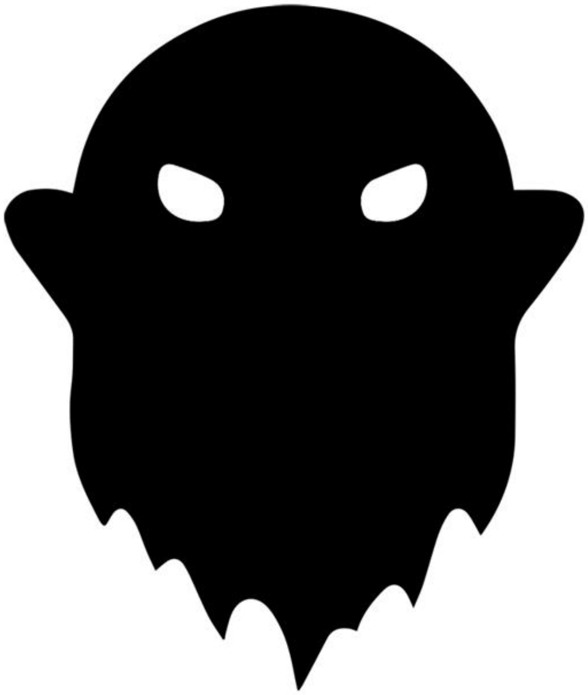
# GHOST
## PRIVACY

A peer-to-peer privacy-oriented electronic cash system



"A Specter is haunting the modern world, the specter of crypto anarchy."

Tim May – The Crypto Anarchy Manifesto (1992)

## Contents

# Abstract

Ghost introduces a privacy-centric, peer-to-peer version of electronic cash that enables secure and anonymous payments without the need for financial intermediaries. Derived from Particl, Ghost builds upon a robust foundation to address the scalability and privacy limitations prevalent in existing cryptocurrencies such as Bitcoin. Utilizing a Proof-of-Stake consensus mechanism, Ghost ensures transaction integrity through a decentralized network that validates transactions and commits them to a secure blockchain. This network not only confirms the history of transactions, but also enforces privacy through advanced cryptographic techniques, including ring signatures, trustless zero-knowledge range proofs using Bulletproofs, and stealth addresses to ensure unlikability and recipient anonymity. Designed to be accessible and straightforward, the blockchain promotes widespread adoption by simplifying user participation in network security. Ghost's innovative approach redefines the potential of cryptocurrencies by combining enhanced privacy, user empowerment, and sustainable growth, setting a new standard for private transactions in the digital age.

# Introduction

In 2008, an entity known as Satoshi Nakamoto published a paper [Nak08] that introduced Bitcoin, a digital currency designed to address critical shortcomings of previous systems. These shortcomings included vulnerabilities such as double-spending[1] and Byzantine[2] fault tolerance. Bitcoin employs cryptographic techniques to assign ownership of funds and utilizes a Proof-of-Work[3] mechanism with predefined rules to achieve network consensus and identify dishonest participants.

Bitcoin, as the first widely adopted decentralized electronic cash system, resolved many issues inherent to previous digital payment systems, yet it introduced new challenges and left some problems unaddressed. Subsequent cryptocurrencies, including Ethereum, which emerged around 2014, expanded Bitcoin’s capabilities by introducing features such as smart contracts, allowing for the execution of complex decentralized applications. These innovations aimed to address some of Bitcoin's limitations, particularly in terms of functionality and consensus mechanisms. This whitepaper introduces Ghost, a cryptocurrency designed from the outset to prioritize user privacy, an aspect insufficiently covered by its predecessors. Unlike systems primarily focused on transaction functionality or programmability, Ghost enhances the privacy features essential for true anonymity in financial transactions within a decentralized framework.

### Ownership of Funds in Bitcoin

Bitcoin uses elliptic curve cryptography[4] to assign funds to different users, where ownership is associated with the possession of a private-key from which an address can be generated. Funds can be sent to this address and can only be spent by using a digital signature that authorizes the transaction.

[1] Double spending is the ability to cheat a digital cash system by spending an amount more than once.

[2] Byzantine fault intolerance is a problem in distributed computing systems, where it is not possible to distinguish honest nodes from dishonest nodes to achieve consensus.

[3] Proof-of-work is a mechanism by which honest nodes prove their honesty in their communications by proving that their communicated state or message is created by solving a problem that needed heavy computation, which, depending on the system, would be impractical for a dishonest node.

[4] Elliptic-curve cryptography is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC allows smaller keys compared to non-EC cryptography to provide equivalent security.

### The Blockchain Ledger

When an owner signs a transaction to spend it, a wallet software broadcasts the transaction to the bitcoin network. These transactions are received by miners, who collect all transactions and place them in a block, which currently can hold up to 1MB of transaction data. After filling a block with all available transactions, the miner "mines" the block, a process in which they use proof-of-work (i.e. spends electricity) to solve a computational puzzle. All miners compete to solve this puzzle. Once one is successful in solving it, they broadcast their block to the network, which adopts it as its new state (hence consensus is achieved). Successful miners are rewarded with newly minted Bitcoin along with transaction fees for their efforts.

Blocks are ensured to be immutable by using hash functions, where the hash of the data in the block is hashed and stored. Any attempt to change the data of a block will immediately be recognized. Hashes are used to link blocks together. Every block contains the hash of the data in the block that preceded it. This brings up the term *"Blockchain",* where blocks are "chained" together using their cryptographic hashes. Attempting to change anything in a block from the past will change its hash, which in turn will change the hash stored in the next block, which will in turn change the block after that, leading to an avalanche to form where all blocks will become different. This is what guarantees the immutability of a blockchain.

### Proof-of-Work Mining

Satoshi planned for Bitcoin mining to be egalitarian, where any person could participate in the network in mining and earn Bitcoin using their personal computers. However, since Bitcoin mining depends solely on executing the hashing function *SHA256* indefinitely, devices that are much more efficient than computers, known as *ASICs*[5], can be specifically suited for this task. *ASICs* are hard to come by for most people and are generally expensive. This has made it practically impossible for the average person to participate in mining and opened the doors to large "farms" to do this on a professional basis.

[5] ASICs: Application Specific integrated Circuits are devices that mostly do one thing very efficiently. In the case of bitcoin, they calculate the hashing function SHA256 but have no other purpose.

Attempts to get rid of *ASICs* have been skyrocketing over the years, with other cryptocurrencies adopting hashing algorithms that require significant memory for their calculations and other functionality that are hard to implement on a chip without a CPU. However, most of these attempts have failed, and the "fight" against *ASICs* continues. Some projects have decided to position themselves as a moving target, where their mining algorithm keeps changing. A good example of this is Monero, which previously changed their mining algorithm every six months. Eventually, a new mining algorithm was invented, *RandomX* [Ran19]. RandomX uses a combination of CPU instructions in the mining process, effectively deeming ASICs useless by definition, since performing CPU instructions is opposite from what an ASIC is supposed to be (i.e. be Application Specific).

However, we view the issue as larger than just banning ASICs due to the aforementioned. We find mining itself non-egalitarian because on top of the high cost of hardware, the cost of electricity will also never be the same for everyone. A study by Elite Fixtures [Eli18] has shown that a significant difference exists in the expense to mine a single bitcoin in different countries, considering all other factors being equal (i.e. ASICs being available for everyone). This discrepancy shows that some people will always be more fortunate than others and have cheaper electricity, and hence profit more from mining. Consequently, it leads to the centralization of mining power. This is particularly evident nowadays in Bitcoin, with Chinese origin "pooling farms" holding over 65% of the market share of this operation [Cry19]. A phenomenon that as a result of the free-market system is only inevitably going to be exacerbated.

# Progression

## Lack of Privacy on the Blockchain

Blockchains are generally not designed to have any privacy features. Privacy, in this case, means that the sender, receiver and the amount being sent should not be visible to any entity on the blockchain except for those who have a financial interest in the transaction. However, in bitcoin, and most blockchains out there, all the previously mentioned information is visible. Anyone viewing the blockchain could see the destination addresses of every transaction, the amounts being sent to these addresses, and since every address has only one private-key that it comes from, we know that the owner of that address is the signer of that transaction. To make things worse, with statistical analysis and machine-learning, addresses can be linked together, and it is even possible to find their ultimate owner. Additionally, there are companies that have taken the initiative in providing services of linking addresses and revealing information about the users of a blockchain; an example is *Chainalysis*[6]. It also provides it as a service for Governments[7]. This is particularly negative for people who live in countries with oppressive authorities, where this information can be freely used to invade civil rights.

In other words, even though addresses are pseudonymous and do not reveal the owner by name, it is practical to follow the senders and receivers of transactions, up to an exchange, where the user submitted his personal information to follow *KYC*[8] and *AML*[9] laws, which will ultimately reveal the owner. Not only that, but this also endangers the state of fungibility [10] of cryptocurrency coins.

[6] https://www.chainalysis.com/

[7] https://www.chainalysis.com/government-agencies/

[8] Know-Your-Customer

[9] Anti-Money Laundering.

[10] Fungibility is a property of money or currency where there is no practical way to distinguish between different units of it in value. For example, there is no difference between $1 in my pocket and $1 in yours. They both carry the same value, acceptance, and characteristics.

For example, if any Bitcoin were to be used for nefarious acts, and then it came into possession of someone who was not aware of its previous history, the person may inadvertently see their value/use diminished, as the coins would be deemed to be "tainted" [Min15]. This is particularly evident in the events where freshly mined bitcoins were sold for a premium [Red20] since they did not have any previous transaction history.

Besides the issues mentioned above, this can also lead to safety concerns. For example, as a result of their holdings being revealed, there have been incidents of people having had their life threatened and being forced to pay a ransom in said cryptocurrency [Gua17].

Noting the above, it's evident that there is an imperative need to eliminate *linkability*[11]

and *traceability*[12] on the blockchain in order to safeguard the privacy of its users.

[11] Linkability is the ability to associate multiple transactions to the same person, address or signature.

[12] Traceability is the ability to follow or trace the source of a coin over its history.

### Proof-of-Stake vs. Proof-of-Work

The Ghost project utilizes a Proof-of-Stake consensus algorithm. In this process, participants use their digital assets as collateral (as opposed to spending electricity in Proof-of-Work), where they prove that they mean well in the network. In other words, instead of spending electricity to prove to other nodes that a miner has worked to create a block, a "staker", in a different trust model, uses the cryptocurrency they own to attest to their honesty through their stake in the network. Participants have a larger influence in the network if they own a bigger fraction of the total supply in the network. It is not in a staker's interest to be dishonest in the network, because if they attempt to break it by disregarding the rules, they will lose the value of their collateral in the free market. Through being an honest participant in the network, the participants gain a reward (just like miners do) for creating new and valid blocks.

There are huge debates on whether Proof-of-Stake or Proof-of-Work are better. However, it's worth mentioning that there has never been a single legitimate 51% attack on a Proof-of-Stake network. This is particularly relevant when compared to the several attacks on Proof-of-Work systems (such as Ethereum Classic [Coi19], Bitcoin Gold [Btg51]), where the miners that do the attack have no concern in the healthiness of the network. With even online lists detailing the costs of attacking every blockchain for a certain amount of time [Bie18, Pow51], there is a clear base for preference of Proof-of-Stake.

However, since Proof-of-Stake does not require physical work like Proof-of-Work, it is possible, theoretically, to replace the whole blockchain with a new one created in a short time [Ioh18]. This problem is solved typically by "checkpointing", where a list of checkpoints of blocks are manually saved to protect from erasing the history of a blockchain and replacing it with another one. Checkpointing is considered controversial in the cryptocurrency community, as it is a "centralized" solution, since developers have to maintain this. However, many proof-of-work blockchains currently employ this tool to protect from future attacks, with an example being Monero. Akin to them, Ghost also sees this as a good trade-off.

Given that Ghost adopts a Proof-of-Stake consensus algorithm, it’s important to understand the differences between the two methods of participating in the network i.e., Hot Staking and Cold Staking.

### Hot Staking

Hot Staking, also referred to as active staking, involves maintaining a network-connected wallet that participates directly in the blockchain's consensus process. In the context of the Ghost network, Hot Staking is a mechanism by which stakeholders contribute to network security and transaction validation by running a fully synchronized node that is always online.

Participants engaging in Hot Staking must ensure continuous connectivity and operation of their nodes. This involves running wallet software that actively signs and broadcasts transactions. By doing so, Stakers validate new transactions and blocks, contributing to the overall robustness and integrity of the blockchain. The primary incentive for Hot Staking includes receiving staking rewards, which are distributed according to the participant's *stake weight*[13].

One drawback to this method of participation is that Hot Staking can be very risky. If a participant keeps their computer open with accessible funds, any breach in the system may lead to the loss of their funds. The question then is, is it possible to keep the funds 100% safe, and stake at the same time? The answer to this dilemma: *Cold Staking.*

### Cold Staking

Cold Staking represents a security-focused approach to staking, where the staking process is decoupled from the custody of the coins themselves. In Ghost, Cold Staking allows stakeholders to participate in the network's consensus mechanisms without exposing their private keys to the internet, thus enhancing the security of their assets.

Cold staking employs a two-key architecture: a spending key (private-key) and a staking key (cold staking pubkey). The spending key, responsible for controlling fund movements, is secured offline in cold storage, while the staking key remains online to participate in the consensus process. This separation ensures that, even if the staking key is compromised, the funds cannot be accessed without the offline spending key. In other words, the staker delegates his stake weight to the cold staking pubkey but retains full control over his collateral with the ability to revoke delegation without being subject to penalty.

[13] Stake weight refers to a participant's net holdings or collateral within the network, used to determine their relative influence or probability of being selected to validate transactions and create new blocks.

## Privacy

In Bitcoin, the recipient’s address is derived from the public key, which itself is generated from a corresponding private key used to authorize transactions from that address. This structure inherently allows for the repeated use of an address, linking it permanently to the owner of the private key. Consequently, all transactions associated with a particular address are publicly traceable, allowing other participants to ascertain the balance and transaction history of that address. Such transparency exposes users to potential scrutiny of their financial activities, risks of social engineering, and the possibility of targeted oversight by public entities, such as government bodies. To mitigate these privacy concerns, Ghost implements Stealth Addresses, which obscures the linkage between transactional records and the public keys of the transaction participants.

### Stealth Addresses

Stealth Addresses[14] are a pivotal feature in the Ghost network, designed to enhance transactional privacy by severing the direct link between transactions and the public identities of their participants. This approach addresses the traceability issue inherent in many blockchain systems, including Bitcoin, by allowing users to maintain public anonymity while engaging in blockchain transactions. Stealth Addresses consist of two key pairs, a spending key and a viewing key, denoted as $A$ and $B$ respectively, with corresponding private keys $a$ and $b$[15]. The spending key, A, is directly involved in accessing funds, while the viewing key, B, is instrumental in maintaining transaction privacy through the *Diffie-Hellman* key exchange protocol.

A
Public Key 1
B
Public Key 2

Stealth Address

[14] Stealth Addresses were first introduced in the Cryptonote protocol [Vanl2].

[15] If we call the base point in the used Elliptic Curve $G$, then $aG=A$ and $bG=B$.

The Diffie-Hellman protocol enables secure communication over insecure channels. It allows two parties to establish a shared secret by exchanging public keys without ever transmitting private keys. If Alice and Bob are transacting, Alice sends her public key A, to Bob, and Bob sends his public key B, to Alice. Each party then computes the shared secret using their own private key and the other party's public key.

Assume Alice's and Bob's private keys are a and b, and their public keys are $A=aG$ and $B=bG$, respectively, where $G$ is the base point on the elliptic curve. The shared secret computed by Alice is $aB=abG$, and by Bob as $bA=baG$. This common value, $abG$, can then be used to encrypt communications.

When a transaction is initiated, the sender generates a random private key $r$ and computes a public key $R = rG$, which is included in the transaction. The sender uses the recipient's public key $B$ to compute a shared secret: $s = rB = rbG.$ The secret $s$ is then combined with the recipient's spending key $B$ to generate a one-time address for the transaction, typically by $Q = H(s)\ G + B,$ where $H(s)$ is a hash function applied to $s$.

The recipient, upon receiving the transaction, can derive the same shared secret using $R$ and their private key $b$: $s = bR = brG.$ Using this shared secret and their private spending key $a$, the recipient can access the funds sent to the one-time address $Q$. This ensures that each transaction address, $Q,$ is unique due to the randomness of $s$ and the cryptographic hash function $H(s),$ making it infeasible to link $Q$ back to the recipient's public key.

Using Stealth Addresses, each anonymous transaction to a Ghost address results in a new, unique public key derived through cryptographic means. This ensures that no two transactions can be publicly linked to the same recipient, significantly enhancing user privacy by making transaction tracing and wallet address linkability impractical. While Stealth Addresses significantly enhance user privacy by anonymizing transaction recipients, Ring Confidential Transactions[16] (RingCT) further extend privacy by concealing transaction amounts and obfuscating sender identities through ring signatures, ensuring comprehensive anonymity and security within the blockchain. Initially starting from *Borromean signatures* by Gregory Maxwell et al [Max15], these were expended by Shen Noether et al [Noe16].

[16] RingCT was first introduced in 2015 by Shen Noether as part of his work on Monero.

## Ring Confidential Transactions (RingCT)

### Overview

Ring Confidential Transactions (RingCT) are integral to Ghost's architecture, designed to enhance the privacy and security of transactions by concealing both the amount and the parties involved. This advanced cryptographic method incorporates several key technologies: decoys, MLSAG signatures, and additional elements such as commitment schemes and zero-knowledge proofs to ensure comprehensive anonymity and integrity of transactions.

### Decoys

Decoys are randomly selected unspent outputs mixed with the actual spendable outputs to form a "ring" in each transaction. This obfuscation helps mask the true source of funds. Ghost uses ring signatures to sign this mixture, providing plausible deniability and preventing outside observers from pinpointing the real spender. Ring signatures are formed by combining public keys of decoys and the actual sender, creating a single digital signature that verifies the group without revealing individual identities.

### MLSAG Signatures

Multi-layered Linkable Spontaneous Anonymous Group (MLSAG) signatures extend the functionality of ring signatures by allowing each input in a transaction to have its own unique ring. This significantly boosts privacy, especially in transactions involving multiple inputs. The verification process for an MLSAG signature is given by:

$\sigma = (\{ c_1 \} , \{r_1\})$,

with verification computed as:

$$c_{i+1} = H( r_iG + c_iP_i ),$$

where $H$ is a cryptographic hash function, $G$ is the base point on the elliptic curve, $P_i$ are public keys, and $c_i , r_i$ are scalar values. This ensures that transactions are unlinkable to previous transactions yet remain verifiable without exposing the identity of the signers. Despite ensuring anonymity, MLSAG signatures are linkable in the sense that if the same input is spent twice, it can be detected, thereby preventing double-spending without compromising privacy.

### Pedersen Commitments and Confidential Transactions

RingCT leverages Pedersen Commitments to securely hide transaction amounts while ensuring the network can verify the integrity of the monetary supply. This prevents the illicit creation or destruction of coins, crucial for preserving Ghost's economic stability. The commitments ensure that the sum of the inputs equals the sum of the outputs, as demonstrated by the following formula:

$C = xG + aH,$

where $x$ is a blinding factor that secures the confidentiality of the amount, $a$. Here, $G$ and $H$ are public parameters of the elliptic curve, with $H$ being particularly chosen so its discrete logarithm relative to $G$ is unknown, which safeguards the commitment's security.

This design not only enhances transaction privacy, but also allows for the network to perform efficient and secure audits without access to the actual transaction values and thus compromising anonymity. By ensuring the cryptographic robustness of each transaction, Pedersen Commitments provide a layer of trust and transparency within Ghost's decentralized framework. Additionally, zero-knowledge range proofs are employed to prove that the committed amounts are within valid ranges, preventing negative balances or overflow attacks without revealing the actual amounts. The use of these commitments facilitates a higher degree of scalability and efficiency in processing transactions, making the blockchain more resilient and adaptable to future enhancements.

### Bulletproofs

Bulletproofs are a novel form of non-interactive zero-knowledge proofs that do not require a trusted setup, designed primarily to enhance transaction privacy while reducing computational overhead in blockchain applications (Bue17)[17]. This technology facilitates compact proofs without compromising security, pivotal for blockchain scalability.

### Technical Advantages of Bulletproofs

1. Efficiency in Proof Sizes: Bulletproofs provide a logarithmic reduction in proof sizes, which is critical for high throughput blockchain networks like Ghost. The efficiency is derived from their structure, represented by the equation:

$$Proof\ size \approx log(n) + 2\sqrt{log(n)}$$

   where n is the number of elements in the proof. This formula showcases how Bulletproofs maintain small proof sizes even as transaction complexity increases (Bünz et al., 2017).

2. Elimination of Trusted Setup: Bulletproofs eliminate the need for a trusted setup, a significant advancement over previous zero-knowledge proofs, enhancing the security and decentralization of the network[18].

3. Support for Proof Aggregation: Bulletproofs can aggregate multiple transaction proofs into a single proof, reducing blockchain bloat and improving privacy. This capability is crucial for maintaining performance without sacrificing security.

[17] Non-interactive zero knowledge proofs allow one party to prove a statement's validity to another without revealing any other information or needing interaction.

[18] Bulletproofs avoid the security risks of zk-SNARKs by eliminating the need for a vulnerable trusted setup.

$$A\text{ggregated Proof} = \prod_{i=1}^{n} \mathrm{p}_{\mathrm{roof}_i}$$

Given the equation above, this shows us how the aggregation process multiplies individual proofs, leading to a single, compact aggregated proof (Bünz et al., 2017). Integrating Bulletproofs into Ghost involved updating cryptographic protocols to support the aggregation of proofs, leading to reductions in transaction size and enhancements in verification speeds, critical for network scalability.

**Impact on Ghost**

The integration of Bulletproofs from the outset has provided Ghost with significant advantages in terms of privacy, efficiency, and scalability. By leveraging Bulletproofs instead of traditional range proof methods used in other cryptocurrencies, Ghost offers enhanced performance and security features that set it apart from traditional networks.

Bulletproofs significantly reduce proof sizes compared to traditional range proofs, which is paramount for a high-throughput network. Traditional range proofs used in other cryptocurrencies can be large, contributing to increased transaction sizes and blockchain bloat. In contrast, Bulletproofs provide a logarithmic reduction in proof sizes relative to the number of bits in the range, as represented by:

$$Proof\ size \approx 2log_2(n) + \delta$$

where *n* is the number of bits in the range and δ is a small constant. This efficiency means that confidential transactions in Ghost have significantly smaller proofs, reducing the amount of data that nodes need to store and transmit. With traditional range proofs, confidential transactions might have proof sizes of up to 10 kilobytes. In Ghost, thanks to Bulletproofs, these proofs are reduced to approximately 1–2 kilobytes. As a result, transactions are lighter, reducing the blockchain's overall size and improving network performance. Smaller transaction sizes allow more transactions to fit into each block, enhancing the network's capacity to process a higher volume of transactions without delays. Additionally, Bulletproofs enable quicker verification of proofs compared to traditional methods, reducing computational overhead and leading to faster block validation and propagation.

**Enhanced Privacy and Security**

By utilizing Bulletproofs, Ghost provides stronger confidentiality by concealing transaction amounts while still allowing validators to confirm the validity of transactions. Participants can prove that amounts are positive and within valid ranges without revealing the actual values, thanks to the zero-knowledge properties of Bulletproofs. Moreover, Bulletproofs do not require a trusted setup, unlike other zero-knowledge proof systems such as zk-SNARKs. This elimination enhances security by removing risks associated with compromised initial parameters and or bad actors. The non-interactive nature of Bulletproofs simplifies the verification process and reduces potential attack vectors, minimizing opportunities for interception or manipulation during the proof process.

**Optimized User Experience**

Bulletproofs contribute to an optimized user experience and are designed to be future-proof. The efficient verification and reduced data sizes lead to faster transaction confirmations, enhancing user satisfaction by making transactions feel instantaneous. Additionally, the smaller transaction sizes enabled by Bulletproofs help keep transaction fees[19] low, even during periods of high network usage when fees might otherwise increase due to competition for block space. Wallet applications benefit from the efficiency of Bulletproofs, requiring less computational power to generate and verify proofs, which enhances performance on older hardware, broadening accessibility. Furthermore, smaller blockchain sizes lower the storage burden for running a full node, encouraging more users to participate as validators, which strengthens the network.

[19] Fees are transaction costs imposed by the network to incentivize and compensate validators for the computational resources and energy expended in validating, securing, and recording transactions within a blockchain.

### Dandelion++

In traditional blockchain networks such as Bitcoin, transactions are propagated using a gossip protocol. When a user broadcasts a transaction, it is sent to all connected peers, which then relay it to their peers, and so on, until the transaction spreads throughout the entire network. While effective for dissemination, this method has a significant privacy flaw: observers can analyze network traffic to trace transactions back to their originating IP addresses [Fan18]. By controlling enough nodes or monitoring the network, adversaries can determine which node first broadcasted a transaction, thereby linking the transaction to a specific IP address. This linkage compromises user anonymity, exposing their entire transaction history once their identity is associated with an address.

Dandelion++[20] addresses these privacy concerns by altering the transaction propagation method to make it more difficult for adversaries to trace transactions back to their source. The protocol divides the transaction dissemination process into two distinct phases: the Stem Phase and the Fluff Phase.

- Stem Phase: Each node sends the transaction to only one randomly selected peer in its local neighborhood.
- Fluff Phase: The transaction is sent to all peers on the network, thus falling back to the Gossip protocol.

Dandelion++ significantly differs from its original protocol in its stem phase where it passes transactions over intertwined paths before diffusing them to the network. These paths are structured as a random 4-regular graph, meaning each node is connected to exactly four other nodes. This structure enhances anonymity by making it more difficult for adversaries to reconstruct the propagation path.

[20] Dandelion++ was first introduced in 2017 by Giulia Fanti, Shaileshh Bojja Venkatakrishnan, Mohammad Alizadeh, Giuliano Cornacchia, Philip J. Levis, and Scott Shenker. The protocol was later proposed in BIP156 but was never implemented.

Both the previous and current versions of Dandelion proceed in asynchronous cycles, meaning each node will advance when its internal clock arrives at a certain threshold. Within these cycles, Dandelion++ functions through four primary components with specific optimizations.

1. Anonymity Graph, which uses a random 4-regular graph, instead of a linear graph for the anonymity phase. Dandelion++ relays nodes independent of whether or not their outbound neighbors support Dandelion++.

2. Transaction Forwarding (own) comes into play every time a node generates a transaction of its own, it then sends the transaction along the same outbound edge in the 4-regular graph. The difference here is that with the original protocol, nodes were only assumed to generate one transaction.

3. Transaction Forwarding (relay) is all about probability, more specifically within the Stem Phase when a node receives a transaction and chooses between relaying the transaction or diffusing it to the network. Deciding to diffuse a transaction to the network is pseudorandom. Nodes are either diffusers or relay nodes for the relayed transactions.

4. Fail-Safe Mechanism kicks in during each Stem Phase and each node tracks whether it is seen again as a Fluff Phase transaction. If not, the node diffuses the transaction.

With negligible overhead, Dandelion++ is a lightweight network layer solution that offers many benefits not just IP obfuscation. The protocol also has built-in resistance to known attack vectors such as:

- Graph Learning Attacks: The randomization and structure of the anonymity graph help prevent adversaries from reconstructing the network topology.

- Intersection Attacks: The probabilistic nature of the stem-to-fluff transition and the fail-safe mechanism mitigate risks associated with timing analysis and transaction interception.

- Black-Hole Attacks: The fail-safe ensures that transactions are not lost even if a node in the stem phase is malicious and tries to drop transactions.

Implementing Dandelion++ enhances Ghost's network-level privacy by making it significantly more challenging for adversaries to trace transactions back to their originating IP addresses. This protocol operates seamlessly with minimal impact on network performance, ensuring users benefit from enhanced privacy without experiencing delays or complexity.

### Quantum Resistance

While current quantum computers are not yet capable of performing such tasks at the necessary scale, significant advancements are being made in the field. Companies like IBM have announced progress towards developing quantum processors with increased qubit counts [IBM17]. However, some experts remain skeptical about the timeline for achieving quantum computers that can break modern cryptographic systems [Dya18]. In this uncertain environment, it is prudent for cryptocurrencies to prepare for the "quantum threat" to ensure long-term security. In Bitcoin, addresses are generated by hashing public keys, and as long as the public key remains unrevealed (i.e., no transactions have been made from the address), quantum computers cannot easily derive the private key due to the one-way nature of hash functions. Hash functions are relatively resistant to quantum attacks, as Grover's algorithm only provides a quadratic speedup, which can be mitigated by increasing the hash output size.

In Ghost, the same address infrastructure of Bitcoin is used. To solve the issue of quantum threat, users are recommended to use addresses only once. However, this is generally not possible with staking, because staking requires revealing the public-key. Therefore, through cold-staking, this problem is solved, since you are not required to reveal your private-key, since the delegate only reveals its public key, and hence, it is quantum-secure. There are special staking methods that we have developed that resolve any threats to quantum computing attacks. One such method is by generating a new spending address each time you hit a stake, which also enhances anonymity.

[21] A quantum computer is a computer that does not use the usual binary state “bit”, or {0,1}, to perform basic logical and arithmetic operations, but uses quantum states {0,1}, which are called qubits. Qubits have the ability to be in multiple states simultaneously (technically called a superposition of states). A qubit can be 0 and 1 simultaneously with a probability associated with each state (e.g., 30% ‘0’ and 70% ‘1’). This leads to very interesting results and new algorithms that scale much better than classical computers we use in present times.

[22] Classical computers are the computers that we use currently. The terms classical vs quantum come from physics, where Newton’s physics is compared to Quantum physics.

## Operational Specifications & Tokenomics

The following outlines Ghost's operational specifications and tokenomic structure.

- Consensus Method: Proof of Stake
- Block time: 120 seconds
- Max Block size: 8 MB
- Model: UTXO
- Coinstake Maturity: 225 confirmations
- Maximum Supply: 55,000,000 (Soft Cap)

**Emission Rate**: For the first two years, the block reward will be 12 GHOST per block. After this initial period, the block reward will decrease every 262,800 blocks, which corresponds to approximately one year given Ghost's block time of 120 seconds. The block reward will follow this formula:

$$Block\ Reward\ =\ 9\frac{round\ (100\ X\ 0.95^{\mathrm{n}})}{100}$$

where $n$ represents the number of years that have passed since the end of the initial two-year period. The blockchain will follow this block reward formula for the next 30 years, or until the blockchain reaches its maximum supply of 55,000,000 GHOST. Once the maximum supply has been reached, the block reward will be reduced to 0.9 GHOST per block indefinitely to maintain network security and incentivize validators.

Block Reward distribution:

- Stakers: 46%
- Ghost Veterans: 33%
- Development Fund: 21%

**Ghost Veteran Rewards**

Initially, we considered implementing masternodes to fulfill this role. However, due to the complexity of setup and potential security vulnerabilities associated with masternodes, we decided on an alternative approach. The Ghost Veteran Reward structure rewards users with larger stake weights without the need for a separate masternode system.

**Eligibility Criteria for Ghost Veteran Rewards**

There are three covenants that must be met in order to participate as a Veteran:

1. An address must be holding at least 20,000 coins at all times.
2. The address must be actively staking, hot or cold.
3. Once an address has met the first and second requirements, the address must sit out a time lock period of 21,600 blocks, which is about 30 days.

During the time lock period, users are free to move their coins without penalty, provided their address balance does not fall below the minimum required threshold of 20,000 GHOST. If an address balance falls below this threshold at any point, the time lock resets, and the user must complete a new set of 21,600 blocks to regain eligibility. By implementing this third covenant, we aim to enhance network security and promote long-term commitment. These covenants are subject to change via community vote, ensuring that the Ghost network evolves in alignment with the community's values and needs.

These Ghost Veteran Rewards (GVR) are automatically paid out by the blockchain on a per block basis. However, if a staker does not meet the criteria mentioned above, the Veteran portion of the block reward (33%) is carried forward. This means that the unclaimed Veteran Rewards accumulate over time. When an eligible Veteran mines a block that has a carry forward balance, the Veteran will receive the accumulated carry-forward amount, in addition to the standard staking reward and current Veteran Reward.

### On-Chain Governance

Ghost employs an on-chain governance protocol that empowers stakeholders to participate directly in the decision-making processes affecting the network. This system is designed to be decentralized and transparent, ensuring that only those with a vested interest in the project can influence its direction. By leveraging stake-weighted voting, Ghost aligns the interests of the network with those of its active participants.

The governance protocol operates on a stake-weighted voting system. Each time a user successfully stakes a block on the network, they register a vote. This method ensures that voting power is proportional to the user's stake and active participation in securing the network. By tying voting rights to staking activity, the system prevents external entities without a stake in the project from exerting undue influence.

### Categories of Proposals

Proposals submitted to the network are classified into two main categories:

1. Non-Protocol - These are proposals that do not require changes to the core protocol of the blockchain.
2. Protocol - Proposals that necessitate changes to the blockchain's core protocol, potentially impacting the entire ecosystem.

Each of the aforementioned proposals has their own set of parameters independent of one another that are required to be met in order to be approved.

Voting Parameters for Non-Protocol:

- Quorum Requirement: 33% of the total staking power must participate for the vote to be valid.
- Voting Period: 5,040 blocks which is about one week.
- Approval Requirement: A minimum of 51% affirmative votes among the votes cast.

Voting Parameters for Protocol:

- Quorum Requirement: 33% of the total staking power must participate for the vote to be valid.
- Voting Period: 10,080 blocks which is about two weeks.
- Approval Requirement: A minimum of 70% affirmative votes among the votes cast.

If a proposal meets the minimum quorum, it will then be considered a valid proposal and voting will commence. If the vote meets the required threshold, it will be considered approved. The approved proposal is then forwarded to the core team, who may allocate funds from the Development Fund (if necessary) and create a bounty for the tasks involved in the proposal. All community members are eligible for the bounty, including core Ghost members. This means anyone can begin work on the open-source platform, resolve the issue or build out the new feature and be paid directly in GHOST coins for their work. Contributors will submit their work via a pull request (PR) for approval by the core team, just as a core team member would have to.

**Acknowledgements**

This white paper was prepared in collaboration by the Ghost Team and distinguished members of academia, including Professor Ravi Sen, Ph.D., of Texas A&M University.

We would like to thank the Particl team for their robust codebase which served as a strong foundation for Ghost.

We extend our sincere gratitude to the Ghost community for their early and unwavering support, and we look forward to advancing our shared vision for the future of Ghost.

In memory of our late Co-Founder, John McAfee, whose bold vision and relentless advocacy for privacy laid the groundwork for Ghost. His influence remains integral to our mission.

## References

[Nak08] Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System.*

[Min15] Minichiello, N. (2015) *The Bitcoin Big Bang: Tracking Tainted Bitcoins, BraveNewCoin, 21st June.* Available at: https://bravenewcoin.com/insights/the-bitcoin-big-bang-tracking-tainted-bitcoins

[Red20] Redman, J. (2020) *Industry Execs Claim Freshly Minted 'Virgin Bitcoins' Fetch 20%, Premium* , *March* . Available at: https://news.bitcoin.com/industry-execs-freshly-minted-virgin-bitcoins/

[Eli18] Jeff (2018) *Bitcoin Costs Throughout the World, Elite Fixtures, February.* Available at: https://www.elitefixtures.com/blog/post/2683/bitcoin-mining-costs-by-country/?mod=article_inline

[Ran19] Github (2020) *The github repository for RandomX* . Available at: https://github.com/tevador/RandomX

[Cry19] Moos, M (2019) *Bitcoin Mining Centralization Reaches Record Levels, Majority China, Crypto Briefing,* Dec 12th *,* Available at: https://cryptobriefing.com/bitcoin-mining-centralization-record-levels-majority-china/

[Btg51] Iskra, E (2018). *Responding to attacks, Bitcoingold, 24th May.* Available at: https://bitcoingold.org/responding-to-attacks/

[Coi19] Nesbitt, M (2019). *Deep Chain Reorganization Detected on Ethereum Classic* (ETC), *Coinbase, Jan 7th.* Available at: https://blog.coinbase.com/ethereum-classic-etc-is-currently-being-51-attacked-33be13ce32de

[Bie18] BitcoinExchange Guide News Team (2018), *List of PoW 51% Attack Costs for Each Cryptocurrency, BitcoinExchange, May 28th. Available at:* https://bitcoinexchangeguide.com/list-of-pow-51-proof-of-work-mining-attack-costs-for-each-cryptocurrency/

[Pow51] Crypto 51 (2020) *PoW 51% Attack Cost, Crypto51, June 9th.* Available at: https://www.crypto51.app/

[Ioh18] Gaži P. (2018) *Stake-Bleeding Attacks on Proof-of-Stake Blockchains, IOHK, June.* Available at: https://iohk.io/en/research/library/papers/stake-bleeding-attacks-on-proof-of-stake-blockchains/

[Van12] Van Saberhagen, N. (2012) *The Cryptonote Protocol* , *December 12th.* Available at https://cryptonote.org/whitepaper_v1.pdf

[Max15] Maxwell, G. et al (2015) *Borromean Ring Signatures, June 2nd.* Available at: https://pdfs.semanticscholar.org/4160/470c7f6cf05ffc81a98e8fd67fb0c84836ea.pdf

[Noe16] Noether, S. et al (2016) *Ring Confidential Transactions, Monero Research Labs, February.* Available at: https://web.getmonero.org/resources/research-lab/pubs/MRL-0005.pdf

[Bue17] Buenz, B. et al (2017) *Bulletproofs: Short Proofs for Confidential Transactions and More, Stanford University.* Available at: https://eprint.iacr.org/2017/1066.pdf

[Gua17] Reuters in Kiev (2017) *Ukraine Kidnappers Release Hostage After $1m bitcoin Ransom Paid, The Guardian, December 29th* . Available at: https://www.theguardian.com/uk-news/2017/dec/29/ukraine-kidnappers-release-hostage-after-1m-bitcoin-ransom-paid

[IBM17] Anthony, S (2017) *IBM Will Sell 50-qubit Universal Quantum Computer "In The Next Few Years", ArsTechnica, June 3rd.* Available at: https://arstechnica.com/gadgets/2017/03/ibm-q-50-qubit-quantum-computer/

[Dya18] Dyakonov M. (2018) *The Case Against Quantum Computing, Spectrum, November 15th.* Available at: https://spectrum.ieee.org/computing/hardware/the-case-against-quantum-computing

[Fan18] Fanti et al. (2018) *Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees* , *ACM, June. Available at:* https://dl.acm.org/doi/10.1145/3224424