Particl - Ecosystem of Decentralized and Anonymous Applications

White Paper Draft 0.3

Particl - Ecosystem of Decentralized and Anonymous Applications

White Paper Draft 0.3

Summary

Particl is a parallel ecosystem of privacy-first, pro-freedom decentralized applications building against the centralization of power and services on the web.

United under the mission of shifting the balance of power from corporate monopolies back to the people, the Particl team has designed a comprehensive and anonymous digital platform devoid of any third-party interference, complemented by a native privacy coin to send and receive untraceable currency payments within smart contracts. It is both protocol and currency agnostic, meaning that its modular infrastructure allows developers to use a plethora of protocols and cryptocurrencies to build or interact with their applications.

These dApps — alternative versions of some of the online services and products we use every day — provide the added benefit of operating completely anonymously and without the need for third-party involvement.

In this paper, we go over Particl's network structure, its three core components (blockchain/cryptocurrency, SMSG network, and modular infrastructure), and the various dApps currently in development or production.

The Particl Blockchain

The Particl Blockchain, at the very center of the Particl ecosystem, is built using the latest Bitcoin codebase[1], incorporating all its most advanced developments such as SegWit, the Lightning Network, Taproot, and more. It functions as a privacy-focused financial settlement layer for the ecosystem.

Particl's privacy-oriented blockchain and native cryptocurrency, PART, provide a privacy-focused environment for its applications (dApps) to benefit from untraceable transactions, concealing both the transferred amounts and participants. This capability to perform private transactions, combined with its flexible and oftentimes off-chain smart-contract capabilities (e.g., scriptless scripts), creates a secure and confidential environment for dApps to operate in.

Particl Blockchain's development process is built upon a foundation of continual maintenance with the latest version of Bitcoin, enabling Particl to take advantage of the vast Bitcoin developer network. It provides flexible yet highly secure smart contracts, operating either on-chain (i.e., BIP-65, Taproot scripts) or off-chain (i.e., scriptless scripts), that enable the construction and operation of various dApps within the ecosystem, along with various other protocols.

PART - An Untraceable and Flexible Cryptocurrency

PART is the native cryptocurrency of the Particl Blockchain. It is an untraceable cryptocurrency based on the Bitcoin codebase on top of which several privacy and utility technologies have been added. This allows users to make independent, secure, borderless, and private payments without the need for third-party intermediaries such as banks or payment processors.

PART is also the settlement currency of certain Particl dApps that require complex yet private smart contracts.

Specifications

Native Blockchain	Particl
Codebase Origin	Bitcoin 24.0
Privacy	Confidential Transactions (CT), RingCT, Stealth Addresses
Block Time	120 seconds
Block Size	2 MB
Consensus Mechanism	Particl Proof-of-Stake (PPoS)
Circulating Supply	~12.8M (100%)
Emission Rate	8% per year, decreases 1% per 2 years until it settles at 6%
Segwit	Enabled
Lightning Network	Enabled
Atomic Swaps	Enabled
Taproot	Enabled
Smart contracts	Yes

Bitcoin Codebase

PART is a privacy coin and the native cryptocurrency of the Particl Blockchain. It is built from the Bitcoin Core codebase and is always updated to its latest version.

Using the Bitcoin codebase as the basis for Particl Blockchain allows the platform to benefit from Bitcoin's stability, usability, and security updates. Furthermore, this setup enables developers to take advantage of its large developer community and conveniently fork any of its products, services, and technologies.``

Given its proven track record of security, Bitcoin is the most reliable and robust blockchain technology available. As such, Particl has chosen to build its blockchain on this codebase in order to ensure the highest level of user security and network stability.

Particl Proof-of-Stake

Proof-of-Stake (PoS)[2] is an algorithmic consensus mechanism employed by cryptocurrency blockchain networks to achieve distributed consensus. In PoS-based cryptocurrencies, the creator of the subsequent block is chosen via a combination of random selection of coin balances and aged outputs.

In contrast, Proof-of-Work (PoW) based cryptocurrencies[3], such as Bitcoin, incentivize participants to solve complex cryptographic puzzles to validate transactions and create new blocks (i.e., mining).

Particl Proof-of-Stake (PPoS) is built and improved upon the popular PoSV3 protocol[4], with the integration of several security and utility features exclusive to Particl. It has an annual emission rate of 8% of the total supply, which decreases by 1% every two years until it reaches a steady rate of 6%.

Cold Staking

One of PPoS's most unique and innovative features is cold staking[5]. Cold staking enables users to delegate their coins' staking power to an external node without requiring their wallets to remain online. This offers a heightened level of security for Proof-of-Stake networks, as well as increased flexibility and usability.

By leveraging cold staking, users can store their coins in cold wallets, hardware devices (i.e., a Ledger Nano device), mobile devices, or even by writing the mnemonic on a piece of paper - while still being able to earn staking rewards on those coins even if the wallets are completely offline.

Staking Pools

Similar to mining pools, staking pools enable stakers to pool their resources, enabling them to earn more frequent, albeit smaller, rewards. When the pool validates a block with the combined staking power of all of its stakers, it receives a staking reward.

All of the staking rewards collected by the pool are then proportionally and periodically redistributed to its members according to their share of the pool's total staking power. For instance, if an individual holds 10% of the staking power of the pool, they will be credited with 10% of the staking rewards, minus the pool's fee.

Staking pools are a secure option for stakers, as their operators are unable to manipulate the funds delegated to them. This is so because of the cold staking protocol that powers it, which allows stakers to delegate staking power to a pool node rather than a privately-run node. The security benefits of cold staking remain constant regardless of whether staking weight is being delegated to a private node or a pool node.

Staking pools provide an attractive option for those with limited PART coin holdings or those who prefer to outsource the management of staking nodes.

Voting

PPoS is at the core of Particl's decentralized governance system. Through this mechanism, users can cast votes on community proposals using their staking weight as a measure of voting power.

Voting rounds on Particl are conducted in a decentralized and provably fair manner. Only active stakers, referred to as "stakeholders" in the specific context of an on-chain vote, can cast votes on proposals. Thus, only individuals with a vested and measurable interest in the network can govern its most important decisions.

The process of voting and counting votes is facilitated by the Particl Proof-of-Stake (PPoS) staking protocol, with the results of each round publicly recorded on the blockchain in a permanent manner. This ensures the highest level of transparency and security, rendering any manipulation of past results or misrepresentation of voting results impossible.

The voting power of each individual is determined by their voting preference when they successfully stake a block. At the conclusion of each voting round, all blocks staked in the specified timeframe are analyzed and the votes cast therein are tallied to arrive at the final result. In other words, the more blocks a single staker finds, the more voting power they hold.

PPoS Privacy

By default, Particl's Proof-of-Stake protocol distributes rewards through publicly-recorded transactions, increasing the network's trustworthiness and security by providing transparent, auditable records, thus mitigating the potential for malicious exploits or malfunctions.

However, this level of transparency also means that outside observers can trace staking rewards, and possibly determine a staker's balance and financial information.

To remedy this, Particl has implemented the Partyman staking application, which allows users to choose between public, confidential (CT) and RingCT transactions when receiving staking rewards. This allows users to maintain their financial privacy without compromising the transparency of the coin creation process.

Privacy

While PART is developed on the robust Bitcoin codebase, it also enjoys additional privacy protocols that enable users to send transactions without permanently exposing their financial details to the public or storing them on the blockchain.

The sender has the option to select from three transaction types (**public**, **blind**, and **anon**) to adjust the privacy level of their PART transaction.

	TX Cost	**Amounts**	**Participants**	**Address Type**
Public TX	Very Low	Public	Public	Public
Blind TX	Low	Hidden	Public	Stealth
Anon TX	Moderate	Hidden	Hidden	Stealth

Confidential Transactions (Blind)

Based on the work of the open-source Elements Project, Confidential Transactions (CT)[6] enable users to perform confidential transactions that maintain the value of the payment private between them and the counterparty. This is achieved through a zero-knowledge proofing method that does not necessitate any trusted setup or direct interaction with the other party.

To validate and guarantee that the amounts being sent and received are accurate, the protocol employs a 'range proof'.

Range proofs

A range proof is a cryptographic protocol used to verify that a payment amount is positive or zero, without revealing the exact amount.

Without range proofs, the amounts in a transaction could be set so large that it would be considered a negative number, thus allowing coins to be generated out of thin air. An attacker could add a negative amount output and another different output, generating extra coins. The negative output would make the commitments still sum to zero.

However, range proofs are computationally intensive and can result in significant transaction fees due to their size, which can be exacerbated by the number of range proofs associated with each output. In fact, range proofs constitute the bulk of a blinded transaction's size.

Bulletproofs

To improve the scalability of private transactions and reduce their associated costs, the Particl team integrated Bulletproofs into its blockchain — a new generation of range proofs that scale logarithmically rather than linearly.

The Bulletproofs range proof improvement protocol, which had its name coined by Shashank Agrawal when he described the new type of range proof that is “short like a bullet, with bulletproof security assumption”[7], is referred to as “*non-interactive zero-knowledge short proofs”*. This improvement protocol reduces the size of range proofs by around ~70%, resulting in a similar reduction in transaction fees and the space they occupy on the blockchain.

Stealth Addresses

Particl enables users to employ stealth deposit addresses in lieu of standard, public addresses. Stealth Addresses are one-time addresses that bolster privacy since only the owner can discern whether a given output belongs to them or not. ‘One-time addresses’ refer to the feature of stealth addresses to accept payments multiple times, while generating a new ‘one-time address’ for each output.

Without knowledge of the private key of an address, an observer is unable to link and deduce which outputs correspond to which stealth address. This aids in safeguarding the identity of the recipient of a transaction.

The use of stealth addresses can be seen as a viable means of obfuscating the participants in a Confidential Transaction (CT). However, an observer would still be able to ascertain which inputs were used in the transaction. This could lead to the inference of additional information, depending on the observer's knowledge of the inputs.

To ensure maximum privacy, stealth addresses should be used in conjunction with RingCT, a stronger, complementary privacy protocol.

RingCT (Anon)

By combining stealth addresses, 'ring signatures', and Confidential Transactions (CT), users are able to benefit from a more advanced privacy protocol known as RingCT.[8].

RingCT, originally developed for the Monero private cryptocurrency, is the most private type of transaction available on Particl. It cryptographically obfuscates all associated transaction data, including values transferred and addresses of the participants, rendering it impossible for any entity not involved in the specific transaction to view its details.

Furthermore, RingCT effectively conceals the state (spent or unspent) of the sender's inputs, a feat which cannot be accomplished via stealth addresses or Confidential Transactions alone.

Ring Signatures (MLSAG)

Multilayered Linkable Spontaneous Ad-Hoc Group Signatures (MLSAG), otherwise known as 'ring signatures', constitute the *Ring* component of *RingCT*. It is a form of digital signature that is generated by multiple outputs within a given set of RingCT outputs. This signature structure ensures that no external observer can identify which of the outputs is responsible for sending or receiving funds, thus providing a high degree of privacy.

Ring signatures, as defined by Wikipedia, are

"*a type of digital signature that can be performed by any member of a group of users that each have keys. Therefore, a message signed with a ring signature is endorsed by someone in a particular group of people. One of the security properties of a ring signature is that it should be computationally infeasible to determine which of the group members' keys was used to produce the signature.*"[9].

RingCT employs a digital signature to execute and broadcast a transaction. This signature is generated through a randomized process in which any user with funds in an Anon balance can be selected without manual input. This selection of users results in a signature that appears to have been initiated by any of the owners of the RingCT outputs used in the ring group. As a result, it is not possible to identify the individual who initiated or received the transaction, as it could be any of the ring members.

This effectively anonymizes all values contained within a transaction — the amount transferred, the sender, and the receiver. It also shields transacting parties with strong plausible deniability. An encryption scheme is considered deniable *"if the sender can generate 'fake random choices' that will make the ciphertext 'look like' an encryption of a different cleartext, thus keeping the real cleartext private."*[10]

Private smart contracts

RingCT transactions, due to their lack of programmable outputs, cannot be used in smart contracts natively. However, their outputs and inputs can be linked to CT transactions, which contain programmable outputs and thus, can be used in smart contracts.

This combination of RingCT and CT transactions is a major capability that makes Particl stand out as a dApp platform and a privacy coin. This relationship is what enables the two-party escrow system of the Particl Marketplace dApp, allowing for anonymous online escrow contracts to be opened up between two parties without the need for a middleman.

It also enables a variety of use-cases, such as anonymous swaps on the BasicSwap DEX or the private entry and exit of the Lightning Network.

Taproot

Taproot is a Bitcoin and Particl protocol enhancementt[11] that provides a range of new features and capabilities, particularly with respect to privacy, output management, and smart contract complexity.

The term "Taproot" is often used to denote the combination of three Bitcoin Improvement Proposals (BIPs): Taproot, Tapscript, and Schnorr Signatures. This amalgamation of BIPs broadens the scope of what can be achieved with Particl, while simultaneously enhancing its efficiency, scalability, privacy, and the flexibility of its transactions and smart contracts.

Schnorr Signatures BIP

Taproot can be better understood by gaining a thorough comprehension of Schnorr signature algorithms.[12] At its core, Particl uses Elliptic Curve Digital Signature Algorithm (ECDSA) digital signatures to secure the network, prove the ownership of coins, and validate transactions. While ECDSA digital signatures are secure, open-source, and well-tested, they possess certain drawbacks that Schnorr Signatures mitigate, particularly in the realms of privacy and scalability.

The most notable improvement over ECDSA that Schnorr Signatures offer is the capacity to aggregate multiple keys and signatures into a single key and a single signature per transaction. While ECDSA necessitates one key and one signature for each participant of a transaction, such as with regular multi-signatures, Schnorr Signatures allow for these transactions to only carry a single aggregated key and signature.

This considerably reduces the size of complex transactions and enables the blockchain to verify transactions and signatures in batches instead of one at a time, enhancing efficiency. .

It also significantly improves the privacy of all involved parties by essentially masking their actual key and signature. A multi-signature transaction using Schnorr Signatures appears the same as any regular Particl transaction on the blockchain, obfuscating its actual nature.

Taproot BIP

The Taproot BIP outlines the integration of Schnorr Signatures into the blockchain by modifying Bitcoin scripts and introducing Merkelized Alternative Script Tree (MAST).

MAST is akin to a P2SH script in that it allows multiple Particl scripts to be included in a Particl address. However, MAST transactions differ from P2SH scripts in that the script hash of a single MAST transaction can define multiple scripts at once. When sending PART to a MAST output, the coins are locked into its Merkle root until the user reveals the script required to unlock the coin, as well as the proof that this script is included in the Merkle root of the locking transaction. This unlocking mechanism happens without revealing all of the scripts it contains, thereby improving the privacy of the process compared to P2SH transactions.

Additionally, Taproot introduces Pay-to-Taproot (P2TR) scripts, which allow users to send payments directly into the Schnorr public key or the Merkle root of a script[13]. This allows for script-locked UTXOs to only be unlocked when a user can satisfy the pre-defined conditions inscribed into the Merkle tree of the script.

In essence, Schnorr Signatures enable the creation of complex Bitcoin-style transactions and scripts within Particl's smart contract framework, thus expanding the range of potential use cases. Furthermore, these signatures aggregate complex PART transactions into standard transactions, ensuring the privacy and fungibility of these scripts is maintained.

Tapscript BIP

For Particl Blockchain to support P2TR transactions and scripts, Tapscript is required. Tapscript is a set of operation codes (‘opcodes’) that verify and validate Taproot transactions and Schnorr Signatures[14].

Tapscript can be seen as the scripting language of Taproot. It contains the majority of operations and logic from traditional and Segwit-related Bitcoin scripts, but has some distinct differences. Notably, it substitutes the OP_CHECKMULTISIG and OP_CHECKMULTISIGVERIFY opcodes by OP_CHECKSIGADD and calculates signature hashes differently. It also enables several opcodes that were present in the code but, until now, disabled, making it forward compatible with future, but still to this day unforeseen, upgrades.

Flexibility and Usability

The Particl Blockchain offers a range of flexibility and usability-enhancing features, enabling the PART cryptocurrency to be utilized in dApps, smart contracts, and distributed services while maintaining its privacy and security benefits.

Smart Contracts

The Particl Blockchain is derived from the Bitcoin codebase, thus typically only enabling the deployment of elementary Bitcoin-style smart contracts, in contrast to the more intricate “turing-complete” Ethereum-style smart contracts.

BIP-65 — Simple Bitcoin-Style smart contracts

BIP-65-defined[16] Bitcoin-style smart contracts leverage the OP_CHECKLOCKTIMEVERIFY opcode to script transaction outputs that can only be spent at or after a specific point in time. This allows for the creation of distributed escrow contracts and other 'non-interactive time-locked' transactions to be securely embedded in the blockchain.

Due to their robust and secure design, Bitcoin-style scripting on the Particl Blockchain has enabled the development of innovative applications, such as the Particl Marketplace dApp, without the need for intermediaries. Furthermore, the Taproot series of improvements, along with usage of scriptless scripts, have significantly enhanced their scope and flexibility, significantly broadening the range of possibilities available through smart contracts on Particl.

Taproot Enhancements

Taproot introduces the capacity to script complex logical and condition-based requirements into Bitcoin-style scripts, thereby enabling the development of more sophisticated smart contracts on the Particl Blockchain.

When integrated with scriptless scripts or the SMSG network — Particl's native mixnet detailed later in this paper — it enables the development of privacy-focused dApps with a much lower risk profile than complex, Turing-complete smart contracts, while still allowing for complex and extensive operations.

Additionally, Taproot's capacity to amalgamate multiple signatures, keys, and scripts drastically enhances the privacy of the blockchain's smart contracts and dApps by transforming intricate condition-based transactions into standard-looking transactions. This safeguards the fungibility and financial information of coins transferred through Particl smart contracts and dApps.

Atomic Swaps

Particl utilizes two distinct atomic swap protocols to enable two parties to exchange digital assets between different blockchains, without the need for a third-party intermediary. Both protocols involve three distinct transactions; a ‘lock transaction’, a ‘redeem transaction’, and a ‘refund transaction’.

Hashed Time Lock Contract Swaps

Hashed Time Lock Contract swaps, or HTLC swaps, are based on Decred’s atomic swap protocol[17]. It operates by placing the hash of a secret value into an on-chain script; once the secret is revealed, the swap can be completed.

The Decred project provides an accurate description of the process of conducting HTLC-based swaps:

> “*Atomic swaps involve each party paying into a contract transaction, one contract for each blockchain. The contracts contain an output that is spendable by either party, but the rules required for redemption are different for each party involved.*
>
> *One party (called counterparty 1 or the initiator) generates a secret and pays the intended trade amount into a contract transaction. The contract output can be redeemed by the second party (called counterparty 2 or the participant) as long as the secret is known. If a period of time (typically 48 hours) expires after the contract transaction has been mined but has not been redeemed by the participant, the contract output can be refunded back to the initiator's wallet.*

For simplicity, we assume the initiator wishes to trade Bitcoin for Decred with the participant. The initiator can also trade Decred for Bitcoin and the steps will be the same, but with each step performed on the other blockchain.

The participant is unable to spend from the initiator's Bitcoin contract at this point because the secret is unknown by them. If the initiator revealed their secret at this point, the participant could spend from the contract without ever honoring their end of the trade.

The participant creates a similar contract transaction to the initiator's but on the Decred blockchain and pays the intended Decred amount into the contract. However, for the initiator to redeem the output, their own secret must be revealed. For the participant to create their contract, the initiator must reveal not the secret, but a cryptographic hash of the secret to the participant. The participant's contract can also be refunded by the participant, but only after half the period of time that the initiator is required to wait before their contract can be refunded (typically 24 hours).

With each side paying into a contract on each blockchain, and each party unable to perform their refund until the allotted time expires, the initiator redeems the participant's Decred contract, thereby revealing the secret to the participant. The secret is then extracted from the initiator's redeeming Decred transaction providing the participant with the ability to redeem the initiator's Bitcoin contract.

This procedure is atomic (with timeout) as it gives each party at least 24 hours to redeem their coins on the other blockchain before a refund can be performed.” [18]

Adaptor Signature-Based Swaps

Atomic swaps utilizing the adaptor signature technique[19] enable two parties to securely exchange cryptocurrencies across different blockchains using adaptor signatures, otherwise known as One-Time Verifiably Encrypted Signatures[20], offering far more privacy than HTLC-based swaps. In adaptor signature-based swaps, the initiator is the party initiating the exchange, sending CoinA, and the participant is the other swapper, sending CoinB.

The initiator begins the process by publishing a ‘lock transaction’ in order to exchange an amount of CoinA, which must be a script-enabled cryptocurrency, for CoinB. This lock transaction secures the amount of CoinA being exchanged in an output that can only be accessed if both sides cooperate - otherwise, the initiator could reclaim the funds after the agreed time for the trade has elapsed.

The participant then waits for the CoinA lock Transaction to be confirmed and, if satisfied, publishes his own transaction, locking up the CoinB being exchanged. The CoinB lock transaction outputs to a key, which is the sum of that of the initiator and the participant. Here, it is spendable only using One-Time Verifiably Encrypted Signatures, which require knowledge from both participants of the swap.

Once the initiator is satisfied with the CoinB lock transaction, they reveal information to the participant, which allows them to spend from the CoinA transaction. The participant then spends from the CoinA lock transaction, which discloses information to the initiator, also allowing them to spend from the CoinB lock transaction. If one of the parties abandons the process, the other can reclaim the coins from their side of the trade.

In addition, both parties create a 'refund transaction' that can be spent either by both parties cooperating, or by the participant after a certain period of time. The initiator will be aware of how to spend the CoinA Refund transaction immediately after publishing it, but the participant can also construct the CoinB Refund transaction using the information from CoinA's refund transaction.

This swap style differs significantly from the previous in terms of privacy. In fact, using HTLC-based swaps, it is possible for an external observer to deduce who the two participants are, as well as trace swapped amounts and associated data, by simply analyzing blockchains passively.

When executing HTLC-based swaps, a hash of the swap is permanently inscribed in the two participating blockchains at similar timestamps. For an observer with sufficient motivation, it is then relatively simple to match two transactions and infer that a swap happened, along with all related information, solely based on the presence of an identical hash on both blockchains.

Adaptor signature-based swaps offer a solution to this privacy vulnerability by transferring the hash generated from a swap off-chain. This ensures that the details of the swap are only accessible to the two participants, making it impossible for external parties to gain any insight.

Scalability

With the adoption of its dApps in mind, the Particl Blockchain boasts a range of scalability features and protocols that enables it to accommodate a vast number of users concurrently.

Segwit

Particl is natively Segwit-compatible, meaning

> *"its witness structure is committed to blocks separately from the transaction's Merkle tree. This structure contains data required to check transaction validity but not required to determine transaction effects. In particular, scripts and signatures are moved into this new structure.*
>
> *The witness is committed in a tree that is nested into the block's existing Merkle root via the coinbase transaction, for the purpose of making Segwit soft fork compatible. A future hard fork can place this tree in its own branch."* [21]

This protocol improvement, introduced by BIP-0141, keeps the size of Particl transactions unchanged by removing certain types of data from the transaction structure "committed to the transaction Merkle tree". Notably, it ensures that Segwit transactions have the same transaction ID when signed and unsigned, thus allowing the protocol to create chains of transactions spending the outputs of unsigned transactions[22].

Segwit also offers further advantages, such as eliminating the potential for unintentional transaction malleability, optional transmission of signature data, and the prevention of soft fork circumvention of certain blockchain rules.

Taproot, Adaptor Signatures, and Scriptless Scripts

Taproot's aggregation of signatures, keys, and scripts optimizes the scalability of Particl smart contracts by condensing a plethora of data points into a single value. Moreover, adaptor signatures and scriptless scripts enable "off-chain scripts" and smart contracts to operate, thereby limiting the amount of data stored on the blockchain and making related Particl transactions as streamlined and lightweight as regular transactions.

Lightning Network

The Lightning Network[23] (sometimes simply dubbed LN or LND) is a layer-2 protocol introduced in BIP-112 that improves the scalability shortcomings of 'layer 1' blockchains. Because LN-related data, logic, and processes happen exclusively off-chain (except for entry and exit transactions), payments are near-instantaneous, near-free, and do not leave any data on the blockchain itself.

Similar to blockchains, the Lightning Network is a decentralized network of nodes that validate transactions. However, unlike Particl Blockchain, transactions are not broadcast to a public ledger, nor do they need to be stored by all participants in the network. Instead, peers transact with each other privately and directly through dedicated “channels”.

Particl Governance — A Decentralized Autonomous Organization (DAO)

The Particl network is, fundamentally, a 'decentralized autonomous organization' (DAO). This type of entity does not possess any central authority, but instead is designed to be self-governing, self-sustaining, and transparent. The distributed structure of the network removes any single point of failure, enhancing its resistance to external interference, malicious attacks, and other forms of agenda-driven behavior.

Decentralized Treasury and Network Income

To stimulate the development of dApps, distributed services, and the overall growth of the network, Particl is supported by its own decentralized treasury fund which automatically receives 50% of the staking rewards generated by the blockchain. This staking income is hard-coded directly into Particl Proof-of-Stake (PPoS) and is entirely decentralized.

Circulating PART Supply	~12,800,000 PART
Yearly PART Emission Rate	8%
Share Attributed to the Treasury	50%
Average Monthly Treasury Income	~40,900 PART

Every month, the Particl network's decentralized treasury receives a number of PART coins which can be utilized to fund decentralized applications, distributed service providers, or any other community-driven initiative that furthers the development, adoption, and/or sustainability of the ecosystem.

Treasury Fund Management

Funds allocated to the Particl network's treasury are held in a 3-of-5 multi-signature address administered by various members of the Particl team. These funds can only be apportioned to individuals or teams (‘proposers’) with approved proposals obtained through a blockchain-based voting system. Funds cannot be distributed without the explicit and demonstrable approval of Particl's stakeholders.

This multi-signature-based approach to the treasury's fund management has been implemented to provide a safety measure while the team gradually decentralizes the process of fund allocation, notably with the help of Taproot and its condition-based scripting language.

Community Governance (CCS Platform)

The Community Crowdfunding System (CCS) is an open-source, transparent platform hosted on the Github repository, enabling Particl's community of stakeholders to freely publish, discuss, and vote on proposals.

Publication Process

To prevent abuse of the system, the CCS platform is actively managed and moderated by the Particl team. While this introduces a certain degree of centralization into the governance system of the platform, it helps foster an open but pertinent space for the publication of ideas and for contributors to freely discuss their vision within the context of Particl’s own benefits.

This moderated approach aims to simultaneously promote free discussion and protect the network from ill-intended actors, spam, and proposals that may be harmful to the network. It also provides a last line of defense and a layer of protection against abuse of the system while the team incrementally works on a fully decentralized approach to the governance of the network.

Proposal Types

Particl's voting rounds are conducted within a framework of decentralization, transparency, and verifiable fairness. These voting rounds are limited to active stakers, known as “stakeholders” in the context of on-chain voting, thus guaranteeing that only those with a verifiable stake or interest in the network are able to make the most crucial decisions.

The process of voting and counting votes leverages the Particl Proof-of-Stake (PPoS) staking protocol, and every round's results are publicly inscribed on the blockchain permanently. This provides the maximum level of transparency and security possible, making it impossible to modify past results, misreport voting outcomes, or game the voting mechanism.

In order to calculate each individual's voting power, the voting preference of a staker is only taken into account when they successfully mine a block. Subsequently, at the conclusion of a voting round, all blocks that were mined within the voting round's timeframe are evaluated, and those that cast votes are added to the overall count. To put it another way, the more blocks a single staker mines within the duration of a voting round, the more votes they record and, as a result, the greater their effect on the ultimate outcome.

The voting rules and parameters differ in accordance with the type of propositions being voted on.

Non-Protocol Consensus-Changing Proposals

Quorum	20% of all the blocks during a voting period
Approval Rate	>= 60% in favor
Duration	5,040 blocks minimum

The first type of proposal, non-protocol consensus-changing proposals, does not suggest significant changes to the protocol. Commonly, these proposals may request financial support from the treasury to fund or kickstart a particular project, such as the development of a dApp or the introduction of a distributed Particl service.

In order for a non-protocol consensus vote to be considered valid, the voting period must be 5,040 blocks in length (roughly one week). During this period, at least 20% of the blocks staked must cast a vote, including abstentions. This implies that the quorum must be no less than 20%.

For the proposal to receive approval from the community, it must reach an approval rate of at least 60%, meaning that at least 60% of the votes cast must be in favor of the proposed idea.

Protocol Consensus-Changing Proposals

Quorum	20% of all the blocks during a voting period
Approval Rate	>= 75% in favor
Duration	10,080 blocks minimum

Proposals that require a specific change to the protocol, such as modifying the inflation rate or introducing a new privacy technology, are known as protocol consensus changing proposals. These types of proposals are typically more critical in scope, and can have a significant impact on the blockchain ecosystem.

The quorum requirement for these types of proposals is set at 20%. However, due to their increased level of importance, they require a higher level of approval from the community, with a minimum approval rate of 75%. Furthermore, in order to ensure that all members of the community have a chance to cast their vote, the duration of any protocol consensus vote must be at least 10,080 blocks (roughly two weeks)."

Low-Level Governance

The Particl blockchain, like all UTXO-based blockchains, features a low-level governance mechanism that supersedes its integrated proposal and on-chain voting system. This is due to the fact that certain fundamental alterations may not be compatible with the current version of the blockchain, in which case a hard fork must be initiated.

A hard fork is a permanent divergence in the blockchain caused by a protocol change, resulting in two separate blockchains. In the case of Particl, stakers must choose between the legacy blockchain and the new version, which is typically done by installing and staking on the updated core client. The chain which has the majority of stakers (usually more than 50%) will become the dominant one, unless both chains can sustain a sufficient number of stakers, as observed in the Bitcoin/Bitcoin Cash split, in which case they may co-exist in tandem.

Ultimately, governance power falls into the hands of the network's stakers, who are free to stake either version of a blockchain following the decision to implement protocol-changing updates. Moreover, stakers can decide to implement changes by themselves and collectively start staking their own versions of a blockchain. This consensus-based governance model is of the utmost level of decentralization and is the network's last line of defense against any sort of subversive or ill-intended actions by any party who may otherwise overtake or abuse Particl's on-chain voting system.

Staking Rewards

Particl stakeholders can generate revenue through the process of staking, which involves validating transactions on the blockchain in order to maintain its integrity. As a reward for their efforts, the network dispenses staking rewards in the form of its native cryptocurrency coin.

A staking reward, which is denominated in PART coins, is a reward received from the Particl Blockchain for securing the network. The reward consists of two components: the base reward, which is the number of PART generated by the blockchain at each block, and the platform's usage fees which are determined by the level of activity on the network.

Base Staking Rewards

Particl's current annual emission rate is 8%, with 50% of the block rewards allocated to the network treasury. This results in an estimated annual staking yield between 4% and 8% for stakers.

As the rate of return is subject to various determinants, including chance, it is impossible to accurately forecast the amount of reward a staker will receive in a year. Nevertheless, if the node is kept running 24/7, a minimum of 4% yearly interest is assured.

It’s important to note that this guaranteed 4% yearly staking interest is only true if 100% of the total supply is put up for staking. The smaller the percentage of the network being dedicated to staking, the larger the individual rewards become. As a general rule of thumb, the actual yearly staking interest can be estimated with the following formula:

Projected yearly staking interest rate = X * (Y / 2) / Z

X = Balance held by the staker

Y = Yearly staking interest rate (currently 8%)

Z = Percentage of the total supply being actively staked

Platform Usage Fees

In addition to the base rewards, any PART fees incurred by active users of the network when utilizing the PART cryptocurrency or certain dApps are included in the staking reward of the respective block.

As a result, the staking profitability of the network increases proportionally with the growth of usage and adoption of the Particl platform.

Transaction Fees

When a PART transaction is executed with another person or a smart contract, a nominal fee is required to be paid to the network. This fee is usually quite minimal, typically amounting to a few cents or less, and serves as a deterrent to prevent spam on the blockchain. A staker who successfully stakes a block containing PART transactions will be rewarded with the entirety of the fees generated by it.

DApp-Related Fees

In addition to the customary cryptocurrency transaction fees, any Particl dApp that utilizes the SMSG network, be it developed by the Particl team or a third-party, may levy a usage fee.

Such is the case with Particl Marketplace which utilizes the SMSG network to store marketplace-related data. To discourage spam, a product listing fee is imposed and the revenue is allocated to stakers. Similarly, sellers can promote their markets and storefronts through the SMSG network, however, they must pay a fee to stakers for this service.

Any present or prospective Particl dApp could necessitate corresponding interaction with the SMSG network. As the network's potential for utilization and the diversity of its available dApps are expected to expand, the collective amount of fees paid by the network's users is likely to rise, thus resulting in higher staking rewards.

SecureMessaging Network (SMSG)

While smart contracts are employed to facilitate certain aspects of Particl's dApps, the platform differentiates itself from other dApp networks via its utilization of an auxiliary peer-to-peer (P2P) network, SecureMessaging (SMSG)[24].

Particl's native, custom-built P2P messaging network, SMSG, complements the network's use of smart contracts, enabling dApps to execute more intricate actions. It provides a decentralized and secure data transfer layer for dApps to leverage, making active and passive network analysis unsuccessful. In contrast to complex Ethereum-style smart contracts, which typically run through VM machines on centralized third-party nodes, the majority of Particl dApp users are SMSG nodes, thus guaranteeing an optimal degree of decentralization.

As a result, sophisticated applications that do not rely on intermediaries, and where data extraction is rendered infeasible, can be developed, without the need for convoluted smart contracts that may leave security vulnerabilities exposed to malicious actors.

Privacy specifications

Drawing inspiration from the BitMessage protocol[25], the SMSG network is a privacy-first decentralized storage network (DSN) that facilitates the secure, private transmission and storage of data across nodes while leveraging end-to-end encryption (E2EE) and avoiding the need for a central entity or server. Encryption is accomplished through the use of 256bit AES in cyber block chaining[26] (“CBC”) mode[27], with each message additionally covered by a Message Authentication Code (MAC) to guarantee that the decrypted content has not been altered[28]. Moreover, an Elliptic Curve Digital Signature Algorithm (ECDSA)[29] signature is included in each message to verify its originator.

To ensure the utmost security, SMSG utilizes a newly generated random key for each message, which is then divided and used to initialize the AES cipher and MAC algorithm.[30]

SMSG Usage

SMSG performs a number of pivotal roles within the Particl network, and its utilization is anticipated to expand as more decentralized applications and distributed services are integrated into the platform.

Data storage and transmission: The network enables the secure storage and transfer of a wide variety of data from one user to another, or to the entire network, in an encrypted and decentralized way. At all times, the identities of the sender and receiver(s) of the data remain anonymous to unauthorized individuals, and there is no need for servers at any stage of the process."

Secure communications: The SMSG network facilitates secure communications between two or more parties by providing an instant messaging protocol that does not rely on any centralized servers. All messages are encrypted using end-to-end encryption, thereby ensuring that no unauthorized party can decrypt the data.

Execute smart escrow instructions: The Particl Marketplace dApp features a two-party escrow system which is based on a streamlined Bitcoin-style smart contract. Rather than coding multiple functions and conditions into the smart contract, which can introduce a range of potential vulnerabilities, the Particl smart contract instead receives instructions from the SMSG network based on the actions of the users. This simplification of the smart contract process reduces the likelihood of vulnerabilities, while the complexity of escrow interactions is offloaded to the SMSG network. In the realm of smart contracts, simplicity is a crucial factor for security.

Host dApp content: Due to the potential for blockchain bloat caused by the direct on-chain hosting of dApp-related data (i.e., marketplace product descriptions and images), Particl dApps take advantage of SMSG's private data storage capabilities to store and deliver this information efficiently.

Host dApps and Pages: SMSG 2.0, currently in development, offers capabilities akin to the Tor network or i2p, allowing for the hosting, browsing and utilization of dApps and pages without the need for access to the World Wide Web (http/https/clearnet). This makes the content hosted on the network independent from the traditional web infrastructure, and more resilient to potential attacks or vulnerabilities. Moreover, due to the inherent privacy of SMSG, the content hosted on and accessed from it is provided with the utmost level of data security and privacy.

Enable complex DEX with orderbooks: Atomic swaps and the SMSG network enable the development of decentralized exchanges (DEXs) with comprehensive order book capabilities, without the need for central intermediaries to store and process the data. Atomic swap technology enables two users to exchange cryptocurrencies without the intervention of a third party. However, a secondary messaging layer is required to transfer data between chains without the use of wrapped assets or intermediaries, which is where the majority of the difficulties surrounding cross-chain DEXs are encountered. SMSG assumes the role of securely and confidentially aggregating the pertinent information (order details, prices, user actions, etc.) and facilitating communication between users on different blockchains, such as Particl, Bitcoin, and even Monero.

Modular Architecture

Note: *The following section outlines the currently ongoing development cycle of the project. Accordingly, the specified modularity architecture and upcoming developer SDK toolkit are currently in development and have not yet been implemented in a live environment.*

Development Modules

In order to expedite and facilitate the development of Particl dApps, the services and functions supplied by the Particl environment are compartmentalized into independent components, deemed “modules”.

These modules offer a standardized set of features that can be employed by developers when creating Particl dApps. Instead of contributors needing to program and re-execute every Particl function from the ground up, they can simply import a module or library featuring that module to obtain the desired functionality.

This concept is analogous to mobile development where app developers utilize permissions to provide specific functionalities to their applications. For instance, when a mobile application necessitates access to the camera, it merely requests permission to employ the built-in and standardized functionality provided by the Android or iOS system itself, rather than having this coded from scratch.

In the context of Particl, should a dApp require a feature provided by one of the developer modules (such as the instant messaging feature of SMSG, for example), it can simply query the service by connecting to the pertinent module. This significantly hastens the development of decentralized and private applications within the Particl ecosystem.

SDK Toolkit

If the modules are building blocks that allow developers to integrate standard functionalities into their dApps quickly and efficiently, the SDK toolkit is the glue that binds them together.

The upcoming SDK toolkit provides a comprehensive and useful set of tools for developers to efficiently put dApps together. The SDK toolkit includes tools such as service modules, application modules, and a backbone “eventing” module, which underpins inter-app communication, among other capabilities.

Third-Party Integrations

Particl dApps and features adopt a modular and nested architecture. Thanks to the ecosystem's upcoming SDK toolkit and modular evolution, virtually any dApp, feature, or functionality can be encapsulated into modules that can then be integrated into other dApps or third-party services.

For instance, Particl's two-party escrow system, which provides trade security, is a module integrated into the Particl Marketplace dApp. It can also be integrated into a WooCommerce plugin, enabling any WooCommerce-based web store to send and receive cryptocurrencies while securing these transactions without the need for intermediaries.

Particl's modular design, its Software Development Kit (SDK), and the Community Crowdfunding System (CCS) platform facilitate the creation of private and secure decentralized applications (dApps) that prioritize user rights while embracing a Decentralized Autonomous Organization (DAO) model.

Modular and Developer-Friendly Environment

Particl is a user-friendly ecosystem that facilitates the development of privacy-focused and secure dApps that do not require third-party involvement.

The network's user-friendly and adaptable nature is largely attributed to its modular architecture and comprehensive SDK toolkit, which also provide a multitude of other advantages.

Sandbox-like Modules

Particl's dApp network boasts a powerful modular architecture. Rather than necessitating the hardcoding and replication of critical functions in every dApp, smart contract, or service, they are isolated in sandboxed and independent modules which developers can access to provide their dApps with the desired functionality.

This approach enables developers to concentrate on the special features and capabilities of their applications, rather than needing to re-implement Particl-specific functions.

To better illustrate this concept, Particl dApps can be likened to mobile applications on Android or iOS. When mobile developers require camera-related features, they do not need to reproduce the entire logic within the app. Instead, they simply query the modular functionality provided by the OS itself via 'permissions'. Once the user grants the camera-related permission to the app, it can then leverage the basic camera functionality on which unique app-specific features or functions are added. Particl dApps operate in a similar fashion; instead of developers having to reinvent basic Particl-related features (i.e., user-to-user mixnet messaging capability), the dApp can simply connect to the Particl module, which provides the built-in functionality out-of-the-box.

Independent Maintenance

Particl’s modular architecture enables dApp developers to build and maintain products independently from the Particl team according to their own terms and conditions.

DApp updates, such as integrating new features or bug fixes, can be rolled out as soon as the author feels they are ready without needing to consider an entire client update or get the core Particl development team involved.

That’s because updates are applied directly to the modules that provide specific functionality instead of the framework that hosts the dApp, such as Particl Desktop.

For example, if a dApp uses a Tor module for anonymous routing, there is no need for a full ecosystem update each time Tor pushes a network update; rather, the update is automatically applied to the module, thus ensuring the Particl dApp remains up-to-date with the latest Tor security patches.

Once a module is updated by its maintainer, the application that makes use of it automatically starts using the most up-to-date version, ensuring a maximal level of security. This allows the Particl ecosystem to thrive independently of the Particl team and third-party contributors to manage their dApps without friction.

Nested Design

Particl's modular architecture is structured in a nested fashion, allowing for functions and decentralized applications to be segregated into different modules at various levels of abstraction. In other words, it is possible to compartmentalize a complex dApp into a single module (i.e., Particl Marketplace or BasicSwap DEX), but it is also feasible to isolate certain features of the dApp into independent modules which can be used by other dApps or services.

For instance, Particl Marketplace, a module in itself, utilizes Particl's messenger dApp module to provide communication capabilities between buyers and sellers. This messenger dApp, in turn, relies on the SMSG messaging function module, which operates at a more macro level.

Particl modules therefore vary greatly in terms of their macro/micro levels, and can interact with each other to create increasingly complex yet secure dApps and distributed services.

Access Gateways

Particl's 'access gateways' are the larger frameworks that enable users to access and interact with decentralized applications (dApps). These may take the form of desktop or mobile applications, websites, or pages/dApps hosted directly on mixnets and Decentralized Storage Networks (DSNs) like SMSG.

Depending on the access gateway, it may host a single dApp (e.g. a dApp-specific mobile application) or multiple dApps (e.g. the Particl Desktop client). The SDK toolkit contains all the necessary tools for developers to integrate and/or deploy their dApps to the access gateway(s) of their choice, depending on the specific use-case.

Particl Desktop

Particl Desktop is Particl's official access gateway, enabling users to interact with multiple decentralized applications (dApps). Through the future use of a dApp store, users can independently add, configure, and remove dApps, and their maintainers can update them without any assistance from the Particl team or maintenance/update requirements from the access gateway (Particl Desktop).

Particl Desktop serves as a means for independently managing various dApps on a user's local machine. Each dApp is a separate entity, accessible and interactable within the client. The general idea is to have a larger framework which functions as a hub by hosting and managing other apps created with the SDK.

DApp Store

Whereas a centralized store of applications for the Desktop client is not a desirable approach from an open and decentralized perspective, a library of "curated" dApps, managed by the gateway's (Particl Desktop) maintainers, will allow users to easily install and manage dApps from other sources as they deem necessary.

In addition to the curated list of dApps, users can also access a wide range of dApps and modules generated by the community, which offer a variety of functionalities and cater to specific requirements. This effectively transforms Particl Desktop into a private and distributed operating system-like platform that facilitates the usage of user-friendly dApps.

Agnostic Design

Particl's modular architecture has been designed with a focus on agnosticism. In the context of information technology, this term refers to the ability of a system to interact with a variety of other systems.

This is especially pertinent for Particl, as its modular architecture enables it to utilize multiple protocols to power its decentralized applications, as well as to work with a wide array of currencies.

Protocol Agnosticism

Particl's modular architecture facilitates the integration and utilization of outside protocols, networks, and services in Particl dApps, thereby broadening the scope of potential applications.

This protocol-agnostic approach enables developers to employ modules that interact with a variety of protocols, such as storage networks, mixnets, messaging protocols, exchange/swap capabilities, payment gateways, identity management, and much more, granting them an almost limitless range of options.

Currency Agnosticism

Much like Particl’s protocol agnosticism, modules can be leveraged by dApp developers and service providers to incorporate different currencies (cryptocurrencies) into their products.

Although PART is necessary for many dApps to function as designed, particularly for intricate, privacy-focused smart contracts such as the two-party escrow system of the Particl Marketplace, simpler dApps may prefer to support multiple cryptocurrencies. This is notably the case with stablecoins — cryptocurrencies that have a relatively stable value — in cases where payment stability may be desired.

This approach furthers Particl's dedication to openness and unrestricted access by enabling the ecosystem and its dApps to reach a broader user base and accommodate more communities and use-cases.

Particl Decentralized Application (dApps)

In addition to offering modules and resources for external developers to create and deploy privacy-first dApps, the Particl team is also working on building a few of their own. These dApps not only provide essential services to the network, but also serve as benchmarks of the potential and scope of what can be accomplished on and with Particl.

Particl Marketplace

Particl Marketplace is the first decentralized application released by Particl. It is a privacy-first, two-sided marketplace network that enables users to directly trade goods and services without any intermediary or limitation. Additionally, this module serves as a network in which anyone can anonymously create and join multiple storefronts or community markets. These can be made public or kept private, broadening the dApp's potential applications and affording users greater personalization.

Trades between two individuals are completely free of charge, requiring no sales or subscription fees, and are secured by a two-party online escrow system based on the Mutually Assured Destruction (MAD) game theory principles. Moreover, payments for products and services available on the marketplace are anonymous by default when using the PART cryptocurrency.

As with any official Particl dApp, no server, central database, or staff is required to keep the marketplace up and running — any use of a module that entails centralized services would need to first be manually approved by the user. Instead, it relies on an intricate combination of distributed technologies developed, maintained, and run by a vast and global network of participants.

Particl Marketplace is:

- **Autonomous** — operates independently of any human intervention;
- **Secure** — maximal level of digital security provided by trustless encryption;
- **Private** — no personal data is ever collected or generated, ensuring complete privacy;
- **Resilient** — immune to censorship or termination by any entity;
- **Bias-free** — no predefined rules or policies, and no ban on items;
- **Near-zero fee** — only pay the bare minimum for the network to sustain itself.

Particl Marketplace — Backbone in a Nutshell

The Particl Marketplace dApp uses the Open Market Protocol (OMP) to connect and interact with the Particl Network, which comprises the Particl Blockchain and the SecureMessaging (SMSG) network. Fundamentally, the OMP library is a standardized and open format containing most of the economic interactions of an online marketplace. The OMP is available as an open-source protocol on Particl's Github page[31] and is licensed under the terms of the MIT license.

By default, the blockchain executes and verifies financial transactions using its native and untraceable currency, PART, ensuring these transactions remain private and secure. Other cryptocurrencies, such as Bitcoin, are intended to be compatible with Particl Marketplace, but using any cryptocurrency other than PART may diminish the privacy of transactions conducted on the marketplace.

On the other end, the SecureMessaging (SMSG) is responsible for processing and securely broadcasting all non-financial data related to the decentralized marketplace to the rest of the network. This is achieved via 256bit AES encryption in cipher block chaining (CBC) mode[32], eliminating the need for any intermediary and hosting service.

Marketplace Content

Storing data on-chain is inefficient and can lead to a rapid expansion of the size of a blockchain. Furthermore, it can lead to risks in terms of what may become permanently embedded on the public ledger, which all participating nodes must keep a copy of on their respective machines.

That is why all marketplace-related data is instead stored on the SMSG network, where it lives for a finite amount of time, as defined by the user, after which it is permanently removed from the network. This includes marketplace listings, their descriptions and associated images, and any other market-related data.

User Markets and Storefronts

Particl Marketplace is not limited to a single, large marketplace; rather, it is a broad network of markets and storefronts that any user can create. Moreover, these user-generated markets can be made public, allowing anyone to access them through the "Market Browser", or kept confidential, granting access only to those with the corresponding access key and allowing them to decrypt its contents.

Within a market, any user with access can either post listings or purchase any of the available products. Conversely, storefronts are owned by their creators, implying that only they and those to whom they explicitly provide the access key can publish listings. Other users without publishing privileges but with access to the storefront can buy any of the listed items.

Any market or storefront-related data, including its description, image, and the listings they contain, is hosted on the SMSG network and disseminated to the rest of the network. This data is encrypted with the market or storefront's key (private key), meaning that only those with its access key (public key) can decrypt the market's content and gain access.

Listings

Individual listings operate similarly to markets and stores. All listings on Particl Marketplace, including their descriptions and images, are hosted on the SMSG network for a predetermined period of time, as determined by the seller. The seller must pay an anti-spam listing fee that is equal to the size of the message multiplied by the number of days it is available on the marketplace. The listing fee rate is determined by Particl Blockchain stakers, who can vote for their desired fee target rate each time they stake a block. The formula to calculate listing fees is as follows:

(Current Listing Fee Rate in PART * Listing Size (in KBs) * Number of Desired Listing Days = Total Number of PART for X Listing Days

i.e., 0.0005 * 243 * 7 = 0.8505 PART

In order to decrypt the individual listings of a private market or storefront, a user must possess the encryption key. Therefore, if a user transmits information from a private market to another peer who does not have access to it, the peer will be unable to decrypt the data or comprehend its content in any way.

Content Moderation

Particl Marketplace is an entirely decentralized application, meaning no single entity has the authority to moderate its contents. Nevertheless, the network still requires the capability to prevent and remove spam, attacks, and any other harmful or undesirable content.

This moderating functionality is present within Particl Marketplace, but instead of being delegated to a central authority or group of policy-applying moderators, it is put into the hands of the stakeholders of the network itself. Using Particl community governance's mechanism, users can upvote or downvote listings based on their own personal preferences using their coin balance as voting weight. Upon reaching a certain downvote threshold, the listing is then removed from the user's client.

This threshold can be adjusted by the user without any external interference, thus preventing any form of censorship, sanctioning, or bias from impacting the marketplace's content and user experience.

User Communication

The SMSG network facilitates communication between buyers, sellers, and potential customers. Allowing users to ask questions prior to making a purchase, address issues with an order, and provide post-sale services are essential components of any online marketplace. The messaging system of Particl Marketplace utilizes the SMSG network to transmit messages between users. Each listing has both a public chat room, where users can ask the seller questions, and the messages posted in this chat room are visible to all.

There is also a private chat room, which is only accessible and visible to the participants of an active market order. All communications initiated in this manner are securely encrypted and anonymous, as no third-party or middleman can intercept and decrypt a message which is not intended for them. All messages are propagated through the SMSG network, and never pass through a central server.

Two-Party Escrow

The Particl blockchain provides a secure and reliable platform for two-party escrow smart contracts. When trading with unknown parties, it is essential to ensure that the agreement is upheld and that both parties act in good faith. This is why contract security and enforcement are so important in any marketplace.

In traditional escrow, a third-party (the escrow agent) holds the asset until the transaction is completed (i.e., the purchased item is delivered). This role is often assumed by the marketplace or exchange (e.g., Amazon), a payment processor (e.g., Paypal, Visa), or a third-party escrow service (e.g., a bank or a financial institution). This offers a degree of protection to both users, but also comes with significant drawbacks.

Issues With Traditional Escrow and Trade Assurance Models

Firstly, the cost of running escrow or dispute resolution services is reflected in the platform's fees and can have a noteworthy effect on retail prices when integrated into the supply chain.

Moreover, when a conflict arises, it is typically settled in accordance with a rigid set of regulations rather than being handled on an individual basis. This often allows for a more expeditious resolution of disputes, but can also lead to prejudiced decisions that are advantageous to the operator's own financial interests. Fraudsters have also become adept at circumventing these inflexible protocols to steal money, goods, or both, from compliant users. Online merchants are aware of this bias and mitigate their risk by adjusting their prices accordingly, resulting in higher costs reflected onto the consumer.

Furthermore, these solutions offer no privacy to their users and necessitate intrusive data requirements, as the operator needs to be aware of all the details pertaining to a single transaction to fulfill its role. This gives them full oversight and insight into all the sensitive, and at times confidential, personal, professional, financial, and commercial data collected from the platform's users — which they can then use in accordance with their own interests, often to the detriment of the individuals and businesses using the platform.

Particl’s Two-Party Online Escrow Solution

Particl has developed a distinct and radically different two-party escrow system that resolves the aforementioned issues.

This system requires only two participants, the buyer and the seller, to deposit an equal amount of collateral into a smart contract. After both parties have marked the transaction as complete, the security deposits are refunded in full.

In the event of a dispute, both parties must agree on a satisfactory resolution for the transaction to be finalized, otherwise both security deposits remain locked in the smart contract. This financial approach is analogous to the Mutually Assured Destruction military doctrine, which encourages collaboration and a reasonable outcome for all involved.

Mutually Assured Destruction Game Theory

Game theory can be defined as the study of mathematical models of strategic interaction between rational decision-makers. This field of study is used to incentivize rational behavior and to discourage irrational or dishonest behavior. Particl implements the Mutually Assured Destruction (MAD) game theory in a financial context to achieve this outcome in a two-party escrow system.

MAD is a military doctrine that is based on the theory of deterrence, *which stipulates that the threat of using strong weapons against the enemy prevents the enemy’s use of those* *same weapons. The strategy is a form of Nash equilibrium in which, once armed, neither side has any incentive to initiate a conflict or to disarm".*[33]

It can be succinctly stated that when two entities possess the same capacity to inflict equal damage upon one another, there is no motivation to initiate an attack, as such an action would likely be met with a retaliatory strike of equal intensity. Consequently, this encourages cooperative behavior and discourages any hostile behavior.

BasicSwap DEX

BasicSwap DEX is Particl's decentralized, trustless trading exchange platform, utilizing atomic swap technology, adaptor signatures, and the SMSG network to enable users to exchange cryptocurrencies without fees, restrictions, or prerequisites such as invasive identification or proof of income requirements.

This platform was created in direct response to the impending threats to freedom posed by the current landscape.

BasicSwap — Backbone in a Nutshell

BasicSwap leverages multiple technologies to provide users with a fully-fledged decentralized trading exchange experience.

Atomic Swaps

Atomic swaps have been a part of the cryptosphere for some time and are a prominent feature of many decentralized exchange (DEX) platforms. These swaps enable two users to exchange digital assets in a peer-to-peer fashion, provided that complementary, necessary infrastructure is in place.

The atomic swap protocol is a relatively focused technology, as it does not match orders between two users or provide any DEX framework; it merely facilitates the safe exchange of assets.

For a DEX to be fully operational, a decentralized channel is needed to transmit information between two parties, often across two distinct blockchains. Without this additional layer, it is impossible for one chain to know when to release the swap as it is not directly linked to the other blockchain. In the case of BasicSwap and the Particl ecosystem, this is where the distributed SMSG network comes into play.

Usage of SMSG

SMSG technology is essential in providing the BasicSwap DEX with functionalities not provided by atomic swaps, such as an order book, order matching system, and with transferring swap data between users of two different chains.

By running a BasicSwap client, users also run an SMSG node, thus maintaining a high level of decentralization by ensuring every user is also a network node. All adaptor signature-based swap data is uploaded and downloaded directly from the SMSG network and interpreted via BasicSwap's support for scriptless scripts, providing users with a comprehensive decentralized trading exchange (DEX) experience.

Usage of Adaptor Signatures

BasicSwap leverages a type of off-chain smart contracts powered by adaptor signatures to safely spend coin outputs collaboratively and without third-party involvement.

When swapping assets using BasicSwap's adaptor signatures, the participants' coins are sent to an output created from the sum of both users' private keys. The only way to spend that output requires them to cooperate through One-Time Verifiably Encrypted Signatures (OtVES), or adaptor signatures — a type of "*signature made invalid by mixing it with the public key of an encryption key pair whereas a valid signature can be decrypted with knowledge of the private encrypting key and the private encrypting key can be recovered with knowledge of both the encrypted and plaintext signatures.*"[34]

Protocol Agnosticism

The BasicSwap protocol, much like most Particl dApps, is built with protocol agnosticism in mind, meaning that modules that are part of its protocol can be substituted by others. This is especially relevant for the swap and order book data transmission layer, which is currently managed by the SMSG network, but can be replaced with alternative solutions that may offer enhanced scalability, privacy, or efficiency.

This characteristic of the DEX, and of Particl dApps in general, ensures that the service remains up-to-date with the latest technological advancements and retains its relevance for a prolonged period of time.

BasicSwap as a Protocol

While BasicSwap is available as a trading platform dApp, on which users can swap by making and taking orders from an order book, it is first and foremost a distributed DEX protocol that can be used as the back-end engine for contributors to develop and deploy their own DEXs.

This enables the development of a variety of unique features and services, using the BasicSwap protocol as the backbone, while still being able to share the same order book and associated liquidity, if desired.

Modularity

For BasicSwap to act as a back-end protocol that powers other DEXs, dApps, and distributed services, it employs the modular architecture outlined earlier in this paper.

This modularity allows its core features, such as the capability to "quick swap" or interact with its order book, to be encapsulated into independent modules which third-party developers can then incorporate into their own applications.

Conclusion

The privacy-centric tools proposed in this paper provide an extensible framework that allows for a multitude of dApps, data storage networks solutions, or cryptocurrencies to be utilized. The PART token and its privacy features are designed to complement the project, and play a central role in the functioning of many of its already existing applications.

Strong, seamlessly integrated encryption allows us to develop communication structures immune to censorship in all its forms. These solutions, when used to their full potential, offer nothing less than a complete technological revolution in potentially every sphere of our digital lives.

Particl is founded on the principles of liberty and freedom, privacy, and decentralization. Integrating these into every product and service enables a truly fair and free digital environment of tomorrow, that puts the user at the very heart of it all.

References

[1] tecnovert. 2022. “Particl Core 23.0.1.0 RC2.”
https://github.com/tecnovert/particl-core/releases/tag/v23.0.1.0rc2

[2] Sunny King, Scott Nadal. 2012. "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake".
https://people.cs.georgetown.edu/~clay/classes/fall2017/835/papers/peercoin-paper.pdf

[3] S. Nakamoto. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System".
https://bitcoin.org/bitcoin.pdf

[4] "Security Analysis of Proof-of-Stake Protocol v3.0".
https://web.archive.org/web/20170928131109/https://bravenewcoin.com/assets/Whitepapers/Blackcoin-POS-3.pdf

[5] tecnovert: "Particl Cold-Staking Pool - Proof of concept". https://github.com/particl/coldstakepool

[6] Elements project: "Confidential Transactions - Investigation".
https://elementsproject.org/features/confidential-transactions/investigation

[7] B. Bunz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, G. Maxwell. "Bulletproofs: Short Proofs for Confidential Transactions and More".
https://www.utwente.nl/en/ces/sal/exams/digital-exams/Blockchain-and-Distributed-Ledger-Technology-test/3-Privacy/bulletproofs-paper.pdf

[8] S. Noether. 2015. "Ring Confidential Transactions". https://eprint.iacr.org/2015/1098.pdf

[9] https://en.wikipedia.org/wiki/Ring_signature

[10] R. Canetti, C. Dwork, M. Naor, R. Ostrovsky. 1996. "Deniable Encryption"
https://eprint.iacr.org/1996/002

[11] P. Wuille, J. Nick, A. Towns. 2020. "Taproot: SegWit version 1 spending rules".
https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki

[12] P. Wuille, J. Nick, T. Ruffing. 2020. "Schnorr Signatures for secp256k1".
https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki

[13] P. Wuille, J. Nick, A. Towns. 2020. "Taproot: SegWit version 1 spending rules".
https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki

[14] P. Wuille, J. Nick, A. Towns. 2020. "Validation of Taproot Scripts".
https://github.com/bitcoin/bips/blob/master/bip-0342.mediawiki

[15] https://github.com/ElementsProject/scriptless-scripts

[16] Peter Todd: "BIP-0065; Consensus".
https://github.com/bitcoin/bips/blob/master/bip-0065.mediawiki

[17] https://github.com/decred/atomicswap

[18] https://github.com/decred/atomicswap#theory

[19] tecnovert.
https://github.com/tecnovert/xmrswap/blob/master/doc/implementation_notes/notes.tex#L199

[20] tecnovert.
https://github.com/tecnovert/xmrswap/blob/master/doc/implementation_notes/notes.tex#L154

[21] E. Lombrozo, J. Lau, P. Wuille. 2015. "Segregated Witness (Consensus layer)"
https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

[22] https://gist.github.com/tecnovert/8929a8704b1dd6b2ef3c722d6b0632a4

[23] BtcDrak, M. Friedenbach, E. Lombrozo. 2015. "CHECKSEQUENCEVERIFY"
https://github.com/bitcoin/bips/blob/master/bip-0112.mediawiki#Lightning_Network

[24] https://kewde.gitbooks.io/protocol/content/data-storage-network/smsg.html

[25] https://www.whonix.org/wiki/BitMessage

[26] https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Cipher_block_chaining_(CBC)

[27] tecnovert. "Particl core"
https://github.com/tecnovert/particl-core/blob/master/src/smsg/crypter.cpp#L44

[28] tecnovert. "Particl core"
https://github.com/tecnovert/particl-core/blob/master/src/smsg/smessage.cpp#L4550

[29] https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm

[30] tecnovert. "Particl core"
https://github.com/tecnovert/particl-core/blob/master/src/smsg/smessage.cpp#L3921

[31] https://github.com/particl/omp-lib

[32] tecnovert. "Particl core"
https://github.com/tecnovert/particl-core/blob/master/src/smsg/crypter.cpp#L44

[33] https://en.wikipedia.org/wiki/Mutual_assured_destruction

[34] tecnovert.
https://github.com/tecnovert/xmrswap/blob/master/doc/implementation_notes/notes.tex#L154