Decentralizing Privacy: The Architecture and Mechanisms of PrivacyVPN

2023

1. Executive Summary

Privacy – Most of us accept this as a fact of life, but behind the scenes there is a competition going on for secret participants to get into as much of our privacy as possible. Internet users, we are restricted in how we use the Services and Applications due to censorship imposed by various regulatory authorities around the world. appears to us in many forms. Disagreement in such a paradigm would be dangerous, and in some places honest political disagreement would be impossible. Being crazy. Each user's daily online activities, communications and behavior are collected and sold to advertisers and any interested buyers. These operations are carried out with little or no consent from the user and with complete disregard for any notion of personal privacy. This is only because the user rating in these particular areas is lower. These factors require the creation of a protection system designed to protect the open and uninterrupted structure of the Internet. Blockchain technology's ability to create reliable censorship bypass mechanisms is possible. Create a new job. Going forward, we hope that the PrivacyVPN platform will provide the foundation for a world where all citizens around the world have open access to content and applications without the worry of censorship or a hacker stealing it from us.

2. Motivation behind PrivacyVPN

The current state of the internet lacks both openness and privacy. We believe that censorship and surveillance are unethical and unnecessary, serving as forms of intimidation and social control that hinder technological and social progress.

Contrary to the common belief that encryption is solely for concealing illicit activities, there are several legitimate and crucial applications for strong encryption. Below are six scenarios where encryption is indispensable:

1) Travelers in areas where their personal emails and social media are restricted or censored by local authorities.
2) Individuals discussing sensitive personal matters such as political views, religious beliefs, gender or sexual orientation, and entertainment preferences, which could potentially lead to discrimination or retaliation.
3) Companies that need to protect their confidential information to prevent corporate espionage.
4) Journalists who require secure communication channels to interact with whistleblowers, especially when these sources are within the organizations controlling the communication infrastructure.
5) Activists and dissidents planning meetings or protests who need to avoid surveillance by the entities they are challenging.
6) People, including protesters and journalists, who are reporting on human rights violations

to international news organizations, ensuring their communications are transmitted without local interference.

These instances illustrate the vital role of encryption in safeguarding privacy and enabling free communication under various circumstances.

We aim to create a decentralized peer-to-peer platform, known as the Node Network, which incorporates sustainable incentive protocols and leverages evolving techniques for evading censorship, developed collaboratively by the community. This platform, once operational, will empower individuals globally to both provide and access content freely, thereby circumventing censorship imposed by external entities.

Considerable discussion has been dedicated to the ethical implications of facilitating censorship evasion through our tools. We contend that the drawbacks of censorship, such as restricted information flow and controlled communication, do not justify its minimal purported benefits like potential crime reduction, increased profits for specific corporations, or enhanced political control. These goals could be pursued through more ethical strategies. Censors commonly employ sophisticated methods, including machine learning, to analyze internet usage patterns and identify undesired activities, yet these measures are often well-understood and circumvented by informed users.

2.1. Primary Goals

2.1.1. Phase I: Establishing a Fully Decentralized VPN Architecture

The initial aim is to fully decentralize the network of VPN nodes through the utilization of established VPN and proxy protocols, blockchain technology such as Ethereum, smart contracts, advanced state channels, and decentralized database technologies, alongside privacy-centric cryptocurrencies including Monero and Zcash, among others. This effort will unfold over three distinct development stages (refer to Section 5. Roadmap). By the conclusion of the third stage, we anticipate launching a wholly decentralized, open-source VPN architecture wherein every function is decentralized, thereby eliminating any single points of failure.

2.1.2. Phase II: Development of the PrivacyVPN Threads Standard

In the subsequent phase, our objective is to develop the PrivacyVPN Threads standard, which will enable the fragmentation of user data and its deep integration into the PrivacyVPN Threads network, thus preventing any potential tracking or censorship. The network is designed to manage the transport of this fragmented and encrypted data in an unrecognizable form to its destination, where the PrivacyVPN Threads will facilitate the reconstitution of the data. This protocol will evolve into a unified system incorporating various elements. Upon completion, it will ensure that user data remains secure, impervious to interception by either the nodes or external parties.

2.2. PrivacyVPN Initiative

PrivacyVPN is set to operate as a fully decentralized, peer-to-peer, and serverless network, aimed at enhancing privacy through innovative technologies while providing economic incentives to its network participants. The framework relies on integrating proven technologies such as blockchain, smart contracts, and enhanced state channels. These are further developed with sophisticated promise mechanisms and robust anti-censorship protocols devised by an active community, functioning as key components of the system.

Upon the completion of the initial development phase (Phase I, Stage 1), the network will safeguard user privacy and data. It will also allow users to monetize their unused bandwidth by providing access to those in need, in return for financial rewards.

PrivacyVPN will serve as a decentralized exchange, facilitating interactions between service providers and consumers who contribute to the ecosystem. This setup will cover provider costs through payments made in digital currencies. The project will unfold in several phases, each designed to mitigate risks, draw insights from early implementations, and integrate emerging tech-

nologies. By the end of Phase I, Stage 3, complete decentralization of the network's operational functions is expected.

Participants in the initial token offering will receive tokens that are essential for all transactions within the network. Post-deployment, the network is poised to support a diverse range of developments from various stakeholders, enhancing its utility with applications aimed at reducing censorship effectiveness, streamlining payment processes, and introducing new services by leveraging existing infrastructure and protocols.

From the early stages of Phase I, VPN-like services will be operational, offering functionalities comparable to, or even surpassing, those of existing centralized VPN services. This model will foster a competitive and highly scalable VPN solution, available for integration by other VPN providers or application developers. The open architecture and financial incentives for service providers will enhance the network's competitiveness. Further advancements and applications are anticipated in subsequent phases, culminating in full decentralization by the end of Stage 3.

3. Token Mechanism

Token Introduction

The token issued during the Token Creation is referred to as the PrivacyVPN Token, or PDVN. This issuance event is unique, establishing the total supply of PDVN as fixed.

Usage in the Network

PDVN will be fundamental to the PrivacyVPN Network. Consumers of VPN services will be charged fees in PDVN. The majority of these fees will be allocated to the VPN node owner (service provider), with the remainder dedicated to protocol development and support. Initially, these fees will be denominated in PDVN, although this could be subject to future changes.

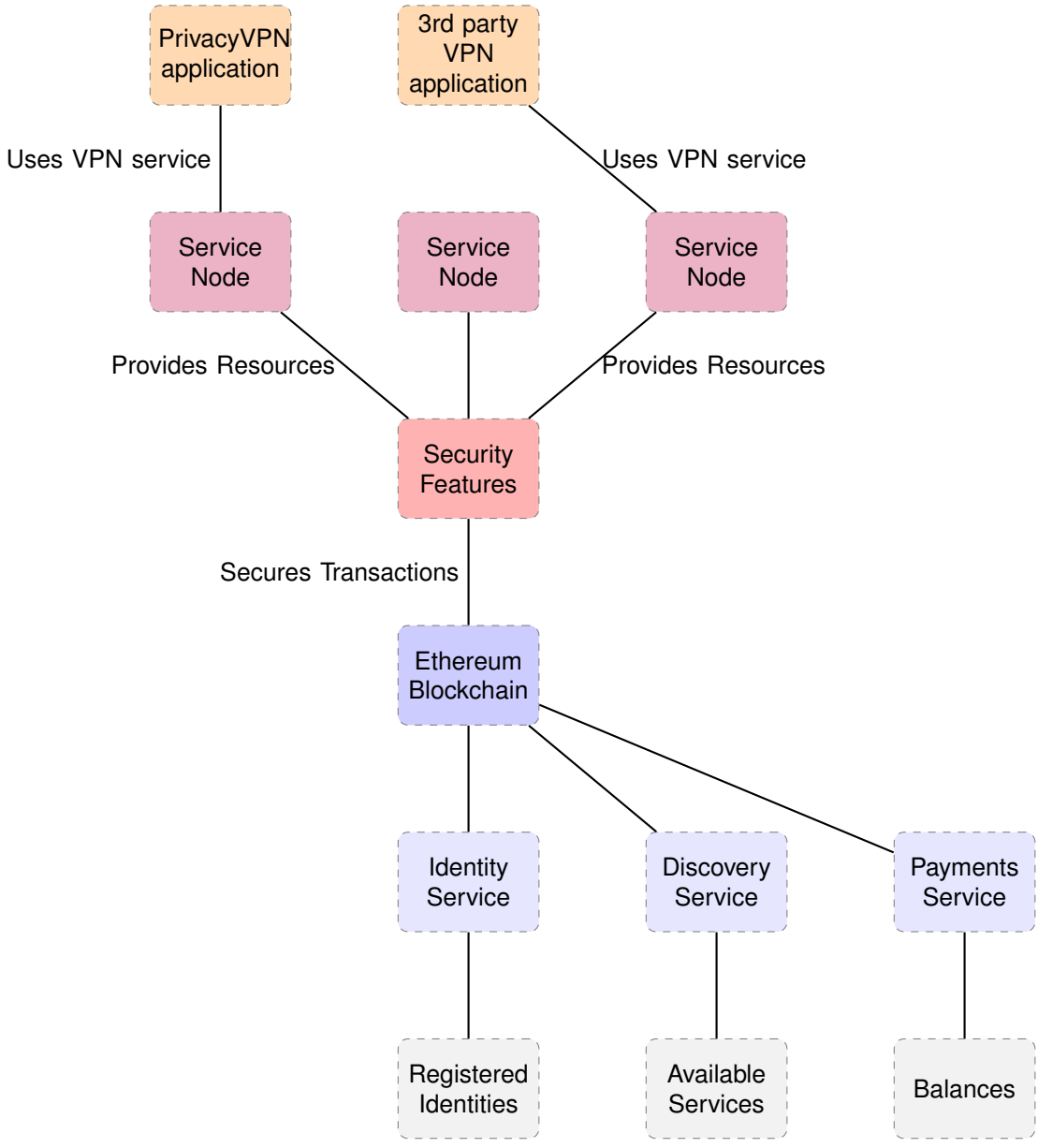
Incentives for Node Owners

Node owners are incentivized to support the network by operating their nodes. In this context, a node owner functions similarly to a miner. However, unlike typical blockchain miners who are rewarded for computing power (proof of work) or ownership of currency (proof of stake), node owners in this network are rewarded for sharing their bandwidth, receiving PDVN tokens as compensation.

Token Value and Growth

The value of the PDVN token is expected to reflect the growth of the PrivacyVPN Network. The PrivacyVPN Foundation will explore ways to enable PDVN holders to benefit by receiving a commission for each transaction conducted within the network, potentially in currencies other than PDVN.

4. Platform layers



The PrivacyVPN Threads architecture will be structured across four fundamental layers: Decentralised Databases,Decentralised Services Infrastructure, Service Providers and Service Clients..

4.1. Decentralised Services Infrastructure and Databases Layers

The foundational layers of the PrivacyVPN Threads include a Peer-to-Peer Service Infrastructure and Ledger Databases. These layers facilitate the essential smart contracts that enable nodes within the network to register, discover one another, and manage microtransactions seamlessly.

4.2. Service Providers Layer

The Node Operators Layer comprises various nodes operating as VPN service providers within the PrivacyVPN Threads ecosystem, delivering decentralized services to users.

4.3. Service Clients Layer

At the End-User Applications Layer of PrivacyVPN Threads, there are client applications. These are developed both in-house and by third-party developers utilizing the PrivacyVPN Threads infrastructure to offer VPN services to the end-users.

5. PrivacyVPN Architecture

The development of PrivacyVPN is an ongoing process and may undergo significant changes. The details provided in this section are therefore provisional and may be updated.

5.1. Technical Overview

In the PrivacyVPN threads, service consumers locate and compensate service providers through built-in smart contract-based Identity, Service Discovery, and Payment services. Operating over the Internet, the network utilizes the Ethereum blockchain to provide a censorship-resistant environment for distributed storage and transaction processing. PrivacyVPN employs Registered Identities, allowing for the establishment of trust when engaging with services and conducting payments.

Individuals with registered identities on the PrivacyVPN threads can offer VPN services in accordance with the network's protocols and the terms of payment under which these services are provided. Users can search for services that meet their requirements (such as location and price), use the search results to connect with chosen VPN service providers, and utilize the advertised services. A service consumer and a VPN service provider will engage in a dialogue to agree upon payment terms (like metering granularity) and the technical details needed for a secure VPN session. During this exchange, the consumer will commit to prepaying for the services and will renew this commitment whenever they wish to extend the service. Subsequently, the VPN service provider can claim payment through the smart contracts on the Ethereum blockchain. If the consumer's balance in the deposit account within the network is adequate, the agreed upon amount of PDVN tokens will be transferred from the consumer's deposit account to the provider's account.

5.2. Fundamental Elements

1) **Ethereum** The utilization of blockchain technology facilitates decentralized execution of code through smart contracts, ensuring the delivery of dependable services and the management of transactions.
2) **Identity service and database** ensures the proper identity acknowledgement between client and service provider
3) **Discovery service** Enable the listing of VPN services and help users choose the best VPN option for their needs.
4) **Payment service and database** allows secure promise-based micropayments for services..

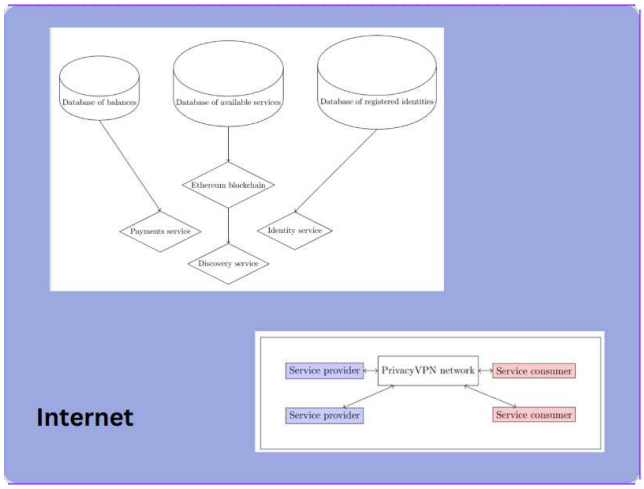


Fig. 1. Description of the figure.

Service Provisioning

In the PrivacyVPN threads, a client seeking VPN services selects a provider based on their needs and initiates a dialogue to discuss service terms and setup. This exchange, which may include negotiating payment and establishing VPN sessions, takes place over existing or new communication channels and continues until a disconnection occurs.

5.3. Identity Service

The system consists of interconnected software agents, each referred to as an identity agent, which represent and manage digital identities. Each identity agent operates on behalf of a user who controls the associated digital identity. These agents are critical components of the application, enabling nodes within the network to offer or utilize VPN services. An identity agent has the capability to authenticate and secure communications by electronically signing and decrypting messages using a private key linked to the identity it manages. Nodes within this architecture can manage multiple identities, enhancing flexibility and service options. Identities are established through the generation of cryptographic public and private key pairs. Each identity is uniquely identified using a unique identifier, which is derived from its public key.

In the PrivacyVPN threads, an identity is derived from the last 20 bytes of a keccak256 hash of the public key. This identity is made public by registering it on the Ethereum blockchain through an identity registration smart contract. The contract requires an identifier and the public key as arguments. Once executed successfully, the public key is appended to the blockchain, establishing it as a Registered Identity. Nodes within the PrivacyVPN network monitor the blockchain to track these registrations, maintaining a local database of all Registered Identities. This database allows nodes to verify public keys associated with other identities, ensuring that communications are from valid, registered sources and are properly authenticated.

5.4. Service Discovery

Service discovery in the PrivacyVPN network is a structured and systematic process:

1) **Service Announcement Preparation:** VPN service providers who wish to offer their services initiate the process by preparing a service proposal. This document includes details such as the proposal format version, a descriptive profile of the provider, a qualitative definition of the services offered, and the methods for accessing the provider's node.
2) **Proposal Signing:** The provider's Identity Agent signs the proposal to verify its authenticity.
3) **Blockchain Interaction:** The signed proposal is then submitted as an argument to a service announcement smart contract on the Ethereum blockchain.

4) **Blockchain Mining:** A miner processes the smart contract, adding the proposal to the Ethereum blockchain. This action makes the proposal publicly accessible, allowing any network participant to read and duplicate it.
5) **Proposal Tracking and Storage:** Nodes within the network monitor the blockchain for new proposals, noting the specific blockchain block number where each proposal appears. They extract these proposals directly from the transactions.
6) **Database Construction:** Nodes use the extracted proposals to build and maintain a local database of available services across the network. This database is kept consistent with the blockchain's state and includes comprehensive service listings.
7) **Service Querying:** Nodes can search this local database, or query databases maintained by other trusted nodes, to find services that meet specific user requirements based on location, service quality, and other criteria.

This detailed process ensures that all service offerings on the network are verified and registered, enabling efficient and secure service discovery.

5.5. Payment service

The PrivacyVPN network utilizes a state channel payment method, which facilitates transactions in a manner akin to traditional banking checks:

1) **Accounts and Deposits:** Each network user maintains an account managed via a smart contract on the Ethereum blockchain. Users deposit a certain amount of value, denominated in PDVN tokens, into their blockchain-managed accounts.
2) **Issuing Promises:** When a user desires to utilize VPN services, they issue a promise to transfer some of their stored PDVN value to the service provider as payment for services rendered.
3) **Clearing of Promises:** Service providers collect these promises and request the execution of a transaction through the PrivacyVPN smart contract. This contract facilitates the transfer of PDVN from the consumer's account to the provider's account based on the accumulated promises.
4) **Netting and Balancing:** All transactions are netted against each other, and the remaining balances are updated and stored within the contract's state. This method ensures efficient management of funds and minimizes the need for frequent transactions.
5) **Withdrawal:** Users can request the smart contract to withdraw a specified amount of PDVN from their account to any Ethereum address of their choosing, providing flexibility in managing their funds.
6) **Risk Management:** To protect against insufficient funds or fraudulent activities, the smart contract verifies each transaction to ensure that the issuer's account has adequate funds to cover the promised value. Similar to a bank refusing a check, the contract will not process transactions if the account balance is insufficient.

5.5.1. Accounts

Users manage their digital wallet accounts through smart contracts, providing security and traceability.

5.5.2. Deposits

Deposits of PDVN tokens are held securely on the blockchain, available for issuing promises or other transactions.

5.5.3. Issuing Promises

Promises act as placeholders for actual payments, allowing service utilization prior to the final transfer of funds.

5.5.4. Clearing of Promises

Promises are converted into actual PDVN transfers through smart contract execution, clearing outstanding balances.

5.5.5. Withdrawal

Users can withdraw PDVN to any Ethereum address, enabling the reallocation or utilization of their funds outside the network.

5.5.6. Risk Management

The system employs checks to ensure that each account has sufficient funds to cover transactions, minimizing the risk of default.

5.6. Messaging Between Nodes

Messaging channels in the PrivacyVPN threads facilitate communication between nodes, employing a variety of channel types based on different carrier protocols and communication schemes. These include direct node-to-node connections, relays via a centralized service, or relays over a peer-to-peer (P2P) overlay network. A dialogue can be initiated over any messaging channel that both participating nodes can access.

The network designates one default messaging channel type with an associated communication protocol, which is supported by all PrivacyVPN client applications. Additional channel types may be introduced as necessary to address and circumvent various forms of information censorship observed in real-time networks.

Implemented messaging channels offer an unreliable datagram messaging interface, and some may support transitive message routing. Due to this, securing the content of communications becomes essential. Each message transmitted is both signed by the sender and encrypted using the Elliptic Curve Integrated Encryption Scheme (ECIES). This encryption method ensures the confidentiality of the message content against eavesdropping, although it does not obscure the identities of the communicating parties, potentially leaving them open to identification.

5.6.1. Dialogues

Dialogues facilitate structured exchanges between two identities (peers), enabling them to coordinate payment for services and to manage service session provisions effectively.

5.6.2. Payment Scheme

[Description of how payments are handled within dialogues, including any protocols or encryption methods used to secure transactions and ensure trust between parties.]

5.6.3. Service Sessions

[Details on how service sessions are established, managed, and terminated within the framework of the network's communication protocols and security measures.]