RHOM: A Decentralized Privacy-Focused Cryptocurrency

info@rhom.com
www.rhom.com

1. Introduction

"It's better to have privacy and not need it, than to need privacy and not have it."

Rhombus Coin, RHOM, is a decentralized and privacy-focused, untraceable, Proof-of-Stake cryptocurrency that can be sent without going through financial institutions. If desired, RHOM can be sent without disclosing who is the sender or the amount being sent. Rhombus has three levels of privacy. They are anonymous, blind, and public. Each level of privacy provides its own use case that has its own degree of traceability and cost.

A blockchain is a digital record of transactions. The name, blockchain, comes from its structure, in which individual records, called blocks, are linked together in a single list, called a chain. Blockchains are used for recording immutable transactions made with cryptocurrencies, such as RHOM or Bitcoin. Blockchains in cryptocurrencies enable peer-to-peer electronic transfer of value by maintaining a globally distributed but synchronized ledger, also known as a blockchain. Any independent observer can verify both the current state of the blockchain as well as the validity of all the transactions on the ledger through an online block explorer. In Bitcoin, all the details of a transaction are transparent including the sender, the receiver, and the amount transferred. For the purposes of cryptocurrency transactions beyond the public ones Bitcoin provides, Rhombus separates privacy for payment into two properties anonymity, hiding the identities of the sender and receiver in a transaction, and confidentiality, hiding the amount transferred. While Bitcoin provides some weak anonymity through the unlinkability of Bitcoin addresses to actual users, Bitcoin lacks any confidentiality. This is a serious limitation for Bitcoin and could be prohibitive for many use cases. For example, does a shopper going to a supermarket to buy some apples want the cashier to know their checking account balance and they're just coming from the candy shop?

2. Transactions

"Only love continuously flows, everything else is a confirmed or unconfirmed transaction."

Cryptocurrency users have a common misperception that Bitcoin transactions are private. In fact, Bitcoin transactions are mostly public. Balances and past transactions are transparent because they can be examined through an online block explorer without the sender making the choice for that information to be public. The Rhombus blockchain allows cryptocurrency transactions to be anonymous and secure. Eventually, either because transactions are large amounts or senders or receivers are of note, their transactions history will be examined. Rhombus uses Ring CT and Bulletproofs innovations and technology to keep transactions anonymous and secure.

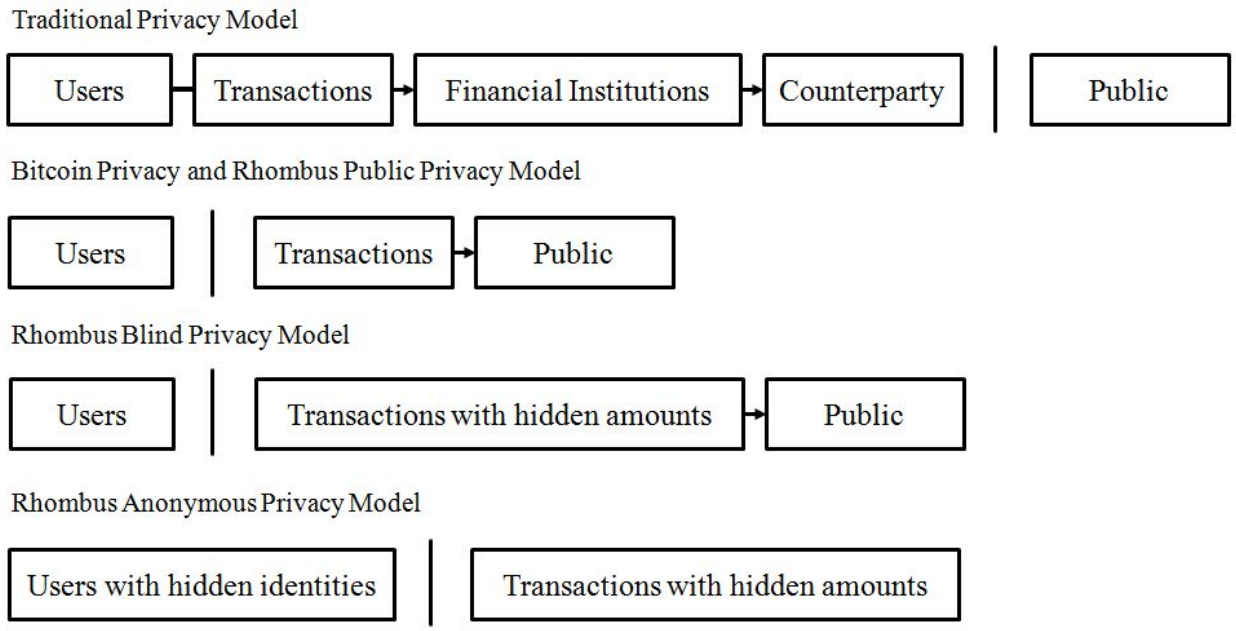
The Confidential Transactions (CT) protocol is used for blind transactions. CT hides transaction amounts from third parties (e.g. financial institutions) - keeping them private. Ring CT enhances RHOM privacy by hiding the transaction participants' identities. Moreover, blind transactions in Rhombus hide transaction amounts, and anonymous transactions in Rhombus hide transaction amounts and participants' identities.

3. Privacy

"As your net worth increases, so does your need for privacy."

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and trusted financial institutions. Bitcoin announces all transactional information but keeps public addresses anonymous. Other cryptocurrency users can see that someone is sending an amount to someone else, but without information linking the transaction to anyone specific.[1] Without a privacy coin like RHOM, there is a 100% probability that some transaction details users prefer to keep private will become public. Rhombus enables cryptocurrencies users to protect themselves from unwarranted interference in their lives by introducing new innovations, Ring CT and Bulletproofs. This additional privacy provided by Rhombus allows cryptocurrency users to negotiate with other cryptocurrency users without disclosing information about their bargaining position.

[1] Nakamoto, Satoshi. "A Peer-to-Peer Electronic Cash System." *Bitcoin*, 2009, bitcoin.org/en/bitcoin-paper.



4. Rhombus Technology

"The privacy technology of the future is here, but needs to be distributed."

a. Ring CT

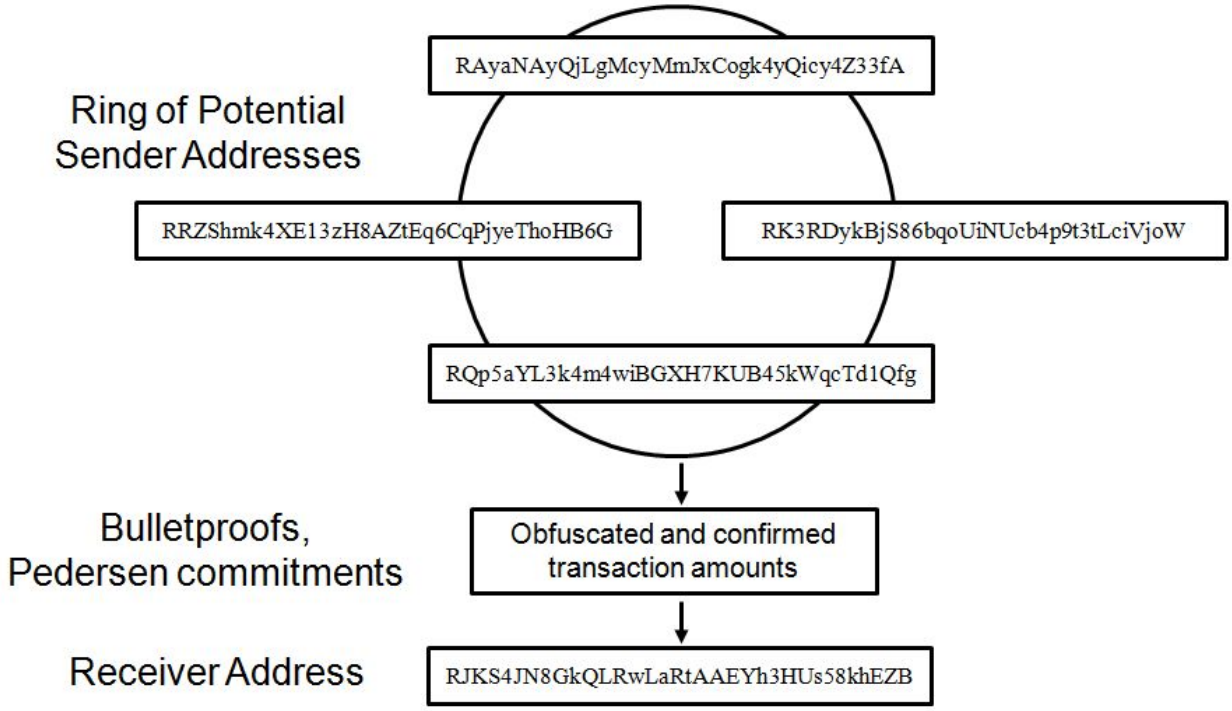
Ring CT, used by RHOM, is a follow-on innovation to a CoinJoin technique described by Greg Maxwell.[2] Shen Noether further lays out the Ring CT technique in his 2015 paper on Ring Confidential Transactions.[3]

b. Bulletproofs

Bulletproofs are designed to enable efficient confidential transactions in cryptocurrencies like Rhombus. Confidential transactions hide the amount that is being transferred in the transaction. Every confidential transaction contains a cryptographic proof that the transaction is valid. Bulletproofs are a follow-on innovation to a technique called zero-knowledge proofs. Moreover, Bulletproofs significantly shrink the size of these cryptographic proofs.

[2] Maxwell, Greg. "Coinjoin: Bitcoin Privacy for the Real World." *Bitcoin Forum*, Aug. 2013, bitcointalk.org/index.php?topic=279249.0.
[3] Noether, Shen. "Ring Confidential Transactions." *Cryptology ePrint Archive*, 2015, eprint.iacr.org/2015/1098

Benedikt Bunz explains Bulletproofs in his Bulletproofs: Short Proofs for Confidential Transactions and More.[4] Confidential transactions are transactions which are publicly verifiable but do not reveal the amounts that are transferred. They rely on cryptographic commitments (e.g. Pedersen commitments) and zero-knowledge proofs. Bulletproofs are a new kind of zero-knowledge proof which is much more efficient and can be used to drastically reduce the size of confidential transactions.



c. Stealth Addresses

Stealth addresses are used with Ring CT and Bulletproofs to keep transactions anonymous and secure. Stealth addresses prevent unspent transaction outputs from being associated with specific wallet addresses. This is done by creating a one-time public key similar to one-time passwords used by hardware key fobs or software-based token authenticators.[5]

[4] Bunz, Benedikt, et al. "Bulletproofs: Short Proofs for Confidential Transactions and More." *Bulletproofs | Stanford Applied Crypto Group*, Stanford University, 2017, crypto.stanford.edu/bulletproofs/.
[5] Yu, Gary. "Blockchain Stealth Address Schemes." *Cryptology ePrint Archive*, May 2020, eprint.iacr.org/2020/548.

d. Proof-of-Stake

Rhombus utilizes a Proof-of-Stake (PoS) consensus mechanism.[6] Rhombus' group of validators are energy efficient at minting block rewards. Rhombus Proof-of-Stake (RPoS) reduces mining inefficiencies by not using Proof-of-Work (PoW). Also, Proof-of-Stake is decentralized, providing additional network security. Rhombus' PoS is resistant to 51% attacks, because a majority of the staking market capitalization would have to be acquired by a hostile attacker which is improbable. Further, RPoS incorporates randomized block and coin age selection methods to not favor only the wealthiest nodes in the network.

e. Verification

RPoS is a type of algorithm by which a cryptocurrency blockchain ecosystem aims to achieve distributed consensus. In PoS-based cryptocurrencies like Rhombus, the creator of the next block is chosen via various combinations of random selection of the amount of staked RHOM coins and age. Conversely, the algorithm of PoW based cryptocurrencies such as Bitcoin rewards participants who solve complicated but trivial cryptographic problems in order to validate transactions and create new blocks (i.e. mining).

RPoS improved upon the popular PoS3 protocol by adding several security and utility features.

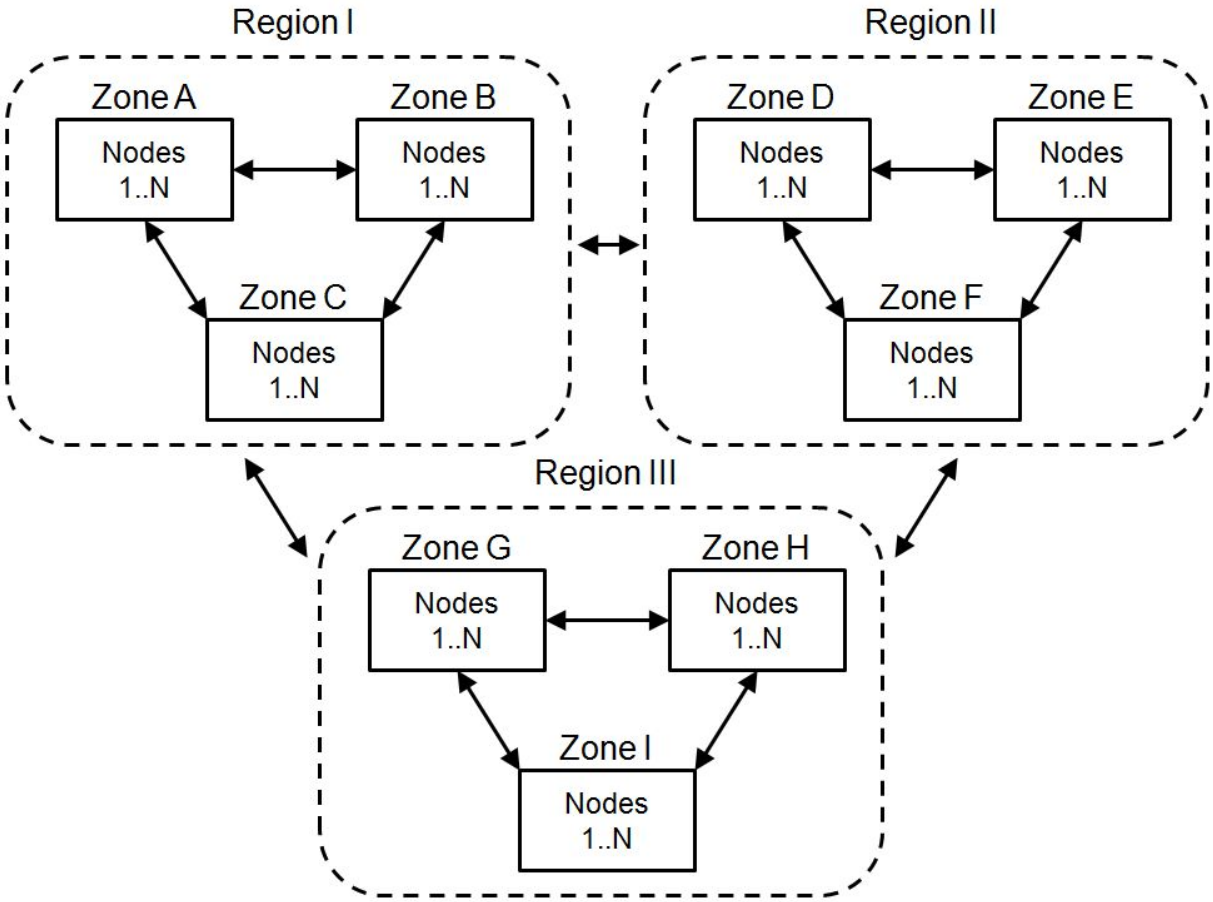
Cold Staking is a way to secure the Rhombus network while keeping your coins offline and safe by delegating your staking power to cold staking nodes which contain no coins but provide a dedicated connection to the Rhombus network. Cold staking nodes can stake for you, but they can't spend them. They only control the rewards from staking. You can stake your own funds on your own cold staking notes or use a staking pool.

5. Network

Rhombus blockchain is a lightweight distributed network built to stay agile, efficient, and fast. The Rhombus network's goal is to achieve always-on availability. Availability is normally expressed in percent terms with 9's. For example, five-nines uptime means the Rhombus blockchain nodes are fully operational 99.999% of the time. This is an average of fewer than 6 minutes of downtime per year. Rhombus' network goal is to have no blocks dropped due to network downtime.

[6] QuantumMechanic. "Proof of Stake Instead of Proof of Work." *Bitcoin Forum*, Jul. 2011, bitcointalk.org/index.php?topic=27787.0.

The Rhombus ecosystem achieves resiliency by promoting a regional configuration of geographically different and jurisdictionally different nodes such as North America, Europe, and Asia.



6. Disk Space

"It's fine to assume infinite disk space in the lab, but not in production."

Blind and anonymous transactions that use Ring CT require more disk space than public ones. By having a 2.5 minute target block time, Rhombus addresses the problems of blockchain bloat by having less blocks with fewer of them empty along with less orphan blocks and less frequent chain-reorganization.

7. Incentive

"Like candy, incentives promote honest behavior."

A constant and perpetual inflation rate of approximately 0.5% annually ensures continued participation by community members to secure the network by keeping their nodes online. This staking rewards one community member per block with 25 RHOM, which is like receiving a dividend payment on stocks. Also, incentives such as notoriety in the community or increasing coin values encourage community members to be honest/good samaritans.

8. Decentralization

"The only free lunch in blockchain technology is decentralization."

Rhombus will distribute RHOM via an airdrop to Bitcoin (Symbol: BTC) holders at a given snapshot. A snapshot is a record of the state of a blockchain at a single point in time. Rhombus will use a snapshot to record who on the Bitcoin blockchain is eligible to participate in the Rhombus airdrop. This will increase the decentralization of the Rhombus ecosystem by increasing the pool of potential stakers. Stakers do not have to acquire any specialized or expensive computing resources or mining equipment before setting up a node to begin to stake. Further, by airdropping RHOM to BTC holders, Rhombus will be bringing Ring CT and Bulletproof innovations and technology to BTC holders.

To further decentralize RHOM, an ICO will be held. Investing in cryptocurrencies is speculative and risky. Do your own research and due diligence.

9. Conclusion

"All cryptocurrency users can have 3 lives: anonymous, blind, and public."

Rhombus has proposed a decentralized and privacy-focused, untraceable, Proof-of-Stake cryptocurrency that can be sent without going through financial institutions. Rhombus builds upon the codebase of Bitcoin Core. Rhombus uses Ring CT and Bulletproofs innovations and technology to keep transactions anonymous and secure. This additional privacy provided by Rhombus allows cryptocurrency users to negotiate with other cryptocurrency users without disclosing information about their bargaining position. Rhombus technology introduces innovations in Ring CT, Bulletproofs, stealth addresses, Proof-of-Stake, and verification to provide state-of-the-art privacy for cryptocurrency users. Rhombus blockchain is a lightweight distributed network built to stay agile, efficient, and fast. The Rhombus Network's goal is to achieve always-on availability. Blind and anonymous transactions that use Ring CT require more disk space than public ones. By having a 2.5 minute block time, Rhombus addresses the problems of blockchain bloat by having less blocks with fewer of them empty. A constant and

perpetual inflation rate of approximately 0.5% annually ensures continued participation by community members to secure the network by keeping their nodes online. By airdropping RHOM to BTC holders, Rhombus will provide decentralization.