WHITE PAPER

https://www.veil-project.io

Veil Project

White Paper

Version 1.00, October 2018.

Written and compiled by Strontium

Input/Support
4x13, presstab, marsmensch, random.zebra, Dango, gets

VEIL Project - est. August 27th, 2018

Website: https://www.VEIL-Project.io

GitHub: https://github.com/4x13/VEIL-PROJECT

Abstract

The intention of cryptocurrency not simply as a token, but a viable form of money, is to replace fiat currencies as a real, workable alternative means of managing one's own finances. To this end, users should reasonably expect a feasible cryptocurrency provide a degree of privacy matching or bettering that afforded them by financial institutes. VEIL Project seeks to offer the most formidable iteration of a privacy-focused cryptocurrency to date, building upon Bitcoin core codebase version 0.17.x, by integrating leading privacy mechanisms Zerocoin, RingCT, and Dandelion without sacrificing usability. Veil uses a combination of anonymous Proof of Stake and the highly ASIC resistant X16R algorithms to build, maintain, and evolve the quintessential digital currency.

TABLE OF CONTENTS

1. VEIL PROJECT

1.1 Introduction

VEIL Project is an ambitious, open-source cryptocurrency undertaking focused on providing users with the very best in privacy and anonymity. VEIL Project looks to stay at the forefront of privacy and anonymity-focused technology by constantly evolving through the efforts of its own dedicated cryptography think-tank, Veil Labs. Through implementing, improving, and inventing solutions to this end, Veil intends to pave the way towards a financial futurescape vastly unfamiliar from that of today, where users can feel secure and in control when managing their personal finances.

Veil ran no Initial coin offering, pre-mine, or other unfair advantage, and was funded as a labour of love by its founder. For more on economics see section 3.1.

VEIL Project is run and maintained by a team of experts in the blockchain field, each with considerable experience in cryptocurrency projects and other fields relevant to their duties within the Veil team.

1.2 Mission and Vision

VEIL Project's mission statement

To deliver to the world a tool by which to seize true financial freedom.

VEIL Project's vision

We envision a world in which participating in its interconnected nature does not stand as acquiescence to forfeiture of freedoms. It's our earnest desire that individuals be afforded privilege and authority over their finances and management thereof, safe from prying-eyes and sticky-fingers.

2. TECHNOLOGY

2.1 Veil coin specs

Consensus mechanism	Hybrid PoW-PoS consensus initially, becoming PoS only.
PoW-PoS hybrid phase period	December 8th onward (at least one year)*
PoS phase period	TBA (commences at the conclusion of the hybrid phase)
Block size	2 MB until commencement of elastic blocks some time after launch.
Block time	60 Seconds (difficulty readjusting every block)
Wallet backup	BIP-0039/BIP-0044 deterministic seed
PoW consensus algorithm	X16R
PoS stake eligibility	Minimum Input Age: 60 blocks Reward Maturity Confirms: 101 confirms Wallet Status: Requires wallet to be kept running & online.
Max coin supply	300,000,000.
Coin emission rate	*See section 3 for in-depth details.*
Coin supply control	Coin emission tapers down over time until reaching hard cap.
Exchanges and services flag	Disabled Zerocoin automint, staking, and other non-essential features. Disabled by default.
Transaction send eligibility	RingCT Minimum Confirm: 6, Zerocoin Minimum Confirm: 20
Privacy technology	Custom Zerocoin protocol based on libZerocoin. Custom RingCT protocol derived from Particl's implementation.
Key features	Custom accumulator check-pointing system
Accumulator modulus	RSA-2048
Zerocoin denominations	10, 100, 1000, 10,000.
Default ring size	11
Mint time	~ 0.5 seconds
Spend time	~ 2.5 seconds
Maximum single spend limit	20 Zerocoin denominations
Maximum single mint denomination count limit	199
Fees (mint)	Variable by data size
Minimum Zerocoin mint confirmations to spend	6 confirmations
Maturity requirement before Zerocoin Veil can be spent	1 new identical denomination mint added to accumulator.

*This phase will not be extended if development of an ASIC takes place by this point.

2.2 Privacy mechanisms

Veil features what we strongly believe to be the most advanced privacy of any cryptocurrency on the market. This is achieved through a combination of vetted, tested, and trusted privacy mechanisms ensuring user privacy and anonymity are protected in their use of the Veil network.

In using a cryptocurrency, there exist several points of vulnerability for the user

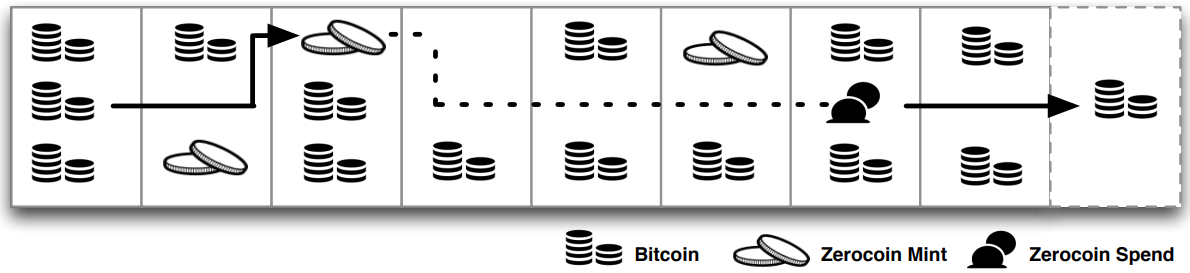
[1] tying the user's **real-world identity to the blockchain**, eg. IP-address to blockchain activity
[2] tying the user's **blockchain identity to their transactions**, eg. wallet address to blockchain activity
[3] tying the user's **blockchain identity to their finances**, eg. wallet addresses to total held funds

Veil employs measures to combat each of these, and being based on Bitcoin, features and maintains Bitcoin Improvement Proposals (BIPs), many of which are towards these goals. This section covers the three main technological measures Veil has in place beyond those of Bitcoin to protect the user from falling victim to these vulnerabilities.

2.2 i Zerocoin

The primary privacy protocol of the Veil currency is the highly vetted Zerocoin, a cryptographic anonymisation protocol developed at Johns Hopkins University Department of Computer Science, Baltimore.

Zerocoin provides anonymity on transactions through a protocol-level coin mixing service utilising zero-knowledge proofs. Use of a zero-knowledge proof ensures no direct flow of critical information between the sender and receiver when performing a transaction, instead relying on the protocol to handle the funds through Zerocoins held by accumulators. Zerocoins from the accumulators are used as a balance from which to pay out the receiver. Funds are burnt and replaced on a mint and spend, so the receiver's obtained funds carry no data pertinent to their origin. The only tie to the funds users have is the zero-knowledge proof, which being untraceable protects the anonymity of the parties involved.



A graphic from the Zerocoin technical paper demonstrating the mint and spend of a Zerocoin. See original paper in link at end of this section for more details.

Zerocoin will have been implemented by release, with MultiSig Zerocoin staking to be added in the months following release.

Minting fees vary with data size. In this way, it's cheaper for the user to rely on automint to manage mints than to mint a large batch.

Technical paper: **Zerocoin: Anonymous Distributed E-Cash from Bitcoin**
Authors: Ian Miers, Christina Garman, Matthew Green, Aviel D. Rubin
Link: http://zerocoin.org/media/pdf/ZerocoinOakland.pdf

2.2 ii RingCT

Where Veil's main currency units are anonymised via the Zerocoin protocol at 10 Veil, the loose change–or basecoin–utilises Ring Confidential Transactions (RingCT), developed and implemented by the Monero research labs to remain obfuscated.

Veil utilises a version of RingCT derived from the Particl project's implementation, which was vetted and implemented successfully in quarter-three, 2018.

RingCT is an enhanced version of a *ring signature*. A ring signature is a means of transmitting a piece of endorsed information as a 'secret' in a random selection of disassociated outputs. The resultant ring signature contains the valid output of the signer, but it remains indistinguishable from those non-signers.

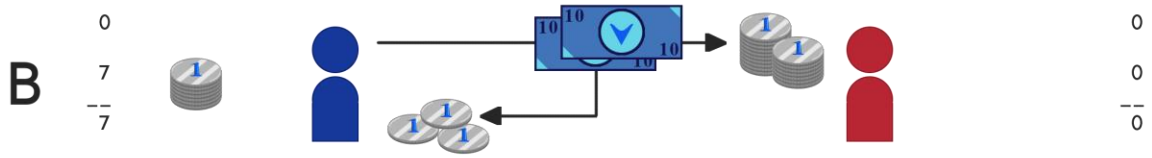
Shen Noether of Monero labs proposed a solution to the need for denominations for ring signatures in RingCT, wherein visible denominations were avoided by the masking of funds at creation. By masking the value of the funds on the blockchain, the origin of the transaction is protected, and the anonymity pool is significantly increased

RingCT will have been implemented by launch, with stealth addresses following in the months following release.

Technical paper: **Ring Confidential Transactions**
Author: Shen Noether
Link: https://eprint.iacr.org/2015/1098.pdf
building on
Technical paper: **How to Leak a Secret**
Authors: Ronald L. Rivest, Adi Shamir, and Yael Tauman
Link: https://people.csail.mit.edu/rivest/pubs/RST01.pdf

2.2 iii Explaining Zerocoin and RingCT in VEIL Project

A: Red requests 17 Veil from Blue. Blue currently holds 2x10 Veil Zerocoin denominations ('bank-notes'), and 7 Veil in RingCT ('change') for a total of 27 Veil.



B: Blue sends 20 Veil as 2x10 Zerocoin denominations to Red. As Red only requested 17, Blue gets back 3 Veil as RingCT in change.

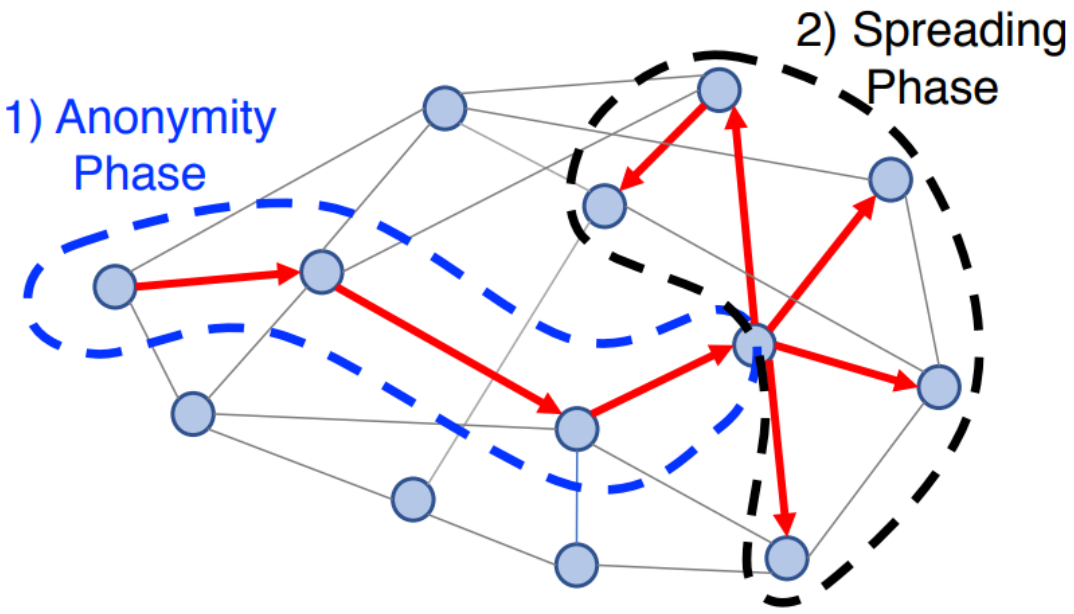
C: As received Veil arrives as change, Blue now has 10 Veil in change. Red now has the 17 requested Veil, which arrived as change also.

D: Blue had sufficient change so minted a 10 Veil Zerocoin denomination. Red also had sufficient change to mint a 10 Veil Zerocoin denomination. However, Red also has 7 Veil remaining as RingCT. Red will need to obtain a further 3 Veil before being able to mint another Zerocoin denomination.

Notes This example uses whole numbers and neglects to include minting fees for the sake of simplicity. Remember, only Veil Zerocoin can stake.

2.2 iv Dandelion

Dandelion is a protocol available at Veil's launch that masks the origin IP-address of a transaction transmitted on the network. It does this by sufficiently complicating the transaction's pathing to make tracing it back to a point of origin unfeasible. It goes about this through two main stages; those being the *anonymity*, or commonly 'stem' phase, and the *spreading*, or commonly 'fluff' phase.



A graphic from the Dandelion technical paper demonstrating the two phases of the protocol. The Dandelion technical paper can be found in the link at the end of this section.

In the anonymity 'stem' phase, a transaction is sent from the origin to a new node in the network with a randomly-varied short time delay having a 50/50 chance to relay the transmission or begin dispersal. The spreading 'fluff' phase, is when the transaction is disseminated across the network to be validated.

Technical paper: **Dandelion: Redesigning the Bitcoin Network for Anonymity**
Authors: Shaileshh Bojja Venkatakrishnan, Giulia Fanti, Pramod Viswanath
Link: https://arxiv.org/pdf/1701.04439.pdf

2.3 X16R Proof-of-Work

Veil chose the X16R Proof-of-Work consensus algorithm for the ease with which anyone can mine with it. X16R is predominantly a CPU-reliant mining algorithm, and at the time of selection was highly underutilised by cryptocurrency projects. At the time of writing, there currently exists no ASIC miner for X16R, making it amongst the fairer mining algorithms available.

It's important to Veil that the PoW phase lasts only so long as it remains reasonably fair for the vast majority of users. For this reason, after the initial year-long hybrid consensus period, a reassessment on the viability of the dual-consensus phase will take place. Should the assessment find X16R remains reasonably fair, the phase will be extended by a period determined by circumstances at the time of assessment. If this is found to no longer be the case, however, the dual-consensus phase will conclude, and Veil will rely solely on its PoS mechanism.

Current projections suggest mining with X16R will be more lucrative than relying on Proof-of-Stake during the hybrid phase; this is intentional to promote a wider spread of coins during the distribution phase.

Block rewards will lower annually beyond launch, with the first year–in which PoW is guaranteed to be operative–rewarding 50 Veil to miners.

Mining via X16R will take place outside of the Veil wallet. Instructions on setting up to mine via X16R can be found at https://www.VEIL-Project.io where details on official mining pools can also be found.

Technical paper: **X16R ASIC Resistant by Design**
Authors: Tron Black, Joel Weight
Link: https://ravencoin.org/wp-content/uploads/2018/03/X16R-Whitepaper.pdf

3. ECONOMICS

3.1 Veil coin emission projection

The following table demonstrates Veil's projected coin emission over time, breaking down the block reward to represent funds to founder, lab (see 4,4), budget, and the mining reward.

Year	Block Reward	Founder	Lab	Budget	PoW/PoS	Drop	Coin Supply
1	100	10	10	30	50		52,290,000
2	80	8	8	24	40	20%	94,338,000
3	60	6	6	18	30	25%	125,874,000
4	40	4	4	12	20	33%	146,898,000
5	20	2	2	6	10	50%	157,410,000
6+	20	0	2	8	10		"+10,512,000/year"

Emission will continue at 20% of the initial year's values from year 6 onwards towards the coin supply cap of 300,000,000 Veil.

Only the first year is guaranteed to utilise both Proof-of-Work and Proof-of-Stake consensus algorithms, so data for year 2 onwards applies primarily to PoS, but may include PoW also. For more details see section 2.3.

4. ROADMAP ITEMS

The following items are technology implementations to be added to Veil in the months following initial release.

4.1 Bulletproofs

Bulletproofs are a cryptographical means of reducing the size of a spend. They will be applied to both the Zerocoin and RingCT protected Veil, though each implementation is not identical, and custom-created to suit each protocol.

Technical paper: **Bulletproofs: Short Proofs for Confidential Transactions and More**
Authors: Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, Greg Maxwell
Link: https://eprint.iacr.org/2017/1066.pdf

4.2 Blockchain pruning

Pruning involves the user's machine only retaining the last 550 blocks on the blockchain, as well as older blocks with data pertinent to their own holdings. Doing so greatly reduces the amount of space on the system's storage the Veil blockchain takes up.

Technical paper: **Bitcoin Ongoing Pruning**
Author: Peter Gregory Jr.
Link: https://www.scribd.com/document/317130737/Bitcoin-On-Chain-Pruning

4.3 Elastic block sizes

Elastic blocks will dynamically change block sizes in response to blockchain activity. The intention of this mechanism is to allow the blockchain to deterministically adjust to the variances in pressure on the network, responding with varied block sizes to best accommodate the variances in volume periodically.

Technical paper: **BIP10X-Hybrid-Bitcoin-Block-Size-Limit-Adjustment**
Author: 1MichaS1
Link: https://github.com/1MichaS1/BIP10X-Hybrid-Bitcoin-Block-Size-Limit-Adjustment/blob/master/BIP-AdaptBlockSizeLimit.mediawiki

4.4 Veil labs

Veil labs is VEIL Project's research and development department. Much like a think-tank, Veil labs is purposed to research, theorise, vet, and prototype new cryptographical technology for the purpose of improving Veil. These improvements may be angled at increasing privacy, making Veil further resistant to future quantum attacks, increasing spend efficiency, lowering resource requirement, and other such tasks.

5. REFERENCES

Zerocoin: Anonymous Distributed E-Cash from Bitcoin

Authors: Ian Miers, Christina Garman, Matthew Green, Aviel D. Rubin

Link: http://zerocoin.org/media/pdf/ZerocoinOakland.pdf

Ring Confidential Transactions

Author: Shen Noether

Link: https://eprint.iacr.org/2015/1098.pdf

building on

How to Leak a Secret

Authors: Ronald L. Rivest, Adi Shamir, and Yael Tauman

Link: https://people.csail.mit.edu/rivest/pubs/RST01.pdf

Dandelion: Redesigning the Bitcoin Network for Anonymity

Authors: Shaileshh Bojja Venkatakrishnan, Giulia Fanti, Pramod Viswanath

Link: https://arxiv.org/pdf/1701.04439.pdf

X16R ASIC Resistant by Design

Authors: Tron Black, Joel Weight

Link: https://ravencoin.org/wp-content/uploads/2018/03/X16R-Whitepaper.pdf

Bulletproofs: Short Proofs for Confidential Transactions and More

Authors: Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, Greg Maxwell

Link: https://eprint.iacr.org/2017/1066.pdf

Bitcoin Ongoing Pruning

Author: Peter Gregory Jr.

Link: https://www.scribd.com/document/317130737/Bitcoin-On-Chain-Pruning

BIP10X-Hybrid-Bitcoin-Block-Size-Limit-Adjustment

Author: 1MichaS1

Link: https://github.com/1MichaS1/BIP10X-Hybrid-Bitcoin-Block-Size-Limit-Adjustment/blob/master/BIP-AdaptBlockSizeLimit.mediawiki