Haven Protocol

Private Decentralised Finance

1. Introduction

Bitcoin paved the way for electronic peer-to-peer currency. It was the first digital currency to successfully implement a distributed ledger of transactions based on cryptographic proof over trust. More recently, with the realisation that all wallets and transactions in Bitcoin and many other cryptocurrencies are visible to all who care to look, the demand for private transactions and privacy coins has grown.

Haven is built on top of Monero, which is widely considered to be the leader in privacy technology. Haven therefore inherits all of Monero's privacy features, including ring signatures and Bulletproofs. It extends that functionality by providing private, anonymous, synthetic currencies and commodities (xAssets) which can only exist through the "burning" of the Haven base currency - $XHV.

Welcome to Haven - Private Decentralised Finance.

i. Project History

The concept of Haven was started by two developers in early 2018. This first attempt reached the stage of a public testnet before weaknesses in the solution, a hiatus in development, and a subsequent lack of progress from the original developers put the project's future in doubt.

In late January 2019, a collection of original Haven community members took the project over with a view to completing the project, delivering the offshore storage mechanism, and building out the supporting infrastructure to gain mass adoption of a much needed utility in the rapidly growing cryptocurrency market.

2. The Haven Protocol

Our promise: 1 xUSD will always be redeemable for $1 worth of XHV.

In contrast to other Proof-of-Work (POW) attempts at algorithmic stable “mint and burn” protocols, Haven has always been focused on ensuring that conversions between our stable and volatile coins maintain their peg and therefore their value. We explain the mechanisms and rules that make this achievable later in this paper.

i. Concept

Haven is an untraceable cryptocurrency with a mix of standard market pricing and real world asset-pegged value storage. It achieves this via a “mint and burn” process within a single blockchain.

In the simplest case, users can burn Haven (XHV) for the equivalent USD value worth of Haven Dollars (xUSD). Or, to restore to a volatile state, the user can equally burn xUSD for $1 USD worth of XHV.

Other major fiat currencies including CAD, GBP, EUR and CNY, as well as BTC and other high profile commodities such as xAU (Gold) are intended to be added to the Haven ecosystem over time to allow users to choose a suitable pegging mechanism for their needs.

ii. The Offshore Process – “Mint and Burn”

Haven uses a system called “mint and burn” to maintain its value relationship against its asset pegs. In practice, using the synthetic U.S. Dollar (xUSD) as an example, this works as follows: Bob decides he wants to put 200 of his Haven (XHV) into Offshore Storage. When users put XHV into Offshore Storage, they are *burning* XHV coins and *minting* the current value of those XHV as new xUSD. Offshore Storage determines the current market value of that Haven (in xUSD) based on a weighted average of volume across supported exchanges. This is done using a pricing oracle – a mechanism to discover real world data and make this data available to a blockchain – to retrieve pricing data for the full Haven ecosystem and create pricing records.

If the current value of Haven is $1 USD, Offshore Storage will burn Bob’s 200 XHV by constructing a special transaction where the 200 XHV that was sent is then burned into xUSD and the total supply of XHV decreases. If the price of Haven then moves to $2 USD and Bob decides to access his Offshore Storage, he will be returned 100 XHV (100 * $2 = $200 USD as per original value). If the opposite

occurs and the price of Haven halves to $0.50, then 400 XHV will be minted and sent to Bob (400 * $0.50 = $200 USD as per original value).

Clearly, the use of mint and burn therefore alters circulating supply of the underlying assets in a dynamic manner. This creates intriguing supply scenarios – very different from other cryptocurrencies – which need to be reviewed in order to fully understand the Haven Protocol concept.

iii. How Does Offshoring Actually Work?

The Haven Protocol enables offshore transactions within the Haven Wallet using a flag within the transaction to indicate which asset type each transaction originates as, and ends up as. Pricing details are obtained from a real-world pricing provider (i.e. a pricing oracle) and a pricing record is created. Pricing records contain the exchange rates (against XHV) for each of the xAsset pegs at the time of the block being mined. The pricing information is updated at 30 second intervals, and presented to the Haven daemon upon request.

Pricing records are embedded into the blockchain in every block header. By including this information in every block, the protocol guarantees that the transaction value cannot be tampered with or altered in any way – the blockchain guarantees that the pricing information is immutable. If multiple blocks are successfully mined within the lifetime of the current pricing record, the same record will get included in multiple blocks.

A pricing record contains the following conversion rates (all against XHV), as well as some reserved space for future additions and the signature of the oracle providing the data:

xAG (Silver), xAU (Gold), xAUD (Australian Dollar), xBTC (bitcoin), xCAN (Canadian Dollar), xCHF (Swiss Franc), xCNY (Chinese Yuan), xEUR (Euro), xGBP (Pound Sterling), xNOK (Norwegian Krone), xNZD (New Zealand Dollar), xUSD (US Dollar)

iv. Pricing Oracles

In order to retrieve data from the real world, blockchains use a construct called an “oracle.”

“A blockchain oracle is a third-party information source that has the sole function of supplying data to blockchains”
Source: https://www.mycryptopedia.com/blockchain-oracles-explained/

In the first iteration of Haven and several subsequent designs since that time, the creation of a secure, accurate and high-performing oracle was considered key to the success of the protocol. However, since the creation and success of services such as Chainlink and Zen Protocol, which are designed purely to provide oracle functions as an independent data source, it is now clear that not only is a separate oracle not required to be built into the Haven system, but it is not desirable to do so. Doing so would increase centralisation of the most important part of the conversion equation – pricing.

With this in mind, Haven Protocol have partnered with Zel (https://zel.network/) in order to utilise their Zelnodes for processing the pricing data. Haven will work in partnership with the Zel team to create a Zel-powered oracle system using Haven's needs as the first reference use case. It should be noted that whilst Haven will assist with the design, specification and delivery of the oracle system, Haven asset holders will not have any governance or reward relationship with it.

Haven also believe that it is vital to build in flexibility in pricing discovery from the start, and as such will never rely solely on one oracle system, but will be able to add, swap and remove oracles over time to ensure Haven uses best-in-class data now, and into the future.

Delivery of the full oracle system is planned to coincide with full release of Haven's offshore mainnet in late 2019.

v. Supply Scenarios

XHV is a pure Proof-of-Work (PoW) coin with the same emission curve as Monero, with an initial minable supply of 18.4 million and a small tail emission once those 18.4 million coins have been mined. This is a very normal, well understood supply scenario in the cryptocurrency market. Once Haven's offshore storage feature is released, the above figures continue to apply to mining rewards, but no longer define the actual circulating supply of XHV since mint and burn will alter this dynamically as previously discussed.

In addition, after offshore release, the circulating supply of XHV will no longer define the total capitalisation of the Haven ecosystem. For this, it is necessary to consider the cumulative value of xAssets held as well as XHV itself.

To understand the potential future supply of XHV and the effect of that supply on the Haven ecosystem, the following high-level macro scenarios are presented. Variables considered in these scenarios include:

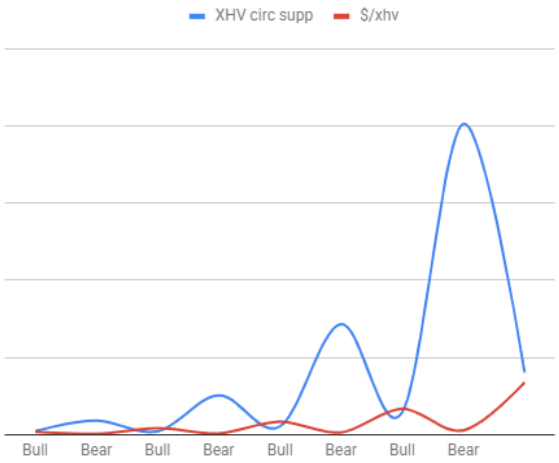
1. The increase in total market capitalisation in a market bull cycle (inc_Bull)

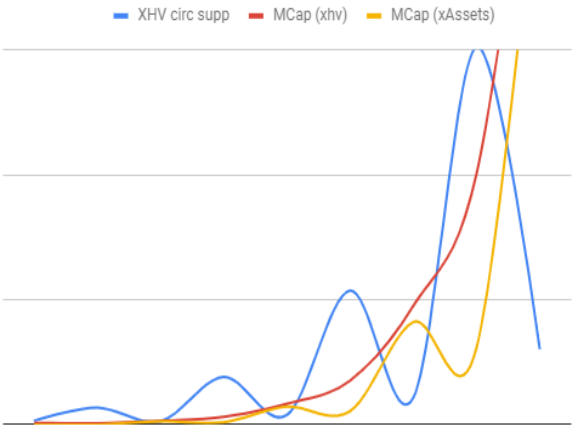
2. The decrease in total market capitalisation in a market bear cycle (dec_Bear)
3. The % of XHV coins sent to and stored in offshore at the end of a bull market cycle (perc_offBull)
4. The % of xAsset (using xUSD as an example) coins onshored back to XHV at the end of a bear market cycle (perc_onBear)
5. The % of the local ATH value of XHV within a bull cycle that is the average of all offshore transaction values (Eg. if the local ATH for XHV is $2.00 then 80% of that ATH is $1.60 and this would be the value used in these scenarios for offshoring if 80% is used for this variable) (perc_LATH)
6. The % of the local ATL value of XHV within a bear cycle that is the average of all onshore transaction values. (perc_LATL)
    - **Note: These values for 5 & 6 can be viewed as how accurate traders are when predicting tops and bottoms of markets.*
7. XHV volatility index - this value is used to simulate how correlated the volatility of XHV might be in comparison to bitcoins volatility. A value of 1 being equal to BTC volatility, 0.5 being 'half as volatile', 2 being twice as volatile etc. (iVol)

Scenario 1 - Expansion in XHV Supply

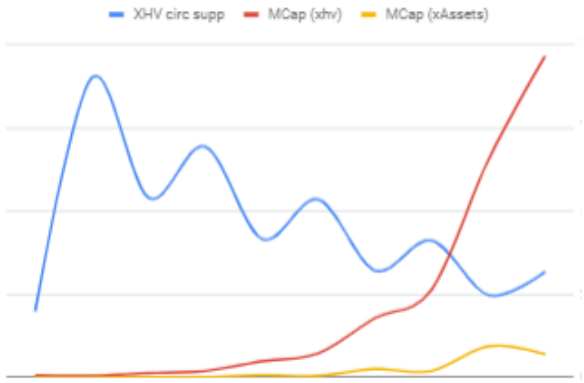
In this scenario we use values that will increase the supply of XHV in the market over time.

inc_Bull	= 2500%
dec_Bear	= 85%
perc_offBull	= 80%
perc_onBear	= 75%
perc_LATH	= 90%
perc_LATL	= 10%
iVol	= 1.0





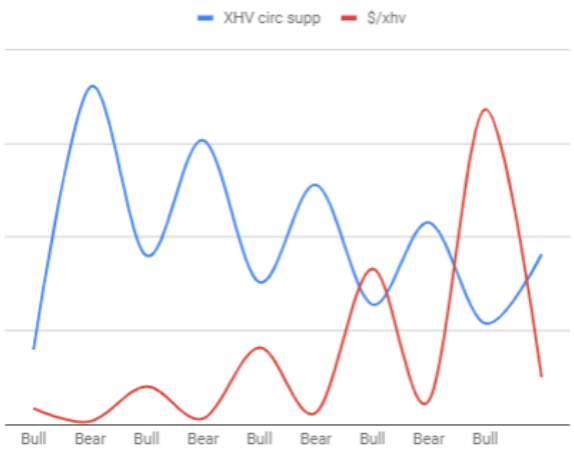
As can be seen in this model of extremely heavy offshore use and high trading accuracy, the use of offshore functionality in an expansion scenario keeps the price of XHV subdued, but over time increases market capitalisation of both XHV and the Haven ecosystem as a whole. This scenario is acceptable to the ecosystem since it lowers volatility of XHV price, which in turn alters the patterns shown and moves the scenario out of expansion, and into equilibrium (or even contraction) as can be seen in the charts below where the only change to the values used above is to iVol (0.5).

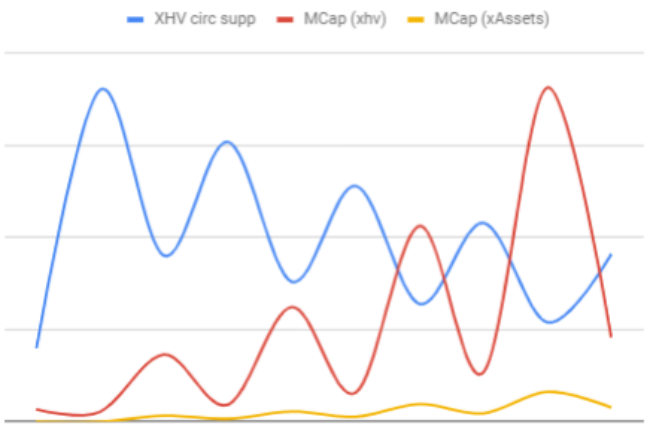


Scenario 2 - Contraction in XHV Supply

In this scenario, values are used which deliberately create deflation in the circulating supply of XHV.

inc_Bull	= 2500%
dec_Bear	= 85%
perc_offBull	= 50%
perc_onBear	= 48%
perc_LATH	= 60%
perc_LATL	= 40%
iVol	= 1.0



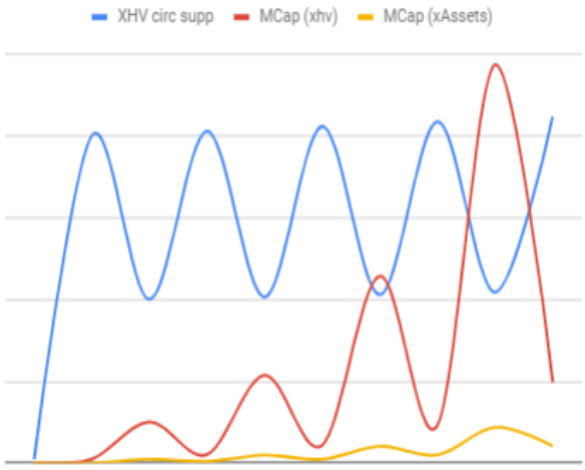


As can be seen in a contraction scenario, the price of XHV increases in volatility, creating the opposite effect from the expansion scenario over time and will move the pattern from contraction towards equilibrium or expansion.

Scenario 3 - Equilibrium in XHV Supply

In this scenario the prediction variables are set with medium use of offshore, and medium trading accuracy. As the central point between the two other scenarios, one can expect this scenario to play out repeatedly over time, with expansion and contraction scenarios both tending towards equilibrium.

inc_Bull	= 2500%
dec_Bear	= 85%
perc_offBull	= 70%
perc_onBear	= 50%
perc_LATH	= 60%
perc_LATL	= 40%
iVol	= 1



In conclusion, while one cannot predict which scenario will play out at any given time, the protocol is designed to adapt to changing usage levels by expanding and contracting supply of XHV directly through user actions, creating a new and unique supply curve purely from natural and organic use.

3. Stability and Economics

Mint and burn requires little in order to implement in a basic form; just a known price at which to perform the conversion, and the ability to convert one type of asset to another on the same chain at that conversion rate. To state the obvious, it is a very simple concept. That being said, the simplest of concepts are sometimes the hardest to fully understand, and to ensure that the Haven ecosystem uses a robust economic model, certain challenges must be addressed.

1. *Supply transparency*

2. *Exchange based price manipulation*

3. *The potential for a 'run on the bank' during BTC price volatility as users exit xUSD to XHV and then to BTC.*

4. *Proving and maintaining the value of synthetic assets in a PoW algorithmic ecosystem.*

These challenges will be addressed one at a time:

1. *Supply Transparency*

The original concept for Haven was based on having an unknown circulating supply of XHV and xAssets. The reasoning for this was to prevent manipulation of the network by large holders of XHV or xAssets. After a great deal of consideration, community discussion, and consultation with expert advisors, it was decided that having a transparent circulating supply would actually be beneficial to the network in the following ways:

- It allows more efficient monitoring of the Haven network, which means attempted attacks and large scale manipulation can be detected and mitigated much faster.
- It gives users greater confidence to enter the Haven network with the ability to view the number of XHV and xAssets in circulation at any given moment.
- It allows for greater visibility and therefore greater analysis on coin metrics websites.

As a result, to ensure accuracy and visibility, each mint and burn transaction will be created in such a way that amounts will be discoverable through analysis of the blockchain, and displayed in the Haven block explorers. This will allow users to maintain standard Monero levels of anonymity and wallet address privacy while allowing a clear view of circulating supply.

2. *Exchange Based Price Manipulation*

Due to the nature of mint and burn, Haven's long standing promise that "1 xUSD will always be redeemable for $1 worth of XHV," and the price-smoothing action of moving averages within Haven's pricing system, certain measures are required to ensure that discrepancies between exchange prices and off/onshore conversions are minimised.

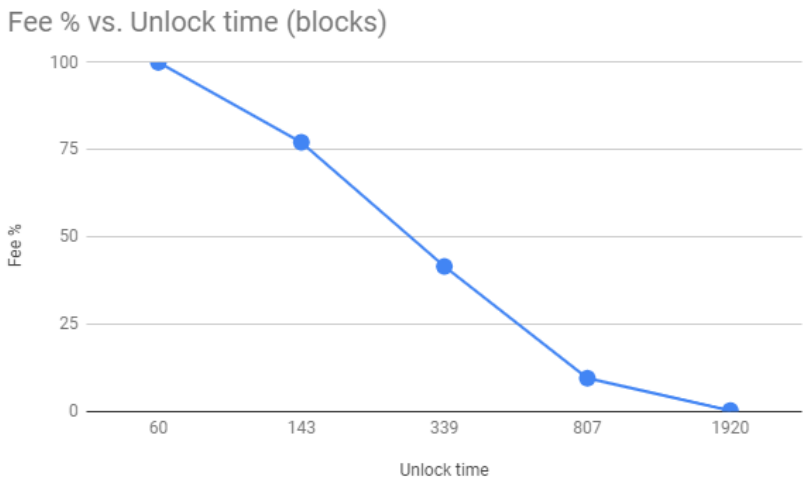
This minimisation is performed by allowing a choice of transaction priority by the user. High priority transactions, with minimal unlock times, will be charged higher fees than low priority transactions with longer unlock times (where the fee will tend to near zero). The fee charged is calculated based on the number of blocks before unlocking using an exponential decay function:

$$N_t = N_0 * e^{-rt}$$

where:
N_t: The amount at time t
N_0: The amount at time 0
r: Decay rate
t: Time passed

Users will be able to choose the unlock time they prefer for each transaction, and will be charged fees based on the above decay formula. This mechanism ensures that users are both able to perform fast conversions when required, as well as have the option to take a longer unlock time and therefore retain their full USD value as per the Haven Protocol promise (subject to a minimum on/offshoring fee of less than 0.3%).

Fees for the use of offshore storage can therefore be represented as shown in the following chart and accompanying table, where the 'Fee %' is the % of the delta between the exchange spot price and the MA smoothed pricing used within the offshoring system.



Fee structure / unlock times for offshore

Hours	Unlock time (blocks)	Fee % of delta
2:00:00	60	100
4:45:25	143	77.11799083
11:18:51	339	41.56808978
26:54:37	807	9.558544718
64:00:18	1920	0.2897732758

By implementing this model of varying fees based on priority of unlock, the networks increases the cost of any exchange based manipulation effort to such an extent that it no longer makes financial sense for a bad actor, while still ensuring that users operating as good actors in the system can still retain their desired full value from offshore functions by opting for longer unlock times.

3. *The Potential for a 'Run on the Bank' During Bitcoin Volatility*

During rising market cycles ('Bull markets'), Bitcoin generally leads the way, and 'altcoins' often suffer drops in value when priced in Bitcoin, this could potentially lead to a scenario where users try to exit xUSD into XHV and subsequently sell for BTC.

During the offshore testnet period for xUSD, Haven will add xBTC (synthetic bitcoin) to the offshore area of the wallet. xBTC will be available as a swap within the offshore system, allowing users to simply swap xUSD for xBTC (or in the future xAU/GOLD, xCNY, xEUR) with no need to exit the ecosystem. Not only will this allow for extremely high liquidity within the wallet (no 'taker' is required to complete the exchange), but it also removes the need for users to convert back to XHV when they desire exposure to market forces.

It is as yet undecided if xBTC will progress through testing and into mainnet, and substantial testing will be performed to allow understanding of the effects of xBTC on the ecosystem. Assuming xBTC does progress, then in wallet exchange of all xAsset types will then be planned for future releases.

4. *Proving and Maintaining the Value of Synthetic Assets in a PoW Algorithmic Ecosystem*

One of the biggest challenges of algorithmic synthetic assets, as well as one of the most frequently asked questions, is centered around the concept of "true

value" or "source of value." Questions like "how can you claim xUSD is worth $1 when it has no collateral backing?" are asked often by users. Once that question has been answered and understood (xUSD is "backed" by a varying and appropriate amount of XHV), users then focus on questions around the supply of, and liquidity of, XHV itself.

Since XHV supply will fluctuate due to offshore transactions as described above, both the supply expansion and contraction cases potentially change the dynamics of the entire ecosystem. In all likelihood, taking into account the cyclic nature of cryptocurrency markets, the potential for both cases to arise is high. This is both expected and desirable. Fluctuations in circulating supply are absolutely required to allow for expansion and contraction in xUSD supply without creating ever larger volatility in the price of XHV.

None of this however answers the question about "source of value." Traditional monetary systems intuitively define their source of value, either in use case or in commodity value, and sometimes both. Typical examples of use case for fiat currencies are of course simple purchasing power and payment of living costs and taxes. While commodity values in fiat currencies are nowadays rare, commodities such as gold or silver provide a clear store of value rather than a spending use case.

While the original concept of Haven Protocol was offshore storage, and this remains the cornerstone of the project, time and consideration has allowed for an extension of this concept so that after the launch of Haven's offshore solution, there is a known and well thought out future roadmap. Haven has for some time been using "offshore banking in your pocket" as a slogan. There is more to this phrase than just brand positioning – this is Haven's use-case and the first additional source of value.

Introducing Haven Loans.

Haven Loans is the first of Haven's decentralised finance functions. Extending the use case for Haven above and beyond offshore storage. It is expected to be in testing in early 2020 and completed mid 2020. Haven Loans is a crypto loan system built on smart contracts which allows Haven holders to earn interest on their offshored assets, and loan takers to leverage their crypto holdings without the need to sell.

Haven Loans does two things:

- It allows users to increase the value of their offshore assets by loaning them out and earning interest.

- It allows users to increase the amount of crypto assets they have by borrowing against their existing assets and paying interest to do this.

Haven holders will be able to assign their xAssets to a secure liquidity pool for given periods of time. During that time, the liquidity pool will make those xAssets available for use by the Loans system offering loans to users and charging interest on these loans. Proceeds of the Loans system will be distributed back to the original holders, creating an interest bearing “savings account” for Haven holders.

We believe this will be the first truly private, decentralised, Proof-of-Work powered Decentralised Finance (“DeFi”) product, with several interest bearing stable coins at its core. This begins the journey to Haven’s full vision to be a decentralised offshore bank in your pocket.

Haven Loans will allow any BTC holder to deposit BTC into the Haven Loans smart contract and draw xUSD from the liquidity pool against that contract at an over collateralised rate (a borrower must always have more collateral than the amount of xUSD they borrow). This in effect creates a simple secured loan using BTC as security. Haven Loans contracts will hence always be over collateralised, ensuring that the Haven Loan system is always in a net positive state.

In the case that the value of collateral drops below a certain threshold, an automated liquidation process will occur, with a liquidation fee being charged against the collateral, the original loan (with accrued interest) repaid to the liquidity pool, and any remainder being returned to the user.

Further details of rates, governance models, rights for XHV holders, risk management, and mitigations will be given in a separate paper focusing purely on the Loans product. The Loans paper is due to be completed in Q4 2019, with delivery of the platform in 2020.

4. Who are Haven?

The Haven team is a community collective of developers and contributors and as such welcomes all input and contributions from any party. The core development team is listed below.

Since taking over the management and development of the coin from the original developers, the community has benefitted from the continued support and guidance of several advisors, consultants and technology industry professionals who have made it their mission to fulfil the promise of Haven, and drive adoption

of this vital part of the cryptocurrency landscape. The continued support and input from these individuals is greatly appreciated.

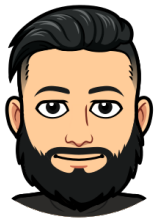
Core development team:

David Bandtock
(@dweab) https://www.linkedin.com/in/david-bandtock-9647101/

A career technologist with a focus on product delivery and strategy, David has held senior positions in major UK Corporations and multiple technology startups over the past 20 years. With a background in Mathematics, encryption technology and Software development, David brings considerable experience both in technical delivery and large scale governance to Haven.

Neil Coggins
(@neac) https://www.linkedin.com/in/neil-coggins-7972352/

Neil is a dedicated full stack software architect and developer. With over 20 years development experience in X86 Assembler, C++, Java, PHP and Javascript, Neil has spent the last 17 years designing and building cryptographic software.



@Marty (anonymous)

Marty is a front end developer with experience in a multitude of frameworks, and brings this to the fore with his work on the Haven wallets and websites.

@Pierre Lafitte (anonymous)

Pierre is a product design specialist, and creates all the user journeys and UI’s in the Haven product portfolio. Pierre is an experienced Front End crypto developer, is a long time contributor to Haven and will be leading the UX/UI side of development and bringing the UX visions of the team to reality.