem.

Solutions with Savitri:

- Decentralized Security: By treating each IoT device as a network node, Savitri enhances security through decentralized consensus, reducing single points of failure.
- Efficient Device Management: Savitri's ability to integrate IoT devices directly with the blockchain simplifies device management and authentication.

Execution:

- Implement a secure IoT platform on Savitri's network, where each device is registered as a unique node with specific access rights and functions.
- Utilize smart contracts for device-to-device communication and transactions, ensuring data integrity and secure automation of tasks.
- Provide a dashboard for users to monitor and manage their IoT devices, leveraging Savitri's secure and transparent ecosystem.

10. Conclusion

In the rapidly evolving world of blockchain technology, the Savitri project emerges as a transformative solution poised to overcome some of the most significant challenges facing decentralized networks today. These challenges, including scalability, security, environmental sustainability, and user accessibility, have hampered the broader adoption and utility of blockchain technology. By introducing the innovative Proof of Unity (PoU) consensus mechanism and a commitment to seamless integration into everyday applications, Savitri aims to democratize access to blockchain technology, making it as foundational and ubiquitous as the internet.

Scalability issues have long plagued existing blockchain networks, leading to increased transaction costs and slower processing times. Savitri addresses these challenges head-on with PoU, which eschews the competitive nature of traditional consensus mechanisms for a collaborative approach, enabling faster transaction speeds and reduced costs. This paradigm shift not only enhances network efficiency but also fosters a more inclusive blockchain ecosystem by ensuring that the network remains open and accessible to all.

Security concerns, particularly the risk of centralized control and vulnerability to attacks, are also significant hurdles. Savitri's distributed authority model, inherent in the PoU mechanism, equitably distributes participation and governance across the network, thereby bolstering its security against attacks and manipulation.

The environmental impact of blockchain technology, especially those relying on energy-intensive Proof of Work (PoW) mechanisms, cannot be overstated. Savitri's PoU consensus requires significantly less energy, aligning with global efforts towards a greener and more sustainable technological footprint. This commitment to environmental responsibility not only addresses one of the critical critiques of blockchain technology but also sets a new standard for future developments.

User accessibility and the integration of blockchain into daily life are at the core of Savitri's vision. By simplifying the user interface and providing educational resources and development support through the Savitri Foundation, the project aims to lower barriers to blockchain adoption. This approach promises to extend the benefits of blockchain technology beyond financial transactions, encompassing various applications that benefit from its principles of transparency and immutability.

The results of implementing the Savitri project's solutions are manifold. Firstly, by solving scalability and security issues, Savitri ensures that its blockchain can support a high volume of transactions efficiently and securely, making it a viable platform for a wide range of applications. Secondly, the project's commitment to sustainability resonates with a growing demand for environmentally responsible technology solutions, potentially attracting a broader user base. Lastly, by focusing on user accessibility and practical applications, Savitri has the potential to drive the widespread adoption of blockchain technology, making it a staple in digital interactions across various sectors.

In conclusion, the Savitri project represents a comprehensive and forward-thinking response to the challenges currently facing blockchain technology. Through its innovative consensus mechanism, commitment to environmental sustainability, and focus on democratizing access, Savitri is not just a blockchain project but a movement towards a decentralized, secure, and equitable digital future. As the project moves forward, it invites collaboration and innovation, setting the stage for a new chapter in the evolution of blockchain technology, where it becomes a central pillar in the digital age, enhancing freedom, security, and community across the globe

230k

Transaction processing per second in our network

"Once the technical and adoption challenges are overcome, blockchain has the potential to revolutionize not only the financial sector but also other industries such as healthcare, logistics, and public administration, ensuring secure, transparent, and immutable transactions.".

Andrea Cadamuro
CEO Savitri Foundation

11. Roadmap

Q2-Q4 2022

- Start developing Proof of Unity
- Realization algorithm for p2p communication between nodes and masternodes
- Developing Monolith block

Q1-Q4 2023

- Test monolith block
- Start of a first marketing campaign
- The presentation of the project for early investors
- Creation of a dedicated website
- Releasing devnet Savitri

Q1-Q2 2024

- Foundation opened
- Developing and release fee voting calibration
- Start Global Marketing pre-sale coin
- Release transaction multi-sig
- Release open test net

Q3-Q4 2024

- Mobile application development
- Coin distribution and unlocking
- Mobile application release
- Launch pad
- Listings
- Release hardware node, masternode Savi Coin
- start cloud mining Savi Coin

Q1 2025

- Release open main net
- Release Gateway IoT Decentralized

Glossary

Blockchain: A distributed ledger technology that maintains a growing list of records, called blocks, linked and secured using cryptography. It serves as the foundation for immutable and transparent transactions without the need for a central authority.

Consensus Mechanism: A process used in blockchain to achieve agreement among all network nodes on the state of the distributed ledger. Ensures that every copy of the database is identical.

Proof of Unity (PoU): An innovative consensus mechanism developed by Savitri, designed to overcome the challenges of scalability, security, and environmental sustainability. It promotes a collaborative environment rather than a competitive one among nodes.

Node: A computer, mobile, device or server that participates in the blockchain network, maintaining a copy of the ledger and, in the case of Savitri, contributing to the consensus process through the PoU mechanism.

Master Node: Nodes with advanced functionalities within the Savitri network, requiring a significant stake of SAVI tokens to operate. Master Nodes perform critical roles, including the creation of Monolith Blocks.

Monolith Block: A special type of block used in the Savitri blockchain to simplify network entry for new nodes by providing a complete snapshot of the network's state.

Smart Contracts: Self-executing contracts with the terms of the agreement between buyer and seller directly written into lines of code. They are executed automatically when predefined conditions are met.

IoT (Internet of Things): The extension of Internet connectivity into physical devices, vehicles, and other objects embedded with electronics, software, sensors to collect and exchange data.

Tokenomics: A combination of the words "token" and "economics," describing the economic properties and governance strategies of a cryptocurrency within the blockchain ecosystem it operates in.

SAVI: The native token of the Savitri network, used for transactions, paying fees, consensus rewards, and as a means of staking in Master Nodes.

Decentralized Finance (DeFi): Financial services built on blockchain technologies that operate without traditional intermediaries, such as banks or insurance companies, offering services like lending, exchanges, and insurances.

Supply Chain Transparency: The complete and unobstructed visibility of all parts and processes along the supply chain, from production to delivery, facilitated by blockchain technology.

Decentralized Applications (DApps): Applications that run on a peer-to-peer network of computers rather than a single computer, often built on a blockchain platform.

Staking: The process of holding funds in a cryptocurrency wallet to support the operations of a blockchain network. Often, users are rewarded for their staking.

Cryptocurrency: A type of digital currency that uses cryptography for securing transactions, controlling the creation of new units, and ensuring the transfer of assets.

Distributed Ledger Technology (DLT): The underlying technology of blockchain, which enables the recording, sharing, and synchronization of transactions in a distributed ledger across multiple sites, without the aid of a central authority.

Hash Function: A function that converts an input (or 'message') into a fixed-length string of bytes, typically a sequence of numbers and letters. Hash functions are a critical component of blockchain technology to maintain data integrity.

Mining: The process through which transactions are verified and added to the public blockchain ledger. In the context of blockchains like Bitcoin, mining also involves creating new coins as a reward for the work done.

Peer-to-Peer (P2P) Network: A network of computers where all machines share and access data without the need for a central server. Blockchains operate on P2P networks to ensure decentralization and censorship resistance.

Public Key Cryptography: A form of cryptography that uses pairs of keys: a public one, which can be shared freely, for encrypting messages, and a private one, for decrypting them. It is fundamental to the security of blockchain transactions.

Scalability: The ability of a blockchain network to handle a growing amount of transactions without compromising its performance or security.

Token Burning: The process of permanently removing a number of tokens from the available circulation, usually to manage inflation or increase the scarcity of a cryptocurrency.

Wallet: Software or hardware that allows users to store and manage their cryptographic keys for cryptocurrencies, facilitating the sending and receiving of digital currencies.

Interoperability: The ability of different blockchain networks to share and access information across networks, allowing seamless interaction between different blockchain platforms.

Consensus Algorithm: The algorithm used by a blockchain network to reach a unanimous agreement on the state of the distributed ledger, ensuring that every copy of the database is updated and consistent with the others.

51% Attack: An attack on a blockchain network where a single entity or a group of miners controls more than 50% of the network's hashing power, allowing them to manipulate transactions or rewrite parts of the blockchain.

Gas: A unit of measure indicating the computational cost necessary to perform operations or transactions on the Ethereum network. Gas is used to allocate network resources and to prevent spam or DDoS attacks.

Fork: A change in the protocol of a blockchain that produces two separate chains: one that follows the new protocol (hard fork) and one that continues to follow the old protocol (soft fork).

References

[1] Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." [Online]. Available: https://bitcoin.org/bitcoin.pdf. Accessed on [Date].

[2] Buterin, V. (2013). "Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform." [Online]. Available: https://ethereum.org/en/whitepaper/. Accessed on [Date].

[3] Swan, M. (2015). "Blockchain: Blueprint for a New Economy." O'Reilly Media. ISBN: 978-1491920497.

[4] Mougayar, W. (2016). "The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology." Wiley. ISBN: 978-1119300311.

[5] Antonopoulos, A. M. (2014). "Mastering Bitcoin: Unlocking Digital Cryptocurrencies." O'Reilly Media. ISBN: 978-1449374044.

[6] Tapscott, D., & Tapscott, A. (2016). "Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World." Penguin Books Ltd. ISBN: 978-1101980132.

[7] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends." In Proceedings of the 2017 IEEE 6th International Congress on Big Data. [Online]. Available: DOI: 10.1109/BigDataCongress.2017.85.

[8] Pilkington, M. (2016). "Blockchain Technology: Principles and Applications." In Research Handbook on Digital Transformations. Edward Elgar Publishing. ISBN: 978-1784717759.

[9] Casey, M. J., & Vigna, P. (2018). "The Truth Machine: The Blockchain and the Future of Everything." St. Martin's Press. ISBN: 978-1250114570.

[10] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). "Blockchain Technology: Beyond Bitcoin." Applied Innovation Review, Issue 2. [Online]. Available: https://sutardja.berkeley.edu/wp-content/uploads/2015/09/AIR-2016-Blockchain.pdf. Accessed on [Date].

[11] Iansiti, M., & Lakhani, K. R. (2017). "The Truth About Blockchain." Harvard Business Review. [Online]. Available: https://hbr.org/2017/01/the-truth-about-blockchain. Accessed on [Date].

[12] Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." [Online]. Available: https://bitcoin.org/bitcoin.pdf. Accessed on [Date].

[13] Buterin, V. (2013). "Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform." [Online]. Available: https://ethereum.org/en/whitepaper/. Accessed on [Date].

[14] Swan, M. (2015). "Blockchain: Blueprint for a New Economy." O'Reilly Media. ISBN: 978-1491920497.

[15] Mougayar, W. (2016). "The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology." Wiley. ISBN: 978-1119300311.

[16] Antonopoulos, A. M. (2014). "Mastering Bitcoin: Unlocking Digital Cryptocurrencies." O'Reilly Media. ISBN: 978-1449374044.

[17] Tapscott, D., & Tapscott, A. (2016). "Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World." Penguin Books Ltd. ISBN: 978-1101980132.

[18] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends." In Proceedings of the 2017 IEEE 6th International Congress on Big Data. [Online]. Available: DOI: 10.1109/BigDataCongress.2017.85.

[19] Pilkington, M. (2016). "Blockchain Technology: Principles and Applications." In Research Handbook on Digital Transformations. Edward Elgar Publishing. ISBN: 978-1784717759.

[20] Casey, M. J., & Vigna, P. (2018). "The Truth Machine: The Blockchain and the Future of Everything." St. Martin's Press. ISBN: 978-1250114570.

[21] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). "Blockchain Technology: Beyond Bitcoin." Applied Innovation Review, Issue 2. [Online]. Available: https://sutardja.berkeley.edu/wp-content/uploads/2015/09/AIR-2016-Blockchain.pdf.

[22] Iansiti, M., & Lakhani, K. R. (2017). "The Truth About Blockchain." Harvard Business Review. [Online]. Available: https://hbr.org/2017/01/the-truth-about-blockchain.

[23] International Conference on Innovative Computing and Communications. (2019b). In Lecture notes in networks and systems. https://doi.org/10.1007/978-981-13-2324-9

Savitri
Foundation

Savitri Foundation
info@savitrifoundation.tech
www.savitrifoundation.tech