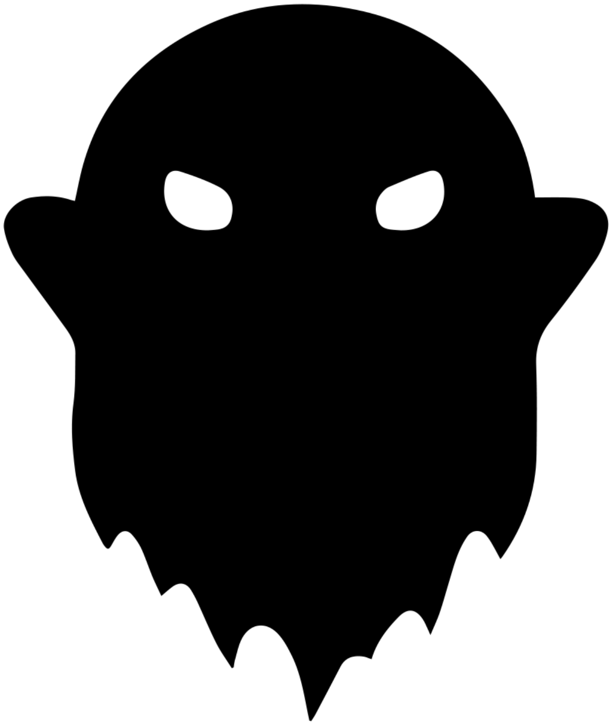


Ghost

A privacy coin by John McAfee

ghostbymcafee.com | @ghostbymcafee

“*A specter is haunting the modern world, the specter of crypto anarchy.*”

Tim May - The Crypto Anarchy Manifesto (1992)

Contents

Abstract

The mission for the Ghost project is to create a privacy focused, anonymous and decentralized payment network that is based on a sustainable proof-of-stake consensus algorithm with incentivized operators. The outlying products and services offered will have a focus on simplicity, while at the same time, providing accessible and practical solutions for mainstream adoption.

This document will consist of a brief overview of the origins of bitcoin, the mechanisms powering the blockchain and a short explanation of the use cases that this technology provides. It will also discuss how the most traded coin on the market, Bitcoin, can be substantially improved in various ways. Furthermore, current solutions that have been introduced to the market thus far will be analyzed, while reviewing the underlying technology that they operate on.

Additionally, it will detail how and why these solutions should be further enhanced and ultimately, how these changes will push cryptocurrencies as a whole, towards making a greater economic impact on society for a truly functional, private and accessible decentralized electronic payment system.

Particl, the privacy focused coin from which Ghost was initially forked from, will also be introduced. Initially diverged from Bitcoin, this project has been greatly developed and improved upon by their engineering team. As opposed to starting from scratch, Ghost concluded Particl would provide a solid foundation from which to jumpstart the initiative. Therefore, allowing the project to begin implementing it’s own innovative technological advancements without having to “reinvent the wheel”.

However, Ghost’s vision goes well beyond their offering. The document will present its current and future development agendum with an explanation following each major

addition. Full technical specifications related to the inner workings and operational functions of the software will also be provided. Finally, information regarding the current Ghost team will be given along with the vision and plans for the future.

GHOST

has entered the chat.

Introduction

In 2008, an entity known as Satoshi Nakamoto, published a paper [Nak08] describing a digital currency that aimed to solve the problems of its predecessors. This included problems such as double-spending[1] and Byzantine fault intolerance[2] - this currency is Bitcoin. Bitcoin uses cryptography to assign ownership of funds, and uses proof-of-work[3] with predefined rules to achieve consensus and to recognize dishonest participants in the network.

Albeit successfully resolving many of the problems of its precursors, being the first widely adopted decentralized digital cash system, other shortcomings remain. In particular, we refer to the lack of specific features that other cryptocurrencies have set out to to solve and build upon. For example, shortly after in 2014, Ethereum emerged to provide the innovative ability to execute computer programs in a decentralized way that achieves consensus among distributed systems. In this whitepaper, we discuss a cryptocurrency design that focuses on the privacy of its users, Ghost.

Ownership of Funds in Bitcoin

Bitcoin uses the 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 the 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],

[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.

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. Attempts to get rid of *ASICs* have been sky-rocketing 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, leading 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 was 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 on 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 coin over its history.

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

The Ghost project utilizes 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.

Cold-Staking

Staking (i.e. using proof-of-stake to participate in the network) practically requires the owner of the cryptocurrency funds to keep their wallet software open, so that blocks can be generated and signed using the private-keys that hold said funds. However, this can be very risky. If someone 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 is a mechanism through which funds are delegated to a cold staking pubkey to stake the delegated inputs[13]. The *hot-storage* (i.e. staking software) is only allowed to sign transactions that perform the staking. Therefore, it is ensured that a breach will never result in users funds being stolen.

[13] A cold-storage, as opposed to hot-storage, is a method for storing cryptocurrency funds in which a wallet that controls the private-key is not connected directly to the internet. A good example of this are hardware wallets, such as Ledger Nano and Trezor.

Privacy

What is Privacy in Blockchain and How It Can Be Improved

Privacy in a cryptocurrency generally entails hiding three elements in a transaction:

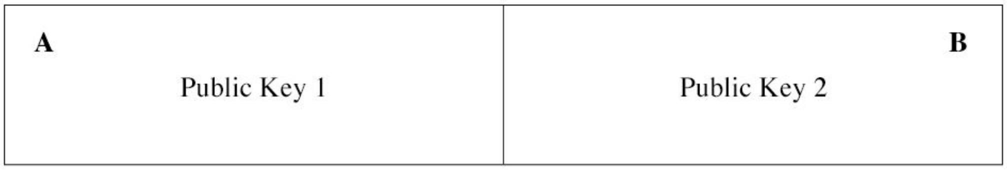
1. The receiver of the transaction
2. The sender of the transaction
3. The amount being sent

Hiding Receiver's Address

In Bitcoin, as discussed before, a receiver's address is directly calculated from the public-key, which in turn is derived from a private-key, that is to be used to spend funds from that address. This directly means that an address can always be reused, and will always point to the owner of the private key. Accordingly, participants can always know how much every address owns, and where the funds went from that address. Consequently, leading to their traceability. As a result, users are exposed to the study of their financial habits, social engineering and overall scrutiny from others, in particular public entities (i.e. Governments).

To solve this problem, instead of a normal address, Ghost employs *Stealth Addresses*[14]. In the following, greater detail on how this works is provided.
A stealth address consists of two public-keys, let's call them (A, B). We call the private keys associated with these (a, b) [15]. The first public-key A is associated with the private-key allowed to spend the funds sent to that address, and the second public-key B is used as part of an agreement protocol called the *Diffie-Hellman protocol*.

[14] Stealth addresses were first introduced in the Cryptonote protocol [Van12].
[15] If we call the base point in the used Elliptic Curve G, then $aG=A$ and $bG=B$.



Stealth Address

Say that Alice and Bob want to communicate over an insecure channel. Both have the ability to generate private keys, and the associated public keys. But they need a way to transmit information securely over that unsecure channel. *The Diffie-Hellman protocol* solves this problem by making it possible to create a shared key between the sender and receiver by only sharing their public-keys. The agreement basically implies that Alice sends Bob her public-key, and Bob sends Alice his. Immediately after that, they can combine their private-keys with the other's (Alice's private key with Bob's, and Bob's private key with Alice's) to create a shared secret key, which they can use to encrypt any communications between them[16].

The second public-key in a stealth address B acts as one public-key in the *Diffie-Hellman protocol*. The creator of a transaction generates a random private-key, let's label it r, and combines it with the second public-key of the stealth address. Then, the public-key R is calculated from the private-key r, and is added to the transaction. The receiver of the transaction can use the view key's private key b, and combine it with R, that was included in the transaction, to recover the shared secret.

Finally, after having created the shared secret, the creator of the transaction also combines it with the first public-key A of the stealth address. The result is a new

[16] If the base point of the Elliptic Curve is G, and if we were to label Alice's private-key and public-key $xG=X$ and Bob's private-key and public-key $yG=Y$; the Diffie-Hellman protocol's shared secret is $xY=yxG=xyG=yX$. Hence, either Alice or Bob can use their private-key and the other's public-key to arrive at the same shared secret xyG.

random address (since r is a new random private-key) that can only be revealed by the owner of the second private-key B of a stealth address (called the view key), and can be spent only by the owner of the first and second private-keys (a, b) of the stealth address (the spend key).

In this way, every time someone sends a transaction to a stealth address, a new public-key (and hence, effectively, a new address) can be generated, which makes traceability and linkability of transactions practically impossible.

Hiding The Sender/Signer of a Transaction

Since inputs are funds that are to be spent, the sender has to verify that they are authorized to spend them. In bitcoin, every input must be accompanied with a digital signature that shows that the creator of this transaction authorized spending it. While this works flawlessly, it can be used to trace transactions and their history and link spends together to recognize user behavior. This is considered to be an issue in the privacy of bitcoin.

As also demonstrated by this project, a potential solution to this issue can be the use of digital signatures to obfuscate the real signer of the transaction. This technology is commonly referred to as *ring-signatures*.

Ring-Signatures

To explain how *ring-signatures* work, let’s use the following example. Say that Alice works for a corrupt governmental institution. Alice is a trustworthy person, and while doing her job, she got her hands on documents that are considered evidence of the corruption that she wants to stop. She now wants to release this information to the public. However, if she does so, her employer will always have plausible deniability claiming that these documents did not originate from within the institution, deeming her efforts a waste. On the other hand, if she uses her official institutional private/public key pair to sign these documents, she risks incriminating herself (i.e., like Edward Snowden did by releasing government information to the public). What can she do?

The potential solution: *ring-signatures*. Along with her private key, Alice can take the public keys of 9 other officials, and create a *ring-signature* of these documents. The *ring-signature* reveals all the public-keys that signed the documents. It, however, does not reveal who the actual signer is (i.e. the person who used his private key to sign the document). There is no practical way to confirm that Alice is the one who in fact authorized this signature. This way, Alice maintains plausible deniability, while at the same time, giving credibility to the signed documents, proving the corruption she wants to make public.

In essence, *ring-signatures*, instead of just using a single private-key to sign a transaction, involve a set of public-keys of involuntary individuals, which are randomly picked from the blockchain, called decoys. This way, a transaction with a ring-size of 10, will have 10 participants, any of whom could have potentially signed that transaction. Any creator of a transaction maintains plausible deniability on who signed the transaction. More importantly, this technology when combined with stealth addresses, means that a transaction will never see the same private key again, making it even harder to link or trace any transactions together.

Hiding The Amounts Sent on the Blockchain

Bitcoin uses clear amounts written on the blockchain to indicate the numbers a transaction contains in its inputs and outputs. This makes it easy to track people who have large balances and aids social engineering and ransom crimes, where the blockchain can be analyzed to find who the senders and receivers of significant transactions are. To solve this problem, a mechanism can be used that hides the amounts in a transaction, while at the same time maintaining their sanity (to prevent sending "negative" amounts or sending money that does not exist).

To illustrate in the simplest way how the amounts are kept a secret and at the same time verified to be valid publicly, consider the following setting. Alice wants to send 10 coins to Bob. Assume that Alice has two inputs that amount to 12 coins (4 and 8). The transaction will look as follows:

$$4 + 8 \rightarrow 10 + 2$$

Where the left-hand-side represents the inputs, and the right-hand-side represents the outputs, where Alice returns 2 coins to her own address. Let's also ignore transaction fees. What can Alice do to hide the amounts in such a way that only Bob can view them, while at the same time allowing miners to verify the transaction's sanity?

A simplified solution would be the following. Remember stealth addresses consist of a view key and a spend key. What can be done is, construct a Diffie-Hellman (as discussed previously) shared secret key using the view key, let's call it *k*, and since the shared secret key is just a huge integer number, we multiply that number by the whole transaction showed above:

$$4k + 8k \rightarrow 10k + 2k$$

If we assume that $k = 50$, the equation becomes

$$200 + 400 \rightarrow 500 + 100$$

A validator can ensure that this transaction is valid, because the total in inputs still is equal to the total in outputs. Therefore, enabling him to perform his task without having to know the original amounts.

RingCT

The discussion above is a simplified one on how hiding amounts and ring-signatures work, when compared to reality in present times. Current technology has progressed and *ring-signatures* are now combined with hiding amounts in what is called *RingCT*, or Ring Confidential Transactions. Initially starting from *Borromean signatures* by Gregory Maxwell et al [Max15], these were expended by Shen Noether's et al [Noe16].

Taking it one step further, RingCT can also be combined with *Bulletproofs* [Bue17] (Which is already part of Particl & Ghost codebase), to prove that transaction inputs and outputs fall within the allowed range (i.e. no negative output amounts or overspend occuring).

Particl

Derived From Bitcoin

Particl, along with many others, began as a fork of bitcoin. Their idea is aimed at adding new technologies on top of the success bitcoin has already achieved. Primarily, adding confidentiality to every aspect of the chain and implementing proof-of-stake to move away from a proof-of-work consensus mechanism for block generation.

Through forking of source code, new projects are able to focus on the constant updates and upgrades of a network as the solid architecture already exists. By leveraging the present foundation on which to build upon, projects are often able to predominantly place their efforts on a specific focus point. Like Ghost, in this project's specific case, it is privacy.

Peer to Peer Marketplace

Particl's blockchain offers a decentralized, anonymous and private marketplace for the buying and selling of goods between users on the network. Any user of their blockchain can list goods or services for sale publicly, and have their listing bought without anyone else on the chain knowing who actually bought or sold it.

Withal, this open marketplace offers *TOR connectivity*, which allows the buyer and seller to be connected to the chain from a TOR IP meaning their originating IP is masked during the transaction. Payments are also handled using the CT and RingCT technology previously discussed. This means that the seller and buyer can anonymously send and receive funds to a stealth address without any way to track the end users.

While the listing itself can be made public, allowing it to be searchable and categorised on the market place frontend, the originating IP and user details are not provided. With the only identifier being an anonymous vendor ID that isn't connected to the user in any traceable way.

The project strives to offer complete privacy when transacting and its market place delivers on this promise. It's a completely anonymous quasi peer-to-peer system running entirely on its own network.

Encrypted Chat

Their network daemon also supports a secure messaging protocol called *SecureMessaging*. This system is built entirely in C++ and runs on the existing network infrastructure[17]. In a broad sense, as a user sends an encrypted message that message is protected by a hash which tells the nodes on the network which node is eligible to decrypt the message. This message is then broadcasted and encrypted, across the entire network and every node will make an attempt to decrypt the message. If they are the designated node, they will be successful and the message will be sent to the user for viewing.

Their hashing process uses a method called *HMAC*[18]. The chat packet will have an added component, the hash, that consists of the *DSN* (Data Storage Network) ID of the receiving node or the public key of that node. As the message is broadcasted over the network, every node will attempt to reverse that hash. However, if they fail to do so, then the message is either faked, incorrect or not designated to them and they will do nothing but store that message for 48 hours.

This process is explained more in the marketplace section of this whitepaper as the *SSMS* function is also used as their DSN provider for the marketplace.

[17] https://github.com/particl/particl-core/tree/master/src/smsg

[18] HMAC, or Hash-based Message Authentication Codes, is a cryptographic tool to verify the authenticity and data integrity of a message. It combines a key and a hashing function, in such a way, where if the verifier has the key,, they can verify that no one tampered with the message except for those who have that key.

Why Particl?

When Ghost was initially started, it was an unanimous decision from the development team to fork the codebase from this open source project[19]. Further to their initial bitcoin fork,[20] they have extended the functionality of their network in a direction that similarly aligned their goals with the ones Ghost has.

[19] https://github.com/particl

[20] https://github.com/particl/particl-core

Ghost

Enhanced Privacy

Ghost currently uses RingCT and stealth addresses as means to secure the privacy of the users and retain their anonymity while transacting on the network. However, the project is committed to staying at the top of privacy technology, in addition to establishing research into better anonymity with lower cost in size and computation to prevent *Denial-of-Service attacks*.

One of the technologies that is under research to be implemented in the Ghost infrastructure is *Triptych ring-signatures* [Noe20], which improves the space complexity of ring-signatures from `O(1)` to `O(log(N))`. This reduces the amount of disk-space required to store ring-signatures significantly, allowing hundreds of decoys in a ring-signatures, instead of a few tens, at the same cost.

More Privacy - Dandelion++

Dandelion++ is a lightweight and straightforward network layer solution with formally guaranteed anonymity [Fan18] that can be implemented into existing cryptocurrencies.

Usually, cryptocurrency transactions are broadcasted across the network using the Gossip protocol, in which every node sends the transaction to all the nodes, to which it is connected. While the current system is efficient, it is also possible to de-anonymize the original sender of the txs [Fan18]. *Dandelion++* makes a simple but crucial change to the current transaction broadcasting pattern.

Instead of sending transactions to all connected nodes on the network, *Dandelion++* initially sends them to only one other node. This next node then randomly decides if it broadcasts the transaction on to just one, or all of its connected peers. With the introduction of the element of chance, the propagation pattern now becomes unpredictable, making it infeasible to trace a specific transaction back to the original tx broadcaster's IP address. This is especially useful in a privacy focused cryptocurrency, such as Ghost, in order to keep your transaction from being traced back to your IP address, which ultimately would de-anonymize the sender's approximate location based on their IP address.

Masternodes (Ghost Veterans)

After much thought, Ghost has decided not to implement masternodes. The project believes the lack of any substantial functionality improvements for the network coupled with it's inherent drawbacks simply do not hold up to the standards the group has for the project. These include:

- DIP3 Masternodes and its dependencies are not required to achieve any of the goals we have for the project.
- Complicated to set up for most new users who have no prior knowledge of the protx system.
- Potential network and security instability.

However, **Ghost is not** adjusting the reward structure that was in the original plan. Instead, a new initiative will be released to replace it - *Ghost Veterans*. Mentions of "Masternodes" on the website[21] can now be assumed to refer to this program.

The Ghost Veterans will consist of a separate pool of GHOSTS that have been accumulated for each block over a period of 30 days. To be eligible to receive these rewards, user must meet the following requirements in a 30 day reward period:

[21] https://www.ghostbymcafee.com/

1) Perform a public transaction of at least 20.000 GHOST to verify holding balance.

2) Funds not to be spent or moved in any way during this time[22].

For multiples of 20,000 GHOST where the requirements above are met their reward will be increased accordingly. For example a user with 40,000 GHOST will receive twice as much as someone who has 20,000 GHOST.

Users will also be allowed to stake their coins concurrently, earning GHOST each time they successfully create a block (i.e. staking will not disqualify you from earning Ghost Veteran rewards)

By adopting this reward structure, Ghost Veterans will not need to undergo the complex process of installing and running a full node as they would have otherwise had to. They will also be free from having to continuously keep their wallet open or perform any sort of advanced technical requirements.

Reward Structure

GHOST utilizes an inflationary reward structure, commonly seen in PoS networks. Every 120 seconds (2 minutes) a new block is created on the network, thus minting 12 GHOST coins (6 GHOST per minute) that are ultimately adjoined to the total supply following this reward structure:

6 GHOST are allocated to the Ghost Veterans reward pool.
4 GHOST goes to the staker that creates the block..
2 GHOST are distributed to a dev fund for future development.

[22] An exception to this rule is staking. Even though staking is considered a kind of spending outputs, outputs that are staked are still considered in the Ghost Veteran Reward. The only other exception is the 1 public transaction required to verify funds on the account.

** This structure is subject to change, given community approval, and likely to decrease as the network reaches maturity.*

After the first two years, the emission rate above will be reduced every year by approximately 5%. The equation that governs the inflation rate every year is:

$$12\frac{\mathrm{round}\left(100 \times 0.95^{n}\right)}{100}$$

The emission rate will remain at 100% (i.e. 12 GHOST), for the first two years (6 for ghost veterans, 4 for stakers, 2 for dev fund). Then it will fall until it reaches 10%. Once 10% is reached (in around 45 years in the future), it will never reduce further. This will provide an incentive for stakers to keep staking.

The dev fund is distributed to the administrators, core developers of GHOST, and will primarily be used to fund community bounty projects as well as new features.

The reward payouts happen automatically at the correct block heights for the period without user intervention. With this method there are multiple avenues for a standard user to participate in the network and earn GHOST.

Quantum Resistance

Public-key cryptography, the kind of cryptography that bitcoin uses, can be relatively easily broken with Quantum Computers[23] using *Shor's algorithm*, which cannot be done in classical computers[24] and is the basis of the security of bitcoin and many other

[23] 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.

[24] 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.

cryptocurrencies. What quantum computers could do is recover the private-key from the public-key relatively fast[25]. Luckily, quantum computers do not exist yet, but are destined to appear and become more popular in the future. While companies are promising "*quantum chips*" in the near future [IBM17], skeptics still believe quantum computers are not gonna show in our lifetimes [Dya18]. In this atmosphere, cryptocurrencies should prepare for this "quantum threat".

In fact, for newly created private-keys that have never spent any outputs that use the associated addresses, bitcoin is already safe against quantum computing. Remember that bitcoin addresses are generated from public-keys. These addresses are calculated by hashing the public-key. Quantum computers cannot break hashes compared to classical computers[26]. However, if anything is spent from that address, the public-key will be revealed on the public blockchain. In the presence of quantum computers, this will become a threat.

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.

Address aliases

Another upcoming feature to the Ghost blockchain is the ability to send funds by a reserved alias that corresponds to a stealth address. The project is motivated to

[25] In theory, it is possible to calculate the private-key from the public-key in classical computers, but even with a super-computer it, realistically, takes a couple million or even billion years.

[26] In fact, quantum computers are much faster than classical computers in breaking hashes, however, it is not fast enough. By using the quantum algorithm named Grover's algorithm, searches can be done with time complexity O(sqrt(N)), where sqrt is square-root, compared to classical computers that require O(N) search complexity. In other words, assuming everything is equal, it will take square-root the time to break a hash in a quantum computer, but that is not good enough to be a threat.

implement this to ensure convenience and privacy for everyone involved in the ecosystem. While this feature is not particularly new, as it has been done through services that provide DNS information for cryptocurrencies, Ghost believes that such a service centralizes cryptocurrencies. Our solution to this problem will be aliases that are defined on a decentralized network. This will be independent of any third parties and as such, 100% decentralized.

One of the serious issues of aliasing is the ability to link names to addresses, and hence to amounts. If someone decides to use their first name and last name as an alias or if the same is used everywhere, their balances are likely to become public. As such, these problems stand against the very principles of Ghost, where privacy of our users is of the utmost importance.

To solve these problems, Ghost will only allow address aliases by utilising underlying stealth addresses to process link to. Given that stealth addresses generate a new effective address with every transaction, there is no way to link or track the balance of any user by their alias.

In order to embed the address vs alias in the blockchain, we will use the `OP_RETURN` output type. When a new alias is to be created, a new transaction should be created with an `OP_RETURN` output. That output will contain the following following data

Size	Type	Data
1 or more	*Variable length integer*	Protocol version number, in big-endian format
1 or more	*Variable length integer*	Function or storage ID, which is the purpose of this function, in big-endian format
2	*Integer*	Size of alias string
Variable	*Binary data*	The binary data that represents the alias

2	*Integer*	Size of address string
Variable	*Binary data*	The address that the alias points to

As can be seen, this is an example of the protocol that will be used to add extra decentralized functionality to Ghost that is part of the consensus.

When creating a transaction that utilizes this, the protocol itself will be responsible for checking whether the alias is taken. With the owner of the private-key of the input also being able to perform this query.

To prevent spam, reserving a large number of aliases will cost roughly a transaction fee equivalent to ~$5 USD, which at the time of writing will be set at 5 GHOST. This amount is subject to change in order to remain affordable. Fees collected will be burnt and will no longer be part of the network.

How does it work? When scanning the blockchain, the GHOST node software will read the transactions that follow the format from the table above. When such a transaction is detected, the node software stores the alias, address and the transaction that created the alias in the key-value store[27].

When a transaction is to be created to send funds to this alias, the key-value store will be polled to check if the alias is used. Then, the wallet software will check whether this transaction is in the main chain. In addition, it will ensure that the chain is synced, so that overwritten addresses are not used. Then, the destination address of the alias will be used to create the transaction. The user will not notice any of these details, and it will look to him as if the alias is the true address.

[27] Currently, leveldb is used as a key-value store for GHOST, but this may change in the future.

Community Powered

One of the main ethos of the Ghost project is transparency within privacy. This means we aim to be completely transparent with the public about what we are doing and why, without breaching the privacy of the users on the platform. Our community driven development is one way we are hoping to achieve this.

GHOST holders will have the opportunity to vote on future developments and roadmap changes with the development fund being used to finance these new initiatives. Ghost hopes to drive the project forward through community involvement, achieving a product that fits with what the users want whilst maintaining the desired high level of security, privacy and functionality.

Voting will be simple, a user can pay a small amount of GHOST to put forward a topic for consideration. This can be any new feature they think the platform could benefit from. From there, any user can put through a vote using one of the pre-existing platforms. Their vote will be weighted based on the amount of GHOST that they hold.

If the vote meets a minimum threshold, it will be considered approved. This is consequently forwarded to the team to allocate funds from the dev rewards and ultimately creating a bounty for the tasks involved in that project. 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 tokens for their work. Public members will submit a PR for approval by the core team, just as a core team member would have to.

This entire process helps bring a whole new perspective to blockchain development and the crypto space in general. Users having a say in how the project moves forward gives a level of transparency and direction which is rare within this space.

Extend Encrypted Chat to a Mobile App, “Telaghost”

A decentralized private network that can communicate anonymously should be utilized for so much more than just sending numeric values back and forth. A driving factor in Ghost’s mission is to provide substantial value in unique external products and services. A network can only be as valuable as the utility it provides.

The goal is not to simply create a brand new chat application and force users to yet move to another platform, lose all their messages and contacts. This is not practical and would be a major hurdle to overcome for adoption. That is why the project plans to have full integration with the Telegram[28] network as a hybrid solution. This will allow a user to login with their existing account, have access to the same contacts, same groups, and setting. Ghost will provide additional functionality on top of their platform[29] which will allow users on the application to access private chat, send/receive GHOST, start private groups, as well as additional features to be announced. This app will be for iOS, Android, as well as desktop versions for PC, MacOS, and Linux.

Future development plans and specific details for the encrypted mobile application, “Telaghost”, will be published in a separate document soon. This is a high priority item on the roadmap.

Google Chrome & Firefox Wallet Extension, “MetaGhost”

As with any new network launch, one of the major issues is adoption. Users are accustomed to existing solutions because of familiarity, ease of use and convenience. This makes it less likely that a user will adopt a new wallet for example.

[28] https://telegram.org/

[29] https://core.telegram.org/tdlib

Ghost could spend over a year to create something brand new and another year trying to get people to use it. However, the project decided a preferable alternative would be to build on an existing popular solution. MetaMask[30] is an open source project[31] that has been widely adopted by various online services [Yah19]. It is a browser extension that allows you to run dApps [Cho18] without being part of the Ethereum network as a Ethereum Node. This has created many instances for users to interact directly with websites to send and receive Ethereum and ERC-20 tokens[32].

The project's goal is to take the same functionality that already exists within MetaMask and the ethereum network and add additional support to connect to the Ghost mainnet as well. This will provide users with the same convenience and ease of use that they are familiar with, while adding an additional layer of privacy that can be utilized as needed. Future plans to have an Ethereum based wrapped GHOST token, paired with Atomic Swaps on the network, will allow for seamless integration into the many features of MetaMask compatible websites, while utilizing the privacy benefits of the Ghost network. In addition, will also make it possible for Ghost to become part of DeFi[33].

In short, users will be able to directly spend their GHOST coins (on the mainnet) through MetaMask compatible websites (using a wrapped ERC-20 Ghost token) while remaining anonymous on "MetaGhost".

[30] https://metamask.io/

[31] https://github.com/MetaMask

[32] ERC-20 is a protocol on the Ethereum blockchain that allows for creating tokens for assets.

[33] DeFi, or decentralized finance, is a set of protocols on the Ethereum blockchain that replace traditional finance, where it is possible to run entities like central banks, make loans, short, long, and many other financial services; all on the blockchain.

Future Developments

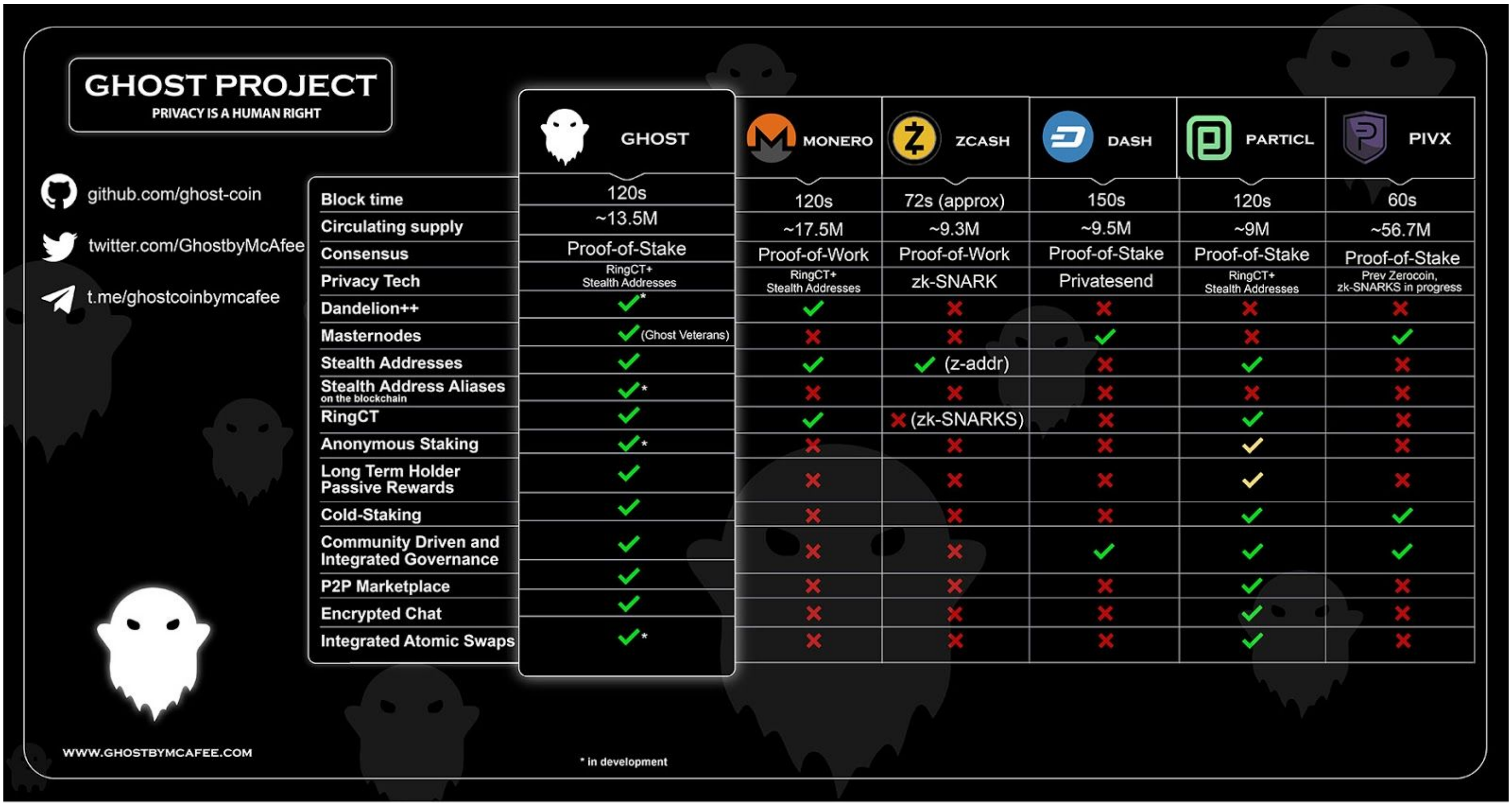
The direction of Ghost must be ever changing to successfully adapt in a notably evolving marketplace where new challenges and obstacles appear quickly and demand attention in the same manner.

The whitepaper and the features we have outlined thus far is only the beginning for Ghost. In order to truly encompass the vision whilst maintaining a stable and secure solution, GHOST coin holders must be offered the means to be empowered. Collectively, they should be the ones to make a change, not a single entity.
This ideology is considered one of essential pieces that truly makes this project unique. Ghost is committed to allocating the majority of the developer fund pool to go towards funding community-approved proposals, and allowing these changes to be approved or denied by the community.

Ultimately, in the future, Ghost wants to continue expanding its own ecosystem of products and services while bridging the gap between existing platforms.

Comparison Diagram

In the following, we compare Ghost alongside other cryptocurrencies with relevant features that have been discussed thus far:



GHOST PROJECT
PRIVACY IS A HUMAN RIGHT

github.com/ghost-coin
twitter.com/GhostbyMcAfee
t.me/ghostcoinbymcafee

	GHOST	MONERO	ZCASH	DASH	PARTICL	PIVX
Block time	120s	120s	72s (approx)	150s	120s	60s
Circulating supply	~13.5M	~17.5M	~9.3M	~9.5M	~9M	~56.7M
Consensus	Proof-of-Stake	Proof-of-Work	Proof-of-Work	Proof-of-Stake	Proof-of-Stake	Proof-of-Stake
Privacy Tech	RingCT+ Stealth Addresses	RingCT+ Stealth Addresses	zk-SNARK	Privatesend	RingCT+ Stealth Addresses	Prev Zerocoin, zk-SNARKS in progress
Dandelion++	✓*	✓	✗	✗	✗	✗
Masternodes	✓ (Ghost Veterans)	✗	✗	✓	✗	✓
Stealth Addresses	✓	✓	✓ (z-addr)	✗	✓	✗
Stealth Address Aliases on the blockchain	✓*	✗	✗	✗	✗	✗
RingCT	✓	✓	✗ (zk-SNARKS)	✗	✓	✗
Anonymous Staking	✓*	✗	✗	✗	✓	✗
Long Term Holder Passive Rewards	✓	✗	✗	✗	✓	✗
Cold-Staking	✓	✗	✗	✗	✓	✓
Community Driven and Integrated Governance	✓	✗	✗	✓	✓	✓
P2P Marketplace	✓	✗	✗	✗	✓	✗
Encrypted Chat	✓	✗	✗	✗	✓	✗
Integrated Atomic Swaps	✓*	✗	✗	✗	✓	✗

WWW.GHOSTBYMCAFEE.COM

* in development

** full resolution version of this image can be found at:*
https://www.ghostbymcafee.com/assets/ghost-project-chart.jpg

Ghost Operational Specifications

In the following, we share the operational specs of the Ghost cryptocurrency

- Block time: 2 minutes
- Max Block size: 8 MB
- Consensus mechanism: Proof-of-stake
- Cold-staking: supported
- Atomic swaps: Will be supported in the future
- Emission rate: 12 GHOST per block for the first year; then following the equation, where n is the year number calculated in blocks:

$$12\frac{\text{round}\left(100 \times 0.95^{n}\right)}{100}$$

This rate will be followed down to 10% of 6 GHOST. Once that is reached, the block reward will remain 0.6 GHOST forever.

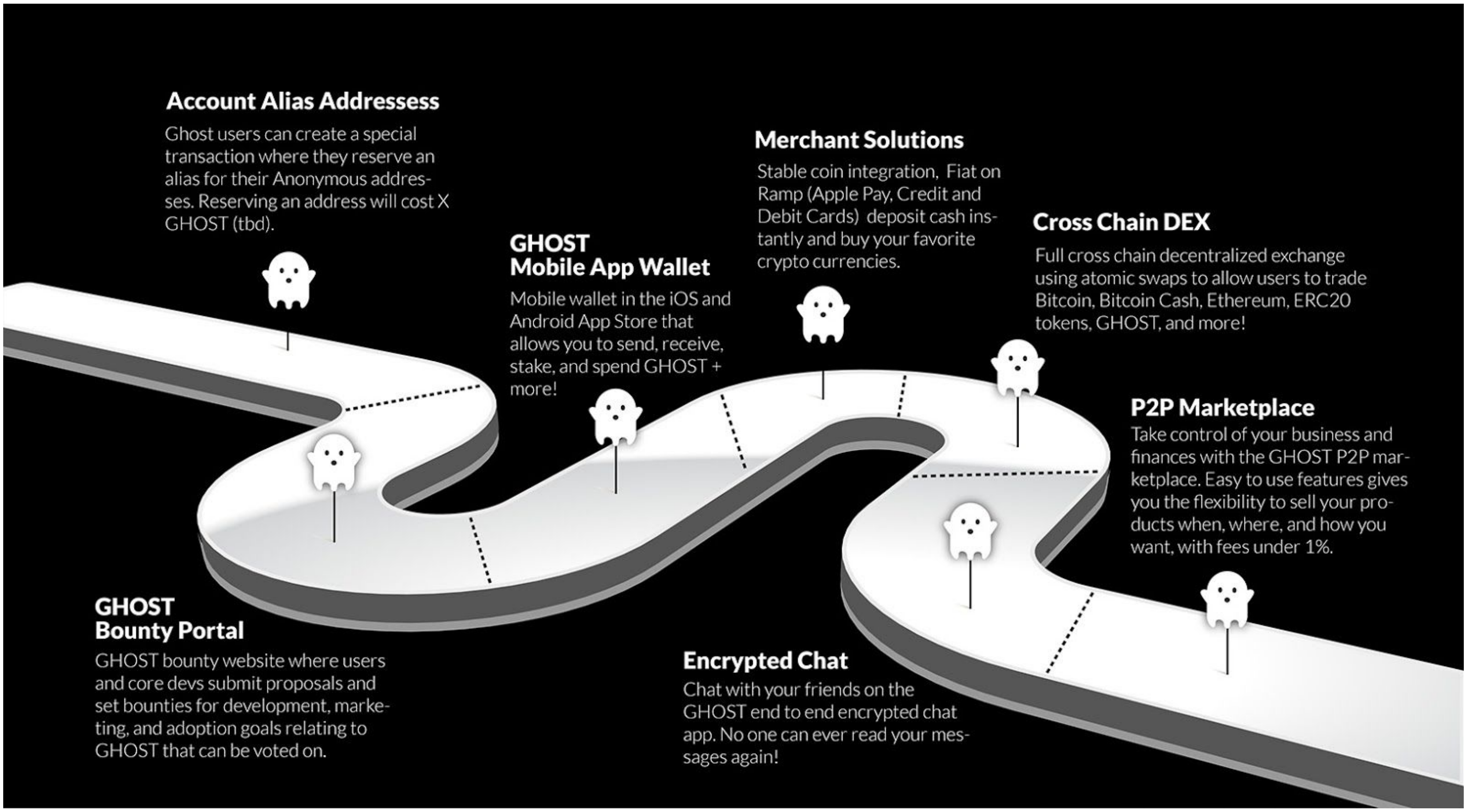
- Rewards, out of the mentioned above:
  - 50% for cold-rewards (Ghost Veterans)
  - 33% for stakers
  - 17% for dev fund
- Coinstake maturity: 225 confirmations
- Privacy: Both anonymous (using RingCT and stealth addresses) and non-anonymous transactions exist[34]
- Hardware wallet support: Several, to be supported in the very near future.

[34] In the future we will be removing non-anonymous transactions completely. They exist now for operational necessity to allow staking to work.

Team & Contributors

John McAfee	founder
Tech pioneer, computer programmer, and security expert. Founder of McAfee AntiVirus and proof of stake privacy coin GHOST.	
reborn1002 dev / project mgr	Developer with 10 years of experience C++, C#. Contributed to Fortune 100 company projects.
TheQuantumPhysicist lead dev	PhD in Particle Physics. Bitcoin & Monero contributor, and a blockchain developer. Expert in computer security with a focus on cryptocurrency.
Akshay CM Core dev	PIVX, ZCoin & Qtum contributor. Experienced C++ dev that is well rounded and knowledgeable in the cryptocurrency space.
Kaddar Core dev	Network Engineer & Developer with CS Degree. Knowledge in C++, JS, Solidity and a deep understanding of the blockchain.
Luna full stack dev	Solidity Developer. Engineering Manager for a large financial provider.
Joao full stack dev	Switch & DEX contributor. Experienced in Angular, PHP/HTML/JS. Ghost Wallet developer.
melvin web dev	Switch & DEX contributor. Experienced in Angular, PHP/HTML/JS. Ghost Wallet developer.
Luis community	Community / Digital Marketing
Geo biz dev	Business development, user adoption, exchange relations, and marketing.

Future Roadmap



Account Alias Addressess

Ghost users can create a special transaction where they reserve an alias for their Anonymous addresses. Reserving an address will cost X GHOST (tbd).

GHOST Bounty Portal

GHOST bounty website where users and core devs submit proposals and set bounties for development, marketing, and adoption goals relating to GHOST that can be voted on.

GHOST Mobile App Wallet

Mobile wallet in the iOS and Android App Store that allows you to send, receive, stake, and spend GHOST + more!

Merchant Solutions

Stable coin integration, Fiat on Ramp (Apple Pay, Credit and Debit Cards) deposit cash instantly and buy your favorite crypto currencies.

Cross Chain DEX

Full cross chain decentralized exchange using atomic swaps to allow users to trade Bitcoin, Bitcoin Cash, Ethereum, ERC20 tokens, GHOST, and more!

Encrypted Chat

Chat with your friends on the GHOST end to end encrypted chat app. No one can ever read your messages again!

P2P Marketplace

Take control of your business and finances with the GHOST P2P marketplace. Easy to use features gives you the flexibility to sell your products when, where, and how you want, with fees under 1%.

** full resolution version of this image can be found at:*

https://www.ghostbymcafee.com/pdfs/GHOST2020_Roadmap_v1.0.2.jpg

Acknowledgements

This paper was prepared in collaboration by the Ghost Team.

We would especially like to thank Particl and their talented development team. In terms of privacy, their consensus algorithm, updated bitcoin codebase, clean code and already existing features, the decision to fork them was a rather easy one.

Finally, we would like to thank our community who have supported us from a very early stage. We look forward to continuing working together on our shared vision for Ghost.

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

[Noe20] Noether, S. (2020) *Triptych: Logarithmic-Sized Linkable Ring Signatures With Applications, Monero Research Labs, May 18th.* Available at: https://eprint.iacr.org/2020/018

[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

[Yah19] Dantoni, J (2019) *MetaMask Releases Metrics That Show How It's Being Used, Yahoo Finance, May 25th.* Available at: https://finance.yahoo.com/news/metamask-releases-metrics-show-being-224953895.html

[Cho18] Choi, S (2018) *What is MetaMask? Really...What is it?, Medium, July 18th.* https://medium.com/@seanschoi/what-is-metamask-really-what-is-it-7bc1bf48c75

[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

Note: All links have been visited and the content is verified upon the release of this document