TABLE OF CONTENTS

1. INTRODUCTION

The Voiceban network is a groundbreaking decentralized blockchain platform created to establish a censorship-free social media ecosystem. By harnessing the power of advanced blockchain technology and implementing strategic design principles, Voiceban aims to provide users with a secure and resilient platform for engaging in social interactions, sharing content, and expressing their thoughts without fear of censorship or restrictions.

At the core of the Voiceban network lies a robust and distributed blockchain infrastructure built on Substrate, a flexible framework for creating customized blockchains. This choice enables Voiceban to leverage the inherent security, transparency, and decentralization of blockchain technology while providing the flexibility necessary to tailor the network to the specific needs of a social media platform. By utilizing a blockchain-based architecture, Voiceban ensures that all transactions and interactions on the platform are recorded immutably and can be verified by network participants, thus establishing a high level of trust and transparency within the ecosystem.

One of the outstanding features of Voiceban is its resistance to censorship attempts. Traditional social media platforms often face challenges related to content moderation, with centralized authorities exerting control over what can be shared or discussed. Voiceban addresses this issue by decentralizing control and decision-making, ensuring that no single entity has the power to arbitrarily restrict or manipulate user-generated content. By distributing governance responsibilities among network participants through consensus mechanisms and decentralized decision-making protocols, Voiceban aims to foster an environment where freedom of expression and diverse perspectives thrive.

Moreover, the Voiceban network is designed to withstand malicious attacks and ensure uninterrupted operation. By leveraging the security features inherent in blockchain technology, such as cryptographic algorithms and consensus mechanisms, Voiceban establishes a robust defense against various forms of attacks, including distributed denial-of-service (DDoS) attacks, and attempts to compromise the integrity of the network. Additionally, the decentralized nature of the network enhances its resilience, as multiple network nodes are involved in validating and storing transactions, reducing the risk of a single point of failure.

Therefore, the Voiceban network represents an innovative step towards creating a censorship-free social media platform. By leveraging the power of blockchain technology and implementing deliberate design choices, Voiceban aims to provide users with a secure and resilient environment for expressing themselves, sharing content, and engaging in social interactions without fear of censorship or disruptions. With its decentralized governance, robust security measures, and commitment to freedom of expression, Voiceban strives to redefine the landscape of social media and empower users to exercise their right to voice their opinions freely.

1.1. IMPORTANCE

Uncensored social media platforms hold significant importance in today's digital landscape. Here are some key reasons why they are crucial:

- **Freedom of Expression:** Uncensored social media platforms prioritize and uphold the fundamental right to freedom of expression. They provide users with a space to voice their opinions, share diverse perspectives, and engage in open discussions without the fear of censorship or repercussions. By enabling individuals to express themselves freely, these platforms foster a healthy exchange of ideas and encourage democratic participation.
- **Protection of Human Rights:** In many parts of the world, traditional media outlets are subject to censorship and control, limiting access to information and suppressing dissenting voices. Uncensored social media platforms act as an alternative avenue for individuals to exercise their right to access and disseminate information. They empower users to shed light on human rights abuses, social injustices, and political repression, ultimately promoting transparency and accountability.
- **Promotion of Pluralism and Diversity:** By allowing a wide range of voices to be heard, censorship-free social media platforms promote pluralism and diversity. Traditional media outlets often prioritize certain narratives or viewpoints, leading to the exclusion of marginalized communities and underrepresented perspectives. In contrast, these platforms encourage inclusivity and provide a space for individuals from all backgrounds to contribute to public discourse.
- **Counteracting Disinformation and Propaganda:** Uncensored social media platforms play a vital role in combating disinformation, fake news, and propaganda. Through transparent and decentralized mechanisms, they allow for collective fact-checking and identifying misleading information. Users can engage in open discussions, provide evidence-based arguments, and contribute to a more informed public discourse.
- **Empowerment of Individuals:** Such social media platforms empower individuals by giving them control over their own data and digital identity. Users can decide what they share, who they connect with, and how they engage with the platform. This shift from centralized control to user autonomy promotes a sense of ownership and agency, fostering a more user-centric online experience.
- **Resilience against Censorship and Authoritarianism:** In regions where freedom of speech is heavily restricted, censorship-free social media platforms provide a means for individuals to bypass government censorship and access information that would otherwise be suppressed. By leveraging decentralized technologies, these platforms make

it challenging for authorities to shut down or control access to information, thus acting as a resilient tool against censorship and authoritarian regimes.

Therefore, uncensored social media platforms, like Voiceban, are essential for upholding democratic principles, protecting human rights, promoting diversity, countering disinformation, empowering individuals, and resisting censorship. By providing a space for open and unrestricted communication, these platforms foster a more inclusive and democratic digital society.

2. Understanding Decentralized Blockchain Networks

Blockchain technology is a distributed and decentralized digital ledger that records transactions across multiple computers, referred to as nodes, in a network. It operates on the principle of consensus, where all participants in the network agree on the validity of transactions through a consensus algorithm. The blockchain consists of a chain of blocks, each containing a list of verified and timestamped transactions.

The decentralized nature of blockchain technology stems from its distributed ledger architecture. Instead of relying on a central authority or intermediary to validate and record transactions, blockchain networks distribute this responsibility across multiple nodes. Each node in the network maintains a copy of the entire blockchain, ensuring transparency and reducing the risk of a single point of failure.

Blockchain technology enables decentralization by providing the following key features:

1) **Trust and Transparency:** Transactions recorded on the blockchain are transparent and immutable. Once a transaction is added to the blockchain, it cannot be altered or deleted without the consensus of the network participants. This transparency enhances trust among participants as they can independently verify and audit the transaction history.
2) **Consensus Mechanisms:** Blockchain networks use consensus mechanisms to validate and agree upon the order of transactions. These mechanisms ensure that all participants reach a common agreement on the state of the blockchain. Popular consensus mechanisms include Proof of Work (PoW), Proof of Stake (PoS), and Nominated Proof of Stake (NPoS).
3) **Security and Tamper Resistance:** Blockchain employs cryptographic techniques to secure the integrity and immutability of transactions. Each block contains a cryptographic hash of the previous block, creating a chain that is resistant to tampering. Modifying a block would require recalculating the hash of that block and all subsequent blocks, making it computationally infeasible and economically costly.
4) **Elimination of Intermediaries:** With blockchain, participants can interact directly with each other without the need for intermediaries such as banks, payment processors, or

central authorities. This eliminates the dependency on third-party trust and reduces costs associated with intermediation.

The role of blockchain in decentralization goes beyond financial transactions. It has expanded to various sectors, including supply chain management, healthcare, voting systems, and social media platforms. By leveraging blockchain technology, these systems can achieve greater transparency, security, and democratization, reducing the reliance on centralized control and enabling peer-to-peer interactions.

Overall, blockchain technology's decentralized nature empowers individuals and communities by providing them with control over their data, enabling peer-to-peer transactions, and fostering trust in a distributed network without the need for intermediaries.

2.1. Blockchain Governance

Blockchain governance refers to the decision-making processes and mechanisms that govern the operation, development, and evolution of a blockchain network. It involves establishing rules, protocols, and mechanisms to coordinate and align the interests of various stakeholders within the network.

In traditional centralized systems, governance is typically centralized, with a central authority making decisions and enforcing rules. However, in blockchain networks, governance is often decentralized, allowing participants to collectively decide on the network's rules and protocols.

Blockchain governance can be categorized into three main components:

- **Protocol Governance:** Protocol governance refers to the decision-making process related to the rules and protocols that define the blockchain network. This includes areas such as consensus mechanisms, transaction validation rules, block size, and network upgrades. Participants in the network may propose changes or improvements to the protocol, and decisions are typically made through consensus mechanisms, such as stakeholder voting or community signaling.
- **Network Governance:** Network governance focuses on the overall management and administration of the blockchain network. It involves aspects such as node operations, network monitoring, security measures, and addressing potential network attacks or vulnerabilities. Network governance ensures the stability, security, and continuity of the blockchain network, often involving collaboration among network validators, developers, and infrastructure providers.
- **Community Governance:** Community governance encompasses the social and organizational aspects of the blockchain network. It involves community participation, decision-making processes, and community guidelines. Community governance allows

stakeholders to voice their opinions, discuss network improvements, and collectively address challenges or disputes. It may include mechanisms such as voting, forums, working groups, or community representatives to facilitate communication and coordination among network participants.

Blockchain governance mechanisms can vary across different networks and may evolve. Some common governance models include:

- **On-chain Governance:** In this model, decision-making occurs directly on the blockchain through the use of smart contracts or on-chain voting mechanisms. Stakeholders can propose and vote on protocol upgrades or changes using the blockchain itself.
- **Off-chain Governance:** Off-chain governance involves decision-making processes that occur outside the blockchain, typically through discussions in forums, community meetings, or social platforms. Stakeholders may discuss and debate proposals before implementing changes to the network.
- **Hybrid Governance:** Some blockchain networks adopt a hybrid governance model, combining both on-chain and off-chain governance mechanisms. This approach allows for a balance between transparency, efficiency, and inclusiveness.

Effective blockchain governance aims to ensure fairness, transparency, and the long-term sustainability of the network. It requires active participation and collaboration from network participants to make informed decisions and address the evolving needs and challenges of the blockchain ecosystem.

2.2. Advantages of Utilizing Blockchain Technology in Social Media Platforms

Using blockchain technology for social media platforms offers several advantages that can significantly enhance the user experience and address the limitations of traditional centralized platforms. Here are some key advantages:

A. **Decentralization and Censorship Resistance:** Blockchain-based social media platforms are inherently decentralized, removing the need for a central authority or intermediary to control and moderate content. This decentralization makes it difficult for any single entity to censor or manipulate the platform, ensuring freedom of expression and protecting against arbitrary content removal or restrictions.

B. **Data Privacy and Ownership:** Traditional social media platforms often collect and control vast amounts of user data, which can be used for targeted advertising or other purposes without the explicit consent or knowledge of users. Blockchain-based platforms can give users greater control over their data, allowing them to choose what personal information they share and with whom. Additionally, the blockchain's immutable nature ensures that once data is stored on the blockchain, it cannot be altered or tampered with without consent, providing enhanced data privacy and security.

C. **Transparent and Trustworthy Content:** Blockchain enables transparent and verifiable content on social media platforms. Each interaction, post, or transaction is recorded on the blockchain, creating an immutable record of content and interactions. This transparency helps combat the spread of fake news and disinformation, as users can independently verify the authenticity and origin of content. Blockchain's trustworthiness also fosters a more reliable and credible social media ecosystem.

D. **Tokenization and Incentivization:** Blockchain platforms can introduce their native tokens or cryptocurrencies, which can be used to incentivize and reward user participation, content creation, and engagement. By tokenizing social media interactions, users can earn rewards for their contributions, such as receiving tokens for posting quality content, participating in discussions, or supporting other users' content. This incentivization mechanism encourages active user engagement and contributes to building vibrant and interactive social media communities.

E. **Enhanced Security and Data Integrity:** Blockchain's cryptographic algorithms and consensus mechanisms provide a robust security infrastructure for social media platforms. Transactions and data stored on the blockchain are encrypted and linked in a tamper-resistant manner, minimizing the risk of hacking or unauthorized access. This heightened security ensures the integrity and reliability of user data, mitigating the chances of data breaches or manipulation.

F. **Community Governance and Consensus:** Blockchain-based social media platforms can implement decentralized governance models where participants have a say in decision-making processes. Through consensus mechanisms and voting protocols, users can collectively shape the platform's rules, features, and policies. This democratic approach empowers the community, promoting a sense of ownership and fostering a more inclusive and responsive platform.

By leveraging the advantages of blockchain technology, social media platforms can redefine user experiences, establish trust, and provide an environment that promotes freedom of expression, privacy, and user control. These advantages address critical concerns associated with traditional social media platforms and pave the way for a more transparent, democratic, and user-centric social media ecosystem.

2.3. Why use Substrate

The Substrate framework is a powerful tool that enables developers to build customized blockchains with ease. Developed by Parity Technologies, Substrate simplifies the process of blockchain development by providing a modular framework that allows for the creation of highly scalable and interoperable decentralized applications (dApps). Here, we will explore the key features and benefits of the Substrate framework, highlighting why it has become a popular choice for building customized blockchains.

- ❖ **Modular Design and Customizability:** Substrate's modular design is one of its standout features, allowing developers to customize and tailor the blockchain according to their specific requirements. It provides a set of pre-built modules that can be combined and configured to create a unique blockchain architecture. This modular approach saves time and effort, as developers can leverage existing functionality without reinventing the wheel, while still having the flexibility to add or modify modules to suit their application's needs.
- ❖ **Developer-Friendly Environment:** Substrate offers a developer-friendly environment that simplifies the process of building blockchains. It provides a comprehensive set of tools, libraries, and documentation, making it easier for developers to understand and work with the framework. Substrate is written in Rust, a programming language known for its safety, speed, and concurrency, which enhances the security and performance aspects of the developed blockchain.
- ❖ **Scalability and Interoperability:** Scalability is a critical factor for blockchain adoption, and Substrate addresses this challenge by providing various mechanisms for optimizing performance. It allows for parallel execution of transactions, enabling higher throughput and faster confirmation times. Moreover, Substrate is designed to be interoperable, which means it can seamlessly interact with other blockchains and decentralized networks. This interoperability opens up possibilities for cross-chain communication, asset transfers, and integration with existing blockchain ecosystems.
- ❖ **Governance and Upgradability:** Substrate includes built-in governance and upgradability mechanisms, empowering blockchain communities to make collective decisions and upgrade their networks without causing disruptions. It provides a framework for on-chain governance, allowing stakeholders to propose and vote on changes, such as protocol upgrades or parameter adjustments. This feature fosters a more democratic and decentralized decision-making process, ensuring the long-term sustainability and evolution of the customized blockchain.
- ❖ **Security and Consensus Flexibility:** Security is of paramount importance in blockchain development, and Substrate incorporates various security measures to protect against attacks and vulnerabilities. It implements the latest cryptographic standards and ensures the integrity and confidentiality of data. Additionally, Substrate offers flexibility in choosing the consensus mechanism, allowing developers to select from a range of options such as proof-of-work (PoW), proof-of-stake (PoS), or even experimental consensus algorithms.

The Substrate framework provides an efficient and flexible solution for building customized blockchains. With its modular design, developer-friendly environment, scalability, interoperability, governance capabilities, and security features, Substrate empowers developers to create innovative decentralized applications tailored to their specific use cases. As blockchain technology continues to evolve, Substrate remains at the forefront, enabling the development of scalable, secure, and feature-rich blockchains.

3. ARCHITECTURE OF VOICEBAN NETWORK

The Voiceban network utilizes a peer-to-peer network architecture, where nodes establish direct connections to form a mesh topology. Each node may maintain a complete copy of the blockchain, ensuring redundancy and fault tolerance. The absence of a central authority mitigates single points of failure and enhances the network's resilience.

In the Voiceban social network, user-generated content such as posts and comments are treated as transactions. This allows the blockchain's inherent properties of immutability, transparency, and censorship-resistance to extend to the content posted by users.

3.1. Posts and Comments as Integral Parts of the Network

In the design of Voiceban, user-generated content, specifically posts and comments, form a significant and integral part. Each piece of content, whether it a post, a comment, an upvoice or a down-voice, is represented as a transaction within the blockchain. This approach allows us to leverage the inherent properties of blockchain technology — immutability, transparency, and censorship resistance — to protect and maintain the integrity of user content.

1. **Content Creation**: Whenever a user creates a post or comment, they initiate a transaction. This transaction, which includes the content data, the user's public key (representing their identity), and a digital signature (verifying the authenticity and integrity of the content), is broadcast to the network.

2. **Content Validation**: Nodes within our network, upon receiving this broadcast, validate the transaction. They check the digital signature against the user's public key to confirm that the content is authentic and hasn't been tampered with. Once validated, the transaction is then added to the block currently being assembled.

3. **Consensus and Block Addition**: To determine which of the assembled blocks are added to the chain, our network utilizes a defined consensus mechanism. Once consensus is reached, the block, containing all its validated transactions, becomes part of the blockchain. This, in turn, means that all posts or comments represented in those transactions are now part of the immutable ledger. For a more detailed explanation of the consensus mechanism utilized in our network, refer to the section titled 'Consensus Mechanisms'

4. **Preserving Content Integrity**: As transactions, posts and comments added to the blockchain cannot be altered or deleted, preserving the original intent and context of the user's contribution. This provides a robust platform for free, open conversation and maintains a high degree of censorship resistance. See section titled ‘Censorship Resistance’

With this architectural design, our blockchain network places posts and comments at its core, serving as key components. In effect, it offers a dependable, transparent, and unalterable infrastructure for user-generated content. It promotes community building and facilitates open discourse, all the while securing the integrity and longevity of users' contributions.

3.2. Consensus Mechanisms:

To achieve consensus and maintain network integrity, the Voiceban network employs a hybrid consensus mechanism. This mechanism combines both the Nominated Proof-of-Stake (NPoS) and the GRANDPA (GHOST-based Recursive Ancestor Deriving Prefix Agreement) protocols to reach consensus and maintain the overall integrity and stability of the blockchain. It initiates a Nominated Proof of Stake (NPoS) algorithm to elect validators responsible for block creation and validation. The mechanism is designed with two kinds of participants: validators and nominators. Participants interested in maintaining the network can run a node as a validator, and nominators can participate by backing up trusted validator candidates with their VBANs. Both get rewarded by the network.

The second part of the consensus mechanism is the GRANDPA protocol, which provides a way to finalize blocks that have been added to the blockchain. This means that once a block has been finalized by GRANDPA, it cannot be reverted or changed. GRANDPA is a Byzantine fault tolerant finality gadget, meaning it can tolerate up to one-third of participants acting dishonestly or failing. As validators form part of the GRANDPA protocol, they engage in voting processes on which blocks can be finalized. A block is deemed finalized when two-thirds of the validators reach a consensus on a set of blocks. This process guarantees the irreversibility of the decisions made, thereby solidifying the trust and reliability of our blockchain. GRANDPA is designed to finalize many blocks at once when network conditions are good, ensuring efficient operation. In more challenging network conditions, GRANDPA can still finalize blocks, but at a slower rate.

This hybrid approach ensures both security and scalability within the network.

3.3. Data Storage:

Data storage is a critical aspect of any blockchain system, including ours. The effectiveness, efficiency, and security of data storage have a direct impact on the performance and trustworthiness of the blockchain network. In this section, we will discuss the mechanisms of data storage used in our blockchain model.

Our blockchain system leverages decentralized data storage. Unlike centralized systems where data is stored on a single server or data center, in our blockchain network, data is distributed and stored across multiple nodes. This design enhances the security and robustness of the system as there is no single point of failure that could compromise the entire network.

In our model, each block in the blockchain stores a list of transactions. When a block is completed, it is added to the chain in a linear, chronological order. Each block contains a cryptographic hash of the preceding block, creating a linked chain from the genesis block to the most recent one. This design ensures the immutability of past transactions, as altering a single block would require the re-calculation of the hash of every subsequent block.

Furthermore, our system employs a Merkle Tree structure for efficient and secure verification of transactions. Each transaction is hashed, and the hashes are paired, hashed, paired again, and hashed again until a single hash remains, the Merkle root. This process enables the system to check the integrity of any transaction efficiently, without reviewing every single transaction.

In terms of data redundancy, nodes in our network holds a copy of the entire blockchain. While this may seem inefficient, it adds a level of security and transparency to the system. Any attempt to alter a transaction can be quickly identified and rejected by the network, maintaining the integrity of the stored data.

Lastly, our blockchain system has implemented sharding, a technique that enhances the scalability of data storage. Sharding partitions the database into smaller, faster, more easily managed parts called data shards, allowing nodes to process only a subset of the total network load. This significantly improves the overall capacity and performance of the system, enabling it to handle larger amounts of data and transactions.

In summary, our blockchain system adopts a comprehensive, secure, and efficient approach to data storage, leveraging decentralization, cryptographic linking, Merkle Trees, redundancy, and sharding to ensure data integrity, security, and scalability.

3.4. Network Security:

To protect against attacks and ensure network stability, the Voiceban network incorporates several security measures. Nodes communicate using encrypted channels, ensuring the confidentiality and authenticity of exchanged messages. Identity verification mechanisms and reputation systems are implemented to prevent unauthorized access and discourage malicious behavior.

3.5. Fault Tolerance and Disaster Recovery:

The Voiceban network is designed to be fault-tolerant, with mechanisms in place to handle node failures and network disruptions. In the event of a node failure, other nodes within the network take over the responsibilities of the failed node, ensuring uninterrupted operation. Data replication and redundancy techniques are employed to safeguard against natural disasters by geographically distributing nodes and data centers.

4. Censorship Resistance:

Censorship resistance is a fundamental characteristic of blockchain technology, including the Voiceban Network. In a blockchain system that's designed for content sharing, like posts and comments, this principle ensures that once the content has been added to the blockchain, it can't be arbitrarily manipulated or deleted by any single entity. Here are the ways by which we ensure censorship resistance in the network:

1. **Decentralization and Distribution**: Decentralization is a key feature contributing to the censorship resistance of Voiceban. Since the ledger is distributed across multiple nodes globally, no single entity has the power to control or manipulate the data stored on it. All nodes participate in validating transactions and maintaining the ledger, which ensures the integrity and censorship resistance of the network.

2. **Consensus Mechanisms**: Voiceban uses hybrid consensus mechanisms, GRANDPA and BABE, to secure the network. These mechanisms ensure that all nodes have to agree, or reach consensus, on the transactions that are added to the blockchain. This prevents a single node or a small group of nodes from unilaterally deciding what posts and comments are valid or invalid.

3. **Pseudonymity**: While all transactions are transparent and traceable on the blockchain, the parties involved are represented by their public keys, which are pseudonymous. End-users are also allowed to use arbitrary usernames which further ensures pseudonymity.

4. **Immutable Ledger**: Once a transaction or a post is confirmed and added to a block, which is then added to the blockchain, it is practically impossible to alter or remove. Any attempt to change a transaction would involve changing all subsequent blocks, which is computationally infeasible. This immutability protects against censorship by making it impossible to alter or erase past transactions.

5. **Permissionless**: Voiceban network is open to anyone who wants to participate. Anyone can become a node, validate transactions and create posts, as well as comments. This openness prevents the censorship of participation.

In summary, the Voiceban Network is designed to resist censorship. Through decentralization, consensus mechanisms, cryptographic security, immutable ledger, pseudonymity, a and a permissionless structure, the network ensures that all end-user interactions such as posts and comments are processed fairly and transparently, free from external manipulation or control.

4.1. Comparison to Centralized Servers:

When compared to centralized servers, the Voiceban network exhibits distinct characteristics. While centralized networks may offer advantages in terms of speed due to concentrated infrastructure, decentralized networks like Voiceban leverage optimization techniques and advanced protocols to achieve comparable or even superior performance. Decentralized networks can scale beyond centralized servers in terms of server resources, such as disk space, due to data distribution and redundancy. Moreover, decentralized networks aim to minimize server downtime through redundancy, fault tolerance mechanisms, and the ability of active nodes to continue serving traffic during outages.

4.2. Security of Data and Server Activity:

The Voiceban network ensures data and server activity security through various mechanisms. Data security is achieved through encryption techniques, safeguarding the confidentiality and integrity of data. Advanced encryption features, such as homomorphic encryption, enable secure computations on encrypted data. Node owners are responsible for implementing robust security measures, including secure access controls, regular software updates, and server hardening practices. Adherence to the consensus protocol ensures secure server activity, while network security measures, secure identity management, and regular auditing and compliance checks further enhance security.

5. Overall Working of Software:

The Voiceban netowork serves as a robust and user-friendly platform that utilizes blockchain technology to foster open conversations through posts and comments. It begins with an intuitive user interface that allows seamless content creation and interaction. When an interaction (post, comment, upvoice or down-voice) is created, it is encapsulated into a transaction that includes the user's public key and a digital signature. This transaction is then broadcasted to the network for validation by nodes, which check the digital signature for authenticity.

Upon validation, the transaction is added to a pool, from which new blocks are periodically formed. The addition of these blocks to the chain is governed by a consensus mechanism specific to our network. Users can effortlessly retrieve and view content stored in the form of transactions on the blockchain via the user interface, with the immutability of the blockchain ensuring the permanence and censorship resistance of each piece of content. Overall, the software provides a transparent, secure, and dependable environment for sharing and preserving user-generated content.

6. VALIDATORS

6.1. Connection of New Devices to Existing Node Architecture:

New devices connect to the existing node architecture through discovery and connection establishment. They undergo identity verification using cryptographic techniques, synchronize their local blockchain copy, and actively participate in the consensus process. Transaction validation, block creation, and agreement on the blockchain ledger occur through communication and consensus algorithms.

6.2. How to run your own validator

This section contains all the information one should need to start a validator node on Voiceban network using the command-line interface. We will start with how to do the initial setup of one's node and proceed to explaining the key managament and monitoring of the validator node. In order to begin the setup, we will use the following terminology of keys for this setup guide:

- ***Stash key:*** The stash keypair is going to be a cold wallet, where most of your funds should be located. The stash key is intended to hold a large amount of funds, so it should rarely, be exposed to the internet or used to submit extrinsics. It should be thought of as a saving's account at a bank, which ideally is only ever touched in urgent conditions.
- **Controller key:** The controller is the keypair, with a smaller balance, that will control your validator settings. The stash accounts register a certificate on-chain that delegates all validator operation and nomination powers to a controller account.
- **Session keys:** Session keys are hot keys that must be kept online by a validator to perform network operations.

One thing to note here is that all the keys are the type of account keys. They are distinguished by their intended use, not by an underlying cryptographic difference.

6.2.1. Pre-requisites

- You will need 6 keypairs: a stash (ed25519 or sr25519), controller (ed25519 or sr25519), and 4 session (3 ed25519 and 1 sr25519) keypairs. You can generate these using the ***subkey*** utility right away or you can use the polkadot.js wallet to create the *controller* and *stash* account addresses. It is strongly recommend that you use the *rotateKeys* node method to generate and manage the session keys.
- You will need at least the existential balance (100 VBAN) in both the *stash* and *controller* accounts plus the balances needed to send transactions from these accounts.

- You will need a live, fully-synced Voiceban node running with the ***--validator*** flag that has set one's session keys, either before or after you complete the onboarding process.

6.2.2. Setup

- First, you need to install the Rust toolchain based on your operating system, following the steps given here .
- Clone the node Repo
- In the root directory of the repo, run *cargo build –release*
- Next, need to run the validator node, by using the VbanChainSpec.json file, so that your node can be synced to the network.

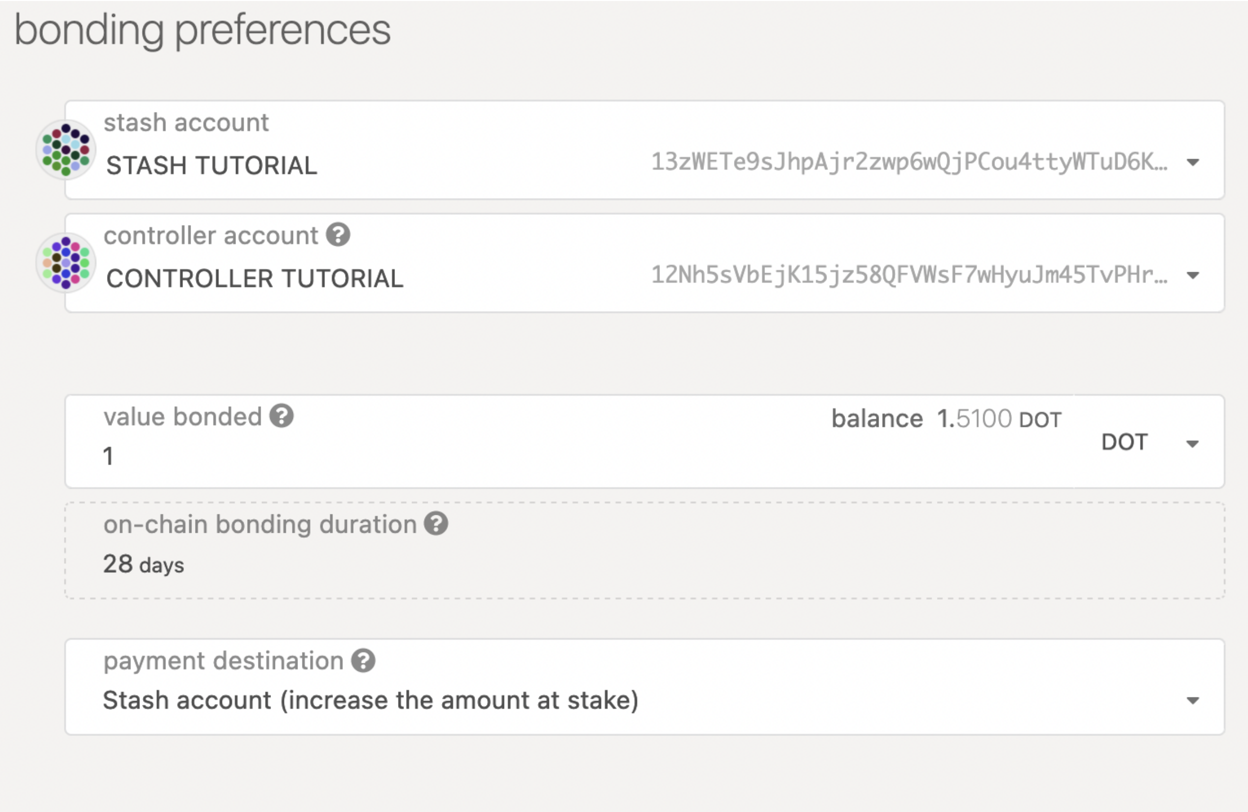
6.2.3. Validating

It is now time to set up our validator. We will do the following:

- Bond the VBAN of the Stash account. These tokens will be put at stake for the security of the network and can be slashed.
- Select the staking proxy. This is the account that will decide when to start or stop validating.

You need to follow the following steps in order to be able to validate in the Voiceban network:

1. First, go to the Staking section. Click on "Account Actions", and then the "+ Stash" button.



bonding preferences

stash account
STASH TUTORIAL 13zWETe9sJhpAjr2zwp6wQjPCou4ttyWTuD6K…

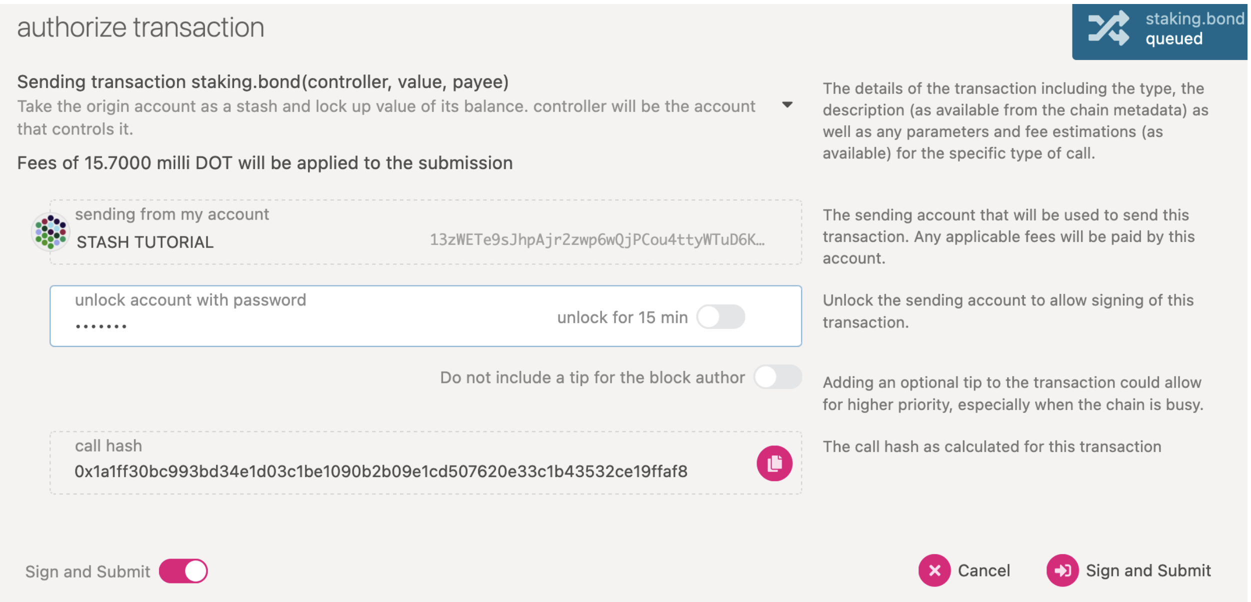
controller account
CONTROLLER TUTORIAL 12Nh5sVbEjK15jz58QFVWsF7wHyuJm45TvPHr…

value bonded
1
balance 1.5100 DOT
DOT

on-chain bonding duration
28 days

payment destination
Stash account (increase the amount at stake)

2. Once everything is filled in properly, click Bond and sign the transaction with your Stash account.



authorize transaction

staking.bond
queued

Sending transaction staking.bond(controller, value, payee)
Take the origin account as a stash and lock up value of its balance. controller will be the account that controls it.

Fees of 15.7000 milli DOT will be applied to the submission

The details of the transaction including the type, the description (as available from the chain metadata) as well as any parameters and fee estimations (as available) for the specific type of call.

sending from my account
STASH TUTORIAL 13zWETe9sJhpAjr2zwp6wQjPCou4ttyWTuD6K…

The sending account that will be used to send this transaction. Any applicable fees will be paid by this account.

unlock account with password
•••••••
unlock for 15 min

Unlock the sending account to allow signing of this transaction.

Do not include a tip for the block author

Adding an optional tip to the transaction could allow for higher priority, especially when the chain is busy.

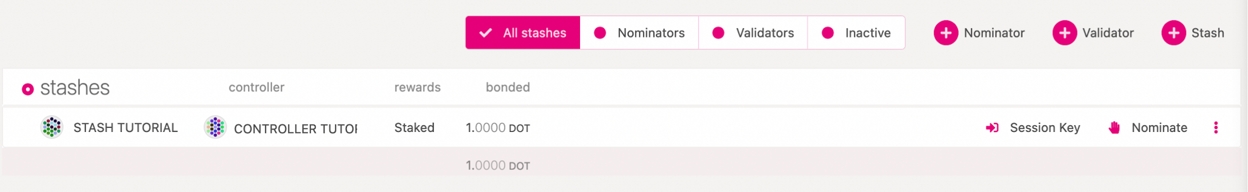
call hash
0x1a1ff30bc993bd34e1d03c1be1090b2b09e1cd507620e33c1b43532ce19ffaf8

The call hash as calculated for this transaction

Sign and Submit

After a few seconds, you should see an `ExtrinsicSuccess` message.

Your bonded account will available under `Stashes`. You should now see a new card with all your accounts (note: you may need to refresh the screen). The bonded amount on the right corresponds to the funds bonded by the Stash account.

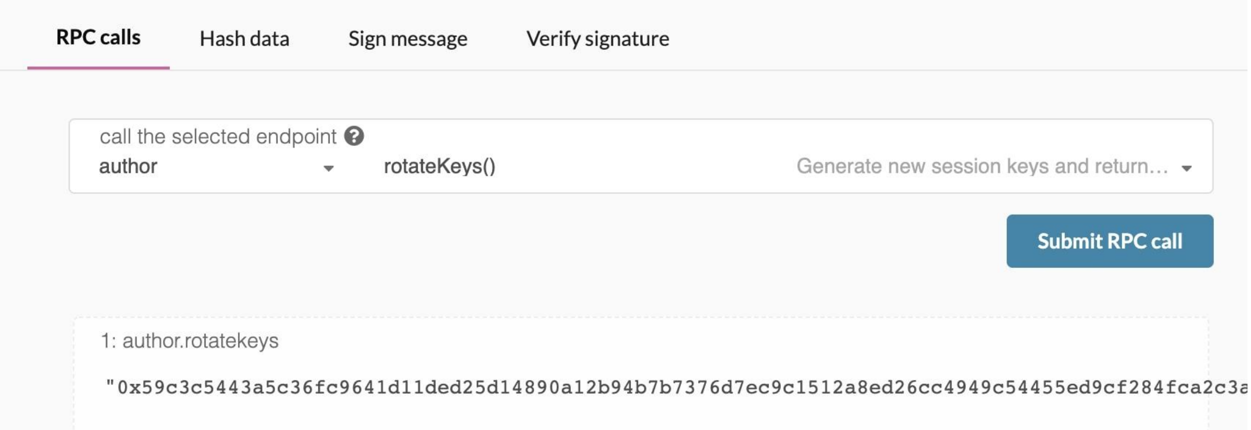


stashes	controller	rewards	bonded			
STASH TUTORIAL	CONTROLLER TUTOI	Staked	1.0000 DOT	Session Key	Nominate	⋮
			1.0000 DOT			

3. You need to tell the chain your Session keys by signing and submitting an extrinsic. This is what associates your validator node with your stash account on Polkadot.

You can generate your session keys in the client via the apps RPC. If you are doing this, make sure that you have the *PolkadotJS-Apps* explorer attached to your validator node. You can configure the apps dashboard to connect to the endpoint of your validator in the Settings tab. If you are connected to a default endpoint hosted by Parity of Web3 Foundation, you will not be able to use this method since making RPC requests to this node would effect the local keystore hosted on a *public node* and you want to make sure you are interacting with the keystore for *your node*.

Once ensuring that you have connected to your node, the easiest way to set session keys for your node is by calling the `author_rotateKeys` RPC request to create new keys in your validator's keystore. Navigate to Toolbox tab and select RPC Calls then select the author > rotateKeys() option and remember to save the output that you get back for a later step.



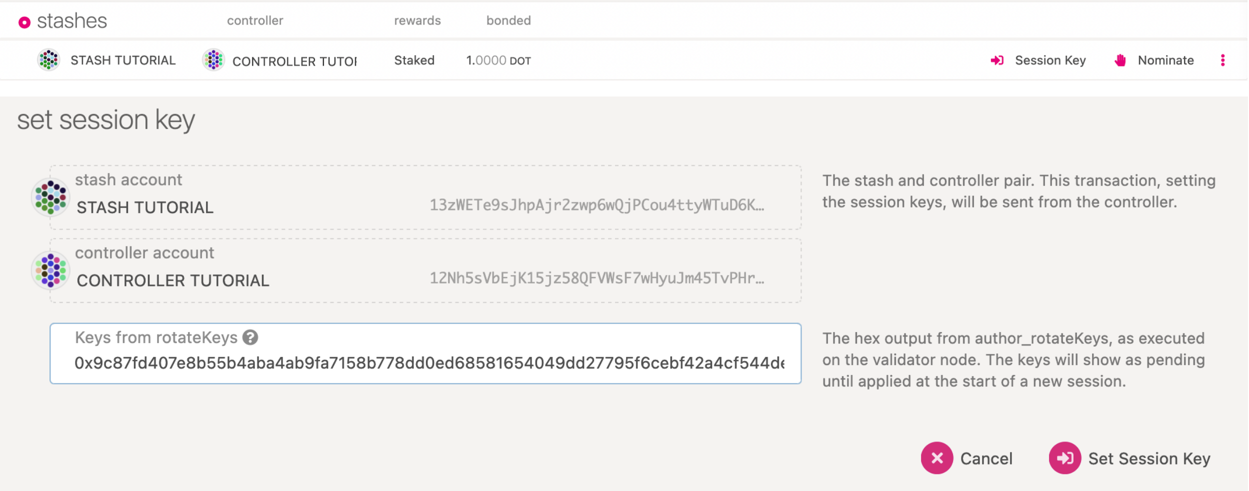
call the selected endpoint: author rotateKeys() Generate new session keys and return…

```
1: author.rotatekeys

"0x59c3c5443a5c36fc9641d11ded25d14890a12b94b7b7376d7ec9c1512a8ed26cc4949c54455ed9cf284fca2c3a
```

4. You need to tell the chain your Session keys by signing and submitting an extrinsic. This is what associates your validator with your staking proxy.

Go to [Staking > Account Actions](), and click "Set Session Key" on the bonding account you generated earlier. Enter the output from `author_rotateKeys` in the field and click "Set Session Key".



stashes	controller	rewards	bonded
STASH TUTORIAL	CONTROLLER TUTOI	Staked	1.0000 DOT

stash account: STASH TUTORIAL 13zWETe9sJhpAjr2zwp6wQjPCou4ttyWTuD6K…

controller account: CONTROLLER TUTORIAL 12Nh5sVbEjK15jz58QFVWsF7wHyuJm45TvPHr…

The stash and controller pair. This transaction, setting the session keys, will be sent from the controller.

Keys from rotateKeys: 0x9c87fd407e8b55b4aba4ab9fa7158b778dd0ed68581654049dd27795f6cebf42a4cf544de

The hex output from author_rotateKeys, as executed on the validator node. The keys will show as pending until applied at the start of a new session.

Submit this extrinsic and you are now ready to start validating.

5. The "reward commission percentage" is the commission percentage that you can declare against your validator's rewards. This is the rate that your validator will be commissioned with. You can specify the percentage of the rewards that will get paid to you. The remaining will be split among your nominators

6.3. Impact of Massive Server Outage on Active Nodes:

In the event of a massive server outage, the Voiceban network demonstrates resilience through its decentralized and fault-tolerant architecture. Active nodes continue to serve traffic as normal, ensuring uninterrupted operations. Decentralization and redundancy mechanisms enable active nodes to participate in transaction validation, block creation, and consensus even when a significant number of nodes experience server outages.

6.4. Impact of Complete Device Downtime:

In the scenario of all devices going down, the state of the ledger remains unaffected. However, availability for queries and transactions is suspended until at least one node recovers and resumes network operations.

By incorporating these technical details into your patent application, you provide a comprehensive and precise description of the Voiceban network, its technical underpinnings, and the specific optimizations that ensure its robustness, security, and uninterrupted operation.