



Money, on Your Terms

White Paper v.2.0

January 15th, 2018

Note: Phore reserves the right to update this whitepaper at any time. Please visit the Phore website (<https://phore.io>) for the most up-to-date version of this whitepaper.

Table of Contents

Guiding Principles	4
Phore Vision	6
History and Accomplishments	8
KryptKoin Origin	8
Coin Swap	9
Proof of Stake	10
Masternodes	11
Zerocoin Protocol (zPHR)	13
Phore Community	16
Phore Marketplace Development	18
Masternode Governance	20
Charitable Donations	22
Current Phore Cryptocurrency Statistics	23
How is Phore Different?	24
Phore Roadmap	26
Q1 2018 Milestones	26
Blockchain Technology	26
Web Wallet and Android Wallet Release	27
Wallet and Core Upgrades	28
Masternode Setup Automation	28
Phore Budget Governance Website	28
Phore Marketplace Launch	28
Phore Developer Team Expansion	29
Continued Team Recruitment	29
Q2 2018 Milestones	29
Segregated Witness (SegWit) Activation	29
iOS Mobile Wallet / App	30
Creation of The Phore Foundation	31
Q3 2018 Milestones	31

Smart Contracts	31
Atomic Swap Implementation	35
Decentralised Crowdfunding	36
Click and Collect Marketplace Vendor Pilot Programme. Location TBC	37
Q4 2018 Milestones	37
Smart Contract Implementation	37
Mobile App Development	37
VR/AR Marketplace Enhancement – Beta Testing	37
Click and Collect Incorporation into Marketplace	38
Phore Labs Investment	38
2019 Goals	38
Join the Phore Community	43

Guiding Principles

The technological advancements over the last century have created enormous wealth and opportunity unlike any other period in history. Humanity is currently at a watershed; a paradigm shift that will recreate how we communicate, transact, pay for goods and services, and innumerable other applications due to the adoption of blockchain technology. Although there are tremendous benefits to these new technologies, they may also come at a cost. Collection, tracking, analyzing, and utilization of personal data has become a much easier task for private and public entities alike. Corporations and governments collect our personal data for myriad reasons but the end result is the same: a loss of individual privacy.

One may think “if I have done nothing wrong, I have nothing to hide” however this sort of thinking fails to grasp the extraordinary impact our collected data can have on us. This information can be utilized for targeted advertising, censorship, boycotts, and retribution for holding views contrary to the status quo, to name a few. Indeed, we can see from recent history that:

- Social media has been utilized to demonetize content, reject advertisements, or ban users who hold contrarian views to those of the media platform
- Large crowdfunding sites have been accused of political bias, reportedly rejecting or removing fundraising campaigns when they are for causes considered unacceptable under the guise of “not meeting community standards”
- Personal information including purchasing habits are used by corporations and government for purposes ranging from advertising to censorship and boycotts, and often have been subject to massive cybersecurity breaches and theft, partially because so much personal information is in one centralized location

More conventional cryptocurrencies like Bitcoin do not offer sufficient protection of one’s identity and information as all transactions are observable and traceable

by any determined investigator. Those who value their privacy are not protected satisfactorily and are thus vulnerable to exposure. An improved privacy-oriented cryptocurrency is one solution to this problem of which Phore is a viable candidate.

Phore's usefulness as a currency is the crux of its ecosystem. Individuals are free to exchange amongst themselves, nearly instantly, with the choice of anonymous or public transactions. Furthermore, they do not risk having their coins confiscated by a legal entity. The benefit to using a means of exchange outside of fiat currencies like the United States Federal Reserve Note (U.S. dollar) or the British Pound is that individuals are not subject to arbitrary and often adverse effects of monetary policy. Phore has an established and immutable distribution of its coin. This knowledge allows individuals to make future decisions with confidence in the security of this system. Arbitrary expansion and contraction of the supply of Phore cannot occur. This will result in a predictable and stable medium of exchange. One does not need to look further than the recent monetary history of the United States or the European Union to see the devastating effects of arbitrary and capricious central bank monetary planning.

- During the Great Depression, the United States government outlawed the private possession of gold bullion and required citizens to sell their gold (apart from jewelry, collector coins, and the like) to the government - at what ended up being for less than 50% of what it was worth.
- More recently, in 2013 the Bank of Cyprus agreed to a 23 Billion Euro (\$30.5 Billion) rescue package with the IMF, an agreement that included depositors losing 47.5% of their savings exceeding 100,000 Euros (\$132,000).
- In 2014, Russia began seizing about \$8 billion per year of its citizens' private pension retirement contributions to finance government spending/debt. Poland (\$39 Billion), Hungary (\$12 Billion), Portugal (\$2.5 Billion), Bulgaria, and Argentina (\$30 Billion) made similar moves in the six years prior to that.
- By many estimates, the US dollar has lost over 90% of its purchasing power over the last 100 years¹. John Maynard Keynes attributed this

¹ "What Has Government Done to Our Money?" by Murray N. Rothbard, Ludwig von Mises Institute, Sept 20th, 2005.

largely to the current system of interventionist economic policies that have eroded the value of currencies worldwide, stating that “[by] a continuing process of inflation, governments can confiscate, secretly and unobserved, an important part of the wealth of their citizens. By this method, they not only confiscate, but they confiscate *arbitrarily*; and, while the process impoverishes many, it actually enriches some.”²

We believe in empowerment of the individual, and of communities. We believe in the right to free speech, and the freedom to conduct commerce as a core component of that right. This can take many forms, whether it is the freedom to contribute to a cause, to buy and sell products and services, to raise money through crowdfunding, or to run a business that has value to your customers.

Using blockchain and related decentralized technologies, we want Phore to help individuals and communities take back that power, and achieve their goals more efficiently and with greater independence, and without the compromises of needing to give up data and being subject to control of corporations and other centralized groups.

Phore Vision

The vision of the Phore community is to provide a private, community-based cryptocurrency and blockchain platform that forms the foundation of free and sustainable decentralized commerce. This vision includes not only the core blockchain, but many related applications and ventures constructed on top of the platform. The technology built into the Phore protocol will accord several capabilities including:

- fast, scalable, secure, and reliable transactions
- options for both private and transparent transactions
- rewards for participation in the Phore network, similar to interest payments
- decentralized marketplace

² “The Economic Consequences of the Peace” by John Maynard Keynes, Serenity Publishers, LLC (February 10, 2009)

- an advanced and flexible smart contract platform for building decentralized applications (dAPPs) that can be used in conjunction with private transactions, enabling new decentralized, privacy-enabled business models that keep you in control of your money and your personal information
- widespread accessibility and ease of use

Accessibility and ease of use are essential elements of our vision. Phore is for everyone, not just those with advanced technical skills. Phore will be easy to acquire and exchange for goods and services globally, with the ability to provide a smooth and intuitive user experience for people around the world.

The development of the Phore coin was only the beginning of our journey. Our flagship creation is the integration of Phore cryptocurrency with a fully decentralized marketplace. Users will be able to buy and sell items using Phore for payment, using private Phore transactions whenever they wish. We will support and develop an ecosystem of Phore applications and businesses built by both the Phore core team and the Phore community. This will be accomplished through both internal development by the Phore core team and community, as well as through partnerships and by assisting in the launch of various other business and educational ventures that are aligned with the Phore vision.

Phore will provide a robust, secure, private, and completely decentralized network backed by the Phore cryptocurrency. It will consist of a thriving ecosystem of privacy-enabled decentralized applications and a marketplace that will provide real world applications to enable private commerce and new privacy-enabled business models. No permissions will be required to utilize Phore or its applications as there is no centralized authority behind them. Applications and improvements to the Phore core code will be made by the Phore community, for the Phore community. Phore will be money, on your terms.

Perhaps most important to our development and success is our thriving and expanding community. The Phore coin is structured to be governed by the community in a transparent fashion. The development team is growing constantly through both outreach and active recruiting by the core team as well as proactive ideas, contributions and offers to help coming from the Phore

community. We are proud of the large and growing following Phore has gathered to date including more than 8,000 followers on Twitter and over 4,000 members of our Discord and Telegram groups. We are fostering a friendly and engaging environment where participation and contribution by everyone in the community is encouraged.

History and Accomplishments

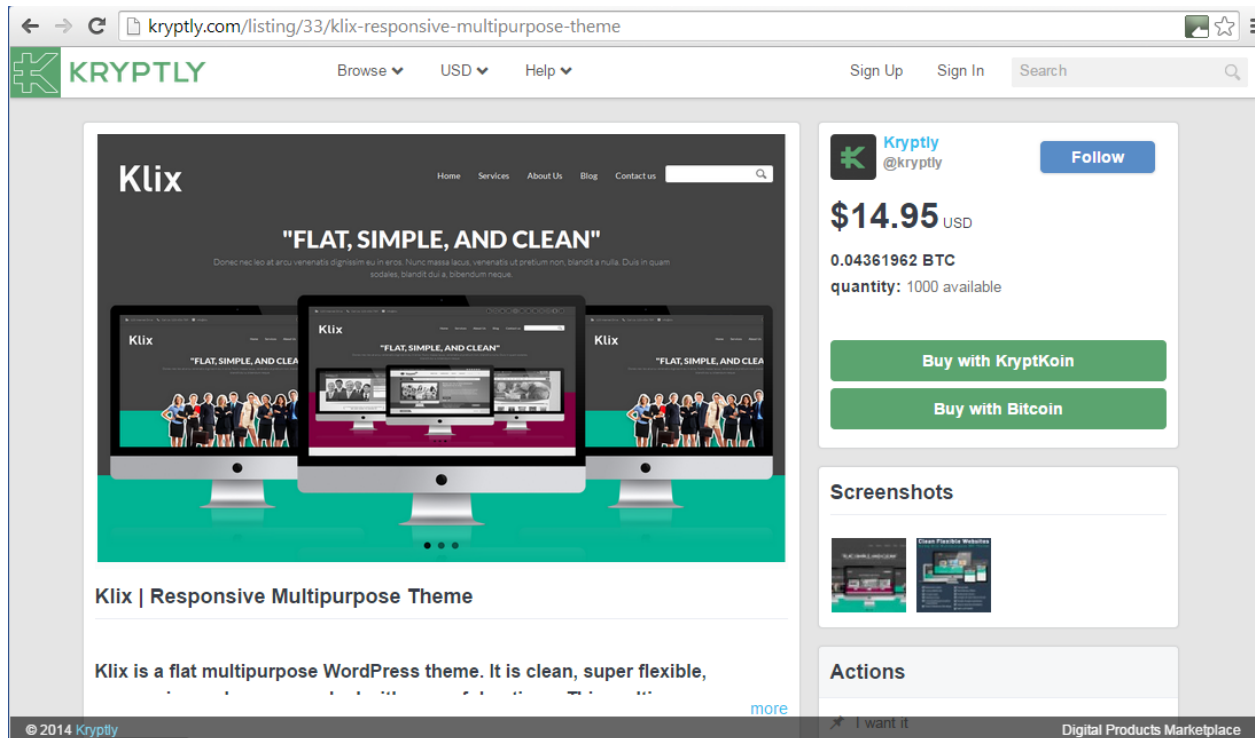
Phore has already come a long way since the project kicked off in September 2017, including formation of the core team, the launch of the Phore cryptocurrency, and significant work towards our initial 2018 milestones.

KryptKoin Origin

Phore is a digital privacy cryptocurrency, an update and rebrand of KryptKoin (KTK) which was pre-announced in May 2014, and whose distribution started on May 21st, 2014.

There was no pre-mine for KryptKoin. It was distributed equally to people who qualified for a stake. In total, 500 stakes were distributed in 2 stages. Bonus KTK was given to those who held for 30 days. There was no ICO, and no developer pre-mine.

The developer, Phroshi, received 1 stake, the same as every other stakeholder. Following launch, KryptKoin quickly developed a large and faithful following and introduced an online marketplace in 2015, which included Paypal integration, where digital items such as Wordpress themes were bought and sold.



Here is a link to a short promotional video for the KTK market published on Aug 20th, 2014 <https://www.youtube.com/watch?v=Sj3f7ucJBlo>

Coin Swap

To accommodate new features and accelerate the Phore vision, the existing code needed to be completely rewritten. This was accomplished with a coin swap from KryptKoin to the new Phore. The initial Phore code base was created from a fork of the PIVX project, which in turn was forked from Dash, all of which have roots going back to Bitcoin Core code.

A two-month window was announced and advertised on cryptocurrency forums and social media for existing KTK holders to swap their coins for new Phore on a 1:1 basis. Well over half of the existing KTK was swapped for Phore coins

through this process. This window closed on November 18th, 2017, and as a result of unclaimed coins, over 7 million Phore (PHR) were destroyed, reducing the total supply to just over 11 million Phore.

Proof of Stake

Unlike bitcoin which uses Proof of Work (PoW) and mining as the primary mechanism around building their blockchain and achieving consensus, the Phore core blockchain is based on Proof of Stake (PoS). Proof of Stake bases rewards based on how much stake each participant has in the Phore network, and for their participation in validating and processing Phore transactions and blocks. This alternative method of achieving distributed blockchain consensus offers a number of advantages over PoW consensus algorithms:

- It uses vastly less computing power and electricity to secure the Phore blockchain. There are estimates that Ethereum and Bitcoin PoW mining burns over \$1 million in electricity and related costs per month. PoS is much more sustainable and environmentally friendly in comparison.
- There is less need to issue net new coins to provide incentives to participate in the blockchain process, leading to less need to inflate the currency. Phore transaction fees are tiny compared to Bitcoin fees, for similar reasons since there is no further need to incentivize a miner to process them. Also, the transaction fees are burned as they are used, reducing the total supply to offset some of the increase in supply from PoS rewards. As transactional use increases, it is possible there could even be negative net issuance of coins.
- PoS allows for greater decentralization, since a Phore node can operate on very inexpensive computers. There is no need for a big centralized mining

farm as you see forming with many PoW coins. This greater decentralization makes it more difficult for centralized coordinating groups of nodes to form, and discourages any groups that do form from harming the Phore network.

These and other benefits of PoS give Phore a solid, secure foundation to build on. Nodes on the Phore blockchain network have to be holders of the Phore currency to participate in blockchain mining, and they have a natural incentive to protect and enhance the value of the currency. Ethereum is in the process of switching from PoW to their PoS algorithm (Casper) right now, launching a testnet for it on January 1st.

Anyone with a Phore wallet can keep their wallet online with staking enabled to help process and confirm Phore transactions and build the Phore blockchain. In return for providing this service and securing the Phore network, stakers can receive a portion of the block rewards, that as of this writing are 2.8 PHR awarded for each block, which is targeted to happen every 60 seconds. The likelihood of being chosen to mine a block and get the associated staking rewards are based on the number of Phore being staked by each Phore node.

The Phore community and advisors have developed a detailed staking guide and provide support in the Discord group for users needing assistance setting up their wallets for staking.

Masternodes

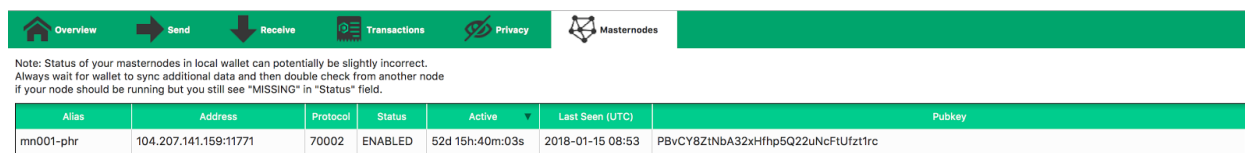
Phore has also implemented masternodes, which are enhanced Phore nodes that provide additional services and security to the Phore network. Two of the current services provided by masternodes are processing zerocoin (zPHR) private transactions (see Zerocoin Protocol below), and handling the Phore budget

governance process (see Masternode Governance below), and additional services may be added in the future as Phore's feature set expands.

Anyone with 10,000 Phore can set up and operate a Phore Masternode, which is online 24/7 and helps provide additional security, reliability, and performance to the Phore blockchain. Given their large stake in Phore, Masternode owners have an even larger incentive to maintain the integrity and security of the Phore blockchain, and to help guide the growth and value of Phore over time.

To establish a masternode, 10,000 Phore is locked as collateral in a transaction performed in the person's Phore wallet, and that transaction is paired with the masternode that can be set up to run on a Virtual Private Server (VPS) in the cloud, or subject to certain technical conditions can be run at home on a PC or even a Raspberry Pi. Phore masternodes support IPv6 and multiple masternodes can be run on a properly sized IPv6 enabled VPS. Masternodes can also be set up to run using Tor/Onion Routers for additional privacy.

Once the masternode is set up, it will keep operating even if the wallet containing the 10,000 Phore is offline, potentially even in cold storage, providing additional security to the masternode owner.



Alias	Address	Protocol	Status	Active	Last Seen (UTC)	Pubkey
mn001-phr	104.207.141.159:11771	70002	ENABLED	52d 15h:40m:03s	2018-01-15 08:53	PBvCY8ZtNbA32xHfhp5Q22uNcFtUfzt1rc

Masternode tab from Phore wallet

If the masternode owner ever wishes to stop operating their masternode and spend some of their 10,000 Phore, they can unlock their coins and stop their masternode at any time. Like stakers, masternode owners receive a portion of the block rewards, as of this writing 4.2 PHR is awarded to a masternode owner for each block. For a masternode owner, this is a new business model, with some

similarities to owning a rental property--for some initial work and ongoing maintenance, a passive income stream is created, and the underlying asset (10,000 Phore) can fluctuate in value, and perhaps eventually be sold.

As of this writing there are about 450 active masternodes operating in the Phore network. This equates to about 38% (4.5 million Phore) locked as masternode collateral, decreasing the circulating supply from ~11.7 million to ~7.2 million Phore. The return on investment for a masternode owner based on these conditions is currently about 400 Phore per month, which equates to about a 48% annualized return. These numbers will change as masternodes are added or removed from the Phore network, and as block rewards gradually decrease over time at specified block intervals.

The Phore team has developed a detailed guide for masternode setup, and the Phore team and community provide support in the Discord group for less technical people who need assistance setting up their Phore masternode.

Zerocoin Protocol (zPHR)

A Bitcoin transaction is recorded on the blockchain ledger and is visible for anyone to see. The sender's address, receiver's address, transaction amount, and any other details or conditions associated with the transaction are all public. While this is a great feature for maintaining accurate account balances, and preventing double spending of the same coins, it reveals a lot of information about the sender and receiver of the transaction. Analytics of blockchain data can use this information to guess which addresses belong to the same wallet. Pieces of information like this can be analyzed for patterns or other data (e.g., deposits from multiple addresses to a single deposit address at an exchange, transactions recorded with their associated IP address) that help associate different addresses,

and may reveal the identity of the owner. The US government and private companies have described similar techniques they use to identify the owner of an “anonymous” cell phone number based on when and who they call and other metadata available from cell carrier records.

We believe every individual may want at least some of their transactions kept private. If you are paid with a cryptocurrency, you may not want your paycheck recorded publicly forever. You may simply not want any of your own personal data to be aggregated and analyzed or to have your purchasing patterns gathered and sold by corporations without your knowledge or consent.

Phore uses a customized version of the zerocoin protocol called zPHR to provide private transactions. Zerocoin has been thoroughly reviewed in the academic community, and you can review the original zerocoin whitepaper published by the Johns Hopkins University Department of Computer Science³.

zPHR is a coin mixing technology that converts (“mints”) Phore into zPHR and adds the person’s Phore to an accumulator pool of zPHR on the Phore blockchain. Zero knowledge proofs are used between the user and a Phore masternode to verify the transaction without revealing or recording the link between sender and receiver on the Phore blockchain. The interaction between Phore masternodes and users make use of RSA-2048 encryption challenge keys so that you do not need a developer trusted setup to achieve this. As a result, no one knows all the information they would need to reveal the identity of the person using a zPHR transaction from start to finish.

The zPHR protocol performs this anonymization service efficiently, with zPHR

³ <https://isi.jhu.edu/~mgreen/ZerocoinOakland.pdf>

minting taking as little as half a second, and spending zPHR taking as little as 2.5 seconds. It also provides flexibility to choose your own level of security—you can specify having the Phore network mix your coins with all previously minted zPHR and those minted for 10 blocks beyond yours, all the way up to stating that it should mix your coins with every other zPHR from the beginning to the end of the Phore blockchain.

Masternodes provide the zPHR minting service, and interact with the zPHR accumulators on the Phore blockchain to issue credits and debits as zPHR are minted and spent.

People who own Phore can use their Phore wallet to mint their Phore into zPHR coins for a small transaction fee (0.01 PHR per minted zPHR coin) in a variety of standardized denominations ranging from 1 to 5,000 Phore. The transaction fee for minting zPHR is higher than a normal transaction, because it is a computationally intensive action and therefore needs a mechanism to prevent spam/freeriding from overwhelming the Phore network. Like other transaction fees, the zPHR fees are burned, reducing the total supply of Phore. Users can later choose to convert their zPHR back into PHR by sending them to one of their own wallet addresses, or to spend them at any other Phore address, and spending zPHR has no transaction fee. While they are held, zPHR are stored in the user's wallet like secure vouchers for PHR that can be redeemed anonymously.

ZeroCoin PHR (zPHR)

ZeroCoin Actions:

Mint ZeroCoin zPHR Available for Minting: 196.68 PHR **Reset**

Coin Control... **Quantity:** Coins automatically selected **ReScan**

Amount: Coins automatically selected

Mint Status: Okay

zPhr Control zPhr Selected: 0 Quantity Selected: 0

Spend ZeroCoin Available Balance: 201 zPHR Security Level: 42

Pay To:

Label:

Amount: zPHR

☐ Convert Change to ZeroCoin (might cost additional fees) ☐ Minimize Change

ZeroCoin Stats:

Total ZeroCoin Balance: 1201 zPHR

Denom. with value 1: 1 x 1 = 1 zPHR

Denom. with value 5: 0 x 5 = 0 zPHR

Denom. with value 10: 0 x 10 = 0 zPHR

Denom. with value 50: 0 x 50 = 0 zPHR

Denom. with value 100: 2 x 100 = 200 zPHR

Denom. with value 500: (2 immature) 2 x 500 = 1000 zPHR

Denom. with value 1000: 0 x 1000 = 0 zPHR

Denom. with value 5000: 0 x 5000 = 0 zPHR

PHR

Another interesting benefit of storing your PHR as zPHR is that on the blockchain, the associated Phore addresses will no longer associate the PHR stored in zPHR accumulators with the holder's address(es). If someone was concerned about being targeted by hackers because they have a high balance in their account, using zPHR will mask their true balance, creating the ability to hold "stealth" value that cannot easily be traced back to the user's wallet.

We believe zerocoin is one of the best available methods to provide flexible, optional, secure private cryptocurrency transactions.

Phore Community

The Phore community is the heart of the project. Since its inception, individuals in the Phore community have not only shared their ideas and aspiration for this project, they also guided the direction of the project. The community started with

a small group of early adopters who met on the original slack channel. Since the project did not have an ICO or pre-mine these early investors chose to spread word of the project through their own time, effort, and personal funds. These efforts were initially spent posting in various forums and social media outlets. The goal of these efforts was aimed primarily at creating a large and vibrant community.

These initial efforts were quite successful. More and more interested investors quickly joined the community, which eventually moved to using the Discord app based on the community's request. Several large Twitter promoters quickly recognized the value of Phore and helped to spread word to their followers. However, the most reported reason for people choosing to invest in Phore was the community itself. The community is very active, and there is almost always a team member available in the Discord to provide support or direct community members to where they can find information they seek. Furthermore, there is a very positive tone to our community. People are friendly, non-judgemental, and eager to support each other.

The early individual efforts to spread word of Phore was quite successful on a shoestring budget. Hundreds of followers were noted on Twitter, Discord, and the Telegram channel. In December of 2017, the governance model came into play, which provided development funds based on proposals submitted by the team and/or community. The initial budget focused on increasing project development and further spreading word of Phore to the world. These funds were used to increase awareness through social media campaigns. These appeared to be quite successful, given that our we currently have 1,100 members on telegram, 3,200 members on Discord, and 8,000 followers on twitter.

In line with the masternode budget governance process, Phore is directed by the

community. We actively engage with the community at every stage, to share our ideas and designs and gather feedback, and to listen and understand what the Phore community wants. We always want to be engaged, transparent, and responsive to the needs of the community, and to evolve our shared vision together as we move forward.

Phore Marketplace Development

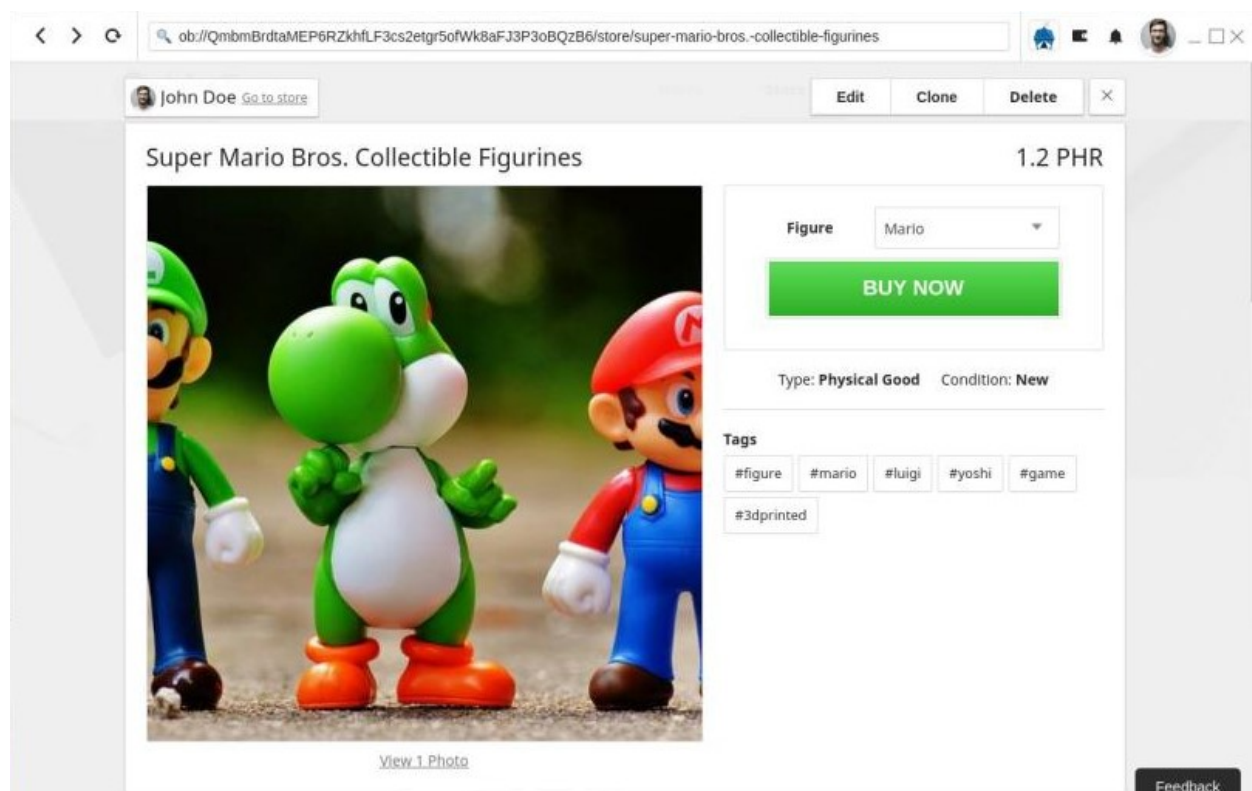
Since the successful launch of the Phore cryptocurrency, most of the development effort of the core team has been focused on preparing the Phore marketplace for its debut, scheduled to go live by the end of Q1 2018. The initial code base for the Phore marketplace was forked from OpenBazaar. This base provides the Phore marketplace with a solid foundation to build on, and meshes well with the core Phore philosophy of decentralized applications. See Q1 2018 below for more detail on the marketplace functionality that will be available during the initial launch.

The development team has been working hard to add the necessary features, user interface, and other changes needed to rapidly deliver a fully featured marketplace supporting private transactions based on the Phore cryptocurrency. In parallel with this, the advisors and Phore community have been identifying vendors that want to be part of the initial beta and launch, providing some of the first products and services available on the marketplace.

The Phore Marketplace is a fork of the OpenBazaar protocol. All transactions between two parties including an escrow system and moderation system are handled at a protocol level. This allows for a completely decentralized and trustless system for exchanging goods. Because all transactions take place at a protocol level, the marketplace itself is uncensorable. However, search engines

act as a centralized way of finding new stores on the Phore Marketplace. We plan to host one central search engine and open-source the code, allowing anyone to run their own search engine with their own rules.

Each shop in the Phore Marketplace has a unique address which identifies the data stored. This hash-based, decentralized system for storing data is a fork of the IPFS protocol. Specifically, it allows users to store and access store data without the need for a centralized server. Any shop can be accessed without a search engine simply by entering the URL of the shop.



Screenshot of a marketplace store item.

The marketplace is continuously being developed including the user-interface, the search engine, and the connection with the Phore network. An open-beta will be released in early-mid Q1 while the final version will be released later in Q1.

Masternode Governance

The funding and direction of Phore's funding is governed by those in the Phore community with the most stake in enhancing Phore's long term value--the Phore masternode owners, who are each staking 10,000 Phore as collateral for their masternode. The mechanism and process behind this governance is built directly into the Phore blockchain code.

10% of the blockchain rewards for Phore are reserved for funding development proposals to enhance the value of Phore. Each budget cycle is 30 days, and anyone can submit a development proposal for a 50 Phore transaction fee that is burned when the proposal is submitted. The Phore team has established a forum at <https://forum.phore.io> for people to post, debate, and discuss the pros and cons of each proposal. Each of the masternode owners can vote yes, no, or abstain on each of the development proposals, and for a proposal to be approved, it needs to be submitted at least 3 days before the end of the budget cycle, and to get a minimum of 10% of the masternode population to vote Yes (or more to offset any 'No' votes). Proposals can be submitted for a one time payment, or spanning multiple budget cycles for ongoing funding of longer term projects.

```
{
  "Name" : "Jan15Budget",
  "URL" : "https://forum.phore.io/t/january-15-budget/71",
  "Hash" : "ca29a85788ad81cf4712d94354afdf9eaa4345a3e2107e8a14d0bc1da3ad8247",
  "FeeHash" : "42ae927f73484b203a7c4f91a8821c75c88bb855a64179ce6e4cd384d2dd65e0",
  "BlockStart" : 172800,
  "BlockEnd" : 216001,
  "TotalPaymentCount" : 1,
  "RemainingPaymentCount" : 0,
  "PaymentAddress" : "PEQNR5oGqggzRcSQqtgaefcYiYbFhDMoBm",
  "Ratio" : 1.00000000,
  "Yeas" : 82,
  "Nays" : 0,
  "Abstains" : 0,
  "TotalPayment" : 27500.00000000,
  "MonthlyPayment" : 27500.00000000,
  "IsEstablished" : true,
  "IsValid" : true,
  "IsValidReason" : "",
  "fValid" : true
}
```

JSON representation of one of the January 2018 Phore budget proposals

Two days before the end of the budget cycle, voting stops and the budget is finalized. Someone must submit another 50 Phore transaction fee to trigger the finalization of the budget, and then the masternodes will sort the ranked list of proposals by the Yes/No vote ratio, and allocate funds until the last proposal is reached or funds for the budget cycle run out. When the block that begins the next budget cycle (superblock) is reached, the finalized budget is paid out to the addresses associated with each approved proposal.

This system provides a decentralized method to determine how to best allocate funds for Phore's development on an ongoing basis. Masternode owners decide who is paid and how much (whether it's the core team or not), and for which changes or feature additions. Unlike an initial ICO or pre-mine, this funding method allows anyone with a valuable and popular idea to gain funding, it provides a recurring and long term funding source, and it better ensures that the funds are used over time to directly support the development of Phore.

Charitable Donations

Whilst its easy to get caught up in this fast paced, rapidly growing industry, it's also very important to be aware of just how fortunate we are. Within the current cryptosphere, everyone is blessed in terms of having some form of access to both electricity and the internet. However, in such a greed fueled space, we need to remember that there are people less fortunate who need help. Here at Phore, we intend to do this.

Although we are a relatively young project and have no mass pool of funds in terms of ICO or pre-mine, we actively look to give to those who are less fortunate. So far we have donated to 6 different charitable organisations:

- Make A Wish Foundation : A charity fulfilling "wish" experiences for children with life-threatening medical conditions.
- Children International : A global non-profit organization that helps children break the cycle of poverty.
- Covenant House Toronto : A homeless shelter for the youth of Toronto offering services such as education, counselling, health care and employment assistance.
- Life For The World (Haiti) : An organization which focuses on supporting orphanages by creating sustainable-living programs, providing life-skills and training to orphans re-entering the world.
- American Kidney Fund : A non-profit organization working on behalf of the 31 million Americans with kidney disease, providing support and resources.
- Canadian Mental Health Association : A voluntary organization who provide nationwide services and support to people experiencing mental illness and their families.

These donations coincided with our community giveaway 'All I Want Phore Christmas'. Our charitable nature is also reflected by Phore team members as well, frequently matching donations on their own accord. Advances in technology are made in order to drive commerce and enhance quality of life. Phore is committed to making the world a better place.

Current Phore Cryptocurrency Statistics

Phore uses Proof of Stake and Masternodes to secure the network and provide for a deep level of privacy and security. Phore was designed to have fast block times (one per minute) and low transaction fees compared to Bitcoin.

Total Supply (as of January 15th, 2018): ~11,722,000 PHR

Circulating Supply (as of December 29th, 2017): ~7,182,000 PHR

Block Time Target: 60 seconds

Transaction Fee: 0.01 for zPHR minting, usually less than 0.001 for other transactions

Transaction Confirmations Needed: 6 for normal transactions, 51 for masternode/staking rewards

Block Maturity: 50

Proof of Stake (PoS) Reward: 2.8 PHR per block

Minimum Stake Age: 3 hours

Masternode Reward: 4.2 PHR per block

Masternode Collateral: 10,000 PHR

Number of Active Masternodes (as of January 15th, 2018): 454

Phore Development Fund - 10% of block rewards, paid every 30 days (43,200 blocks)

The block rewards adjust over time as the Phore project matures to control inflation of Phore supply over time, according to the following schedule:

Date	Starting Block	Ending Block	Masternode Reward	Staking Reward	Development Fund
Current	Current	250,000	4.2 PHR	2.8 PHR	0.77 PHR
Mar. 9th, 2018	250,001	518,399	2.7 PHR	1.8 PHR	0.45 PHR
Sep 11 th , 2018	518,400	1,036,798	2.16 PHR	1.44 PHR	0.36 PHR
Sep 6 th , 2019	1,036,799	None	1.62 PHR	1.08 PHR	0.27 PHR

How is Phore Different?

Phore has incorporated features to differentiate it from other coins such as Particl, Monero, Zcash, Dash and PIVX. For a quick breakdown of what makes Phore stand out from the rest, please see the diagram below:



Privacy Coins Compared

Jan 15, 2018

Specs ▾	phore	MONERO	VERGE	PIVX	particl
Network Consensus	Proof of Stake (PoSv3)	Proof of Work (CryptoNight)	Proof of Work	Proof of Stake (PoSv3)	Proof of Stake (PoSv3)
Circulating Supply	7,182,000 PHR	15,605,931 XMR	14,577,197,956 XVG	55,344,228 PIVX	8,837,157 PART
Market Cap	\$48M	\$5B	\$2B	\$699M	\$198M
Maximum Supply	∞	∞	16.5B	∞	∞
Block Time	60 seconds	2 minutes	30 seconds	60 seconds	120 seconds
Features ▾					
Decentralized Marketplace	Late Q1 2018	---	---	---	Beta Q1 2018
Smart Contracts	Q4 2018	---	---	---	---
SegWit	Q2 2018	---	---	---	✓
Atomic Swaps	Q2 2018	---	---	---	✓
Decentralized Crowdfunding	Q3 2018	---	---	---	---
Masternodes	✓	---	---	✓	---
Staking	✓	---	---	✓	✓
Privacy Technology	Custom Zerocoin (zPHR)	Ring Signatures (Coin Mixing)	Tor / i2p	Custom Zerocoin (zPIV)	CT (Testnet: RingCT)
Private Sends Optional	✓	---	---	✓	✓
Tor Enabled	✓	✓	✓	✓	✓
IPV6 Support	✓	✓	✓	✓	✓



Have questions? Please join us on Discord or any of our social channels.

Phore Roadmap

Phore has set out an ambitious roadmap for 2018 that will transform the Phore blockchain from an already fully featured privacy cryptocurrency into a powerful platform for developing and deploying private decentralized blockchain applications and solutions. It will also open up tremendous future opportunities for future expansion of the Phore ecosystem using the architecture being put in place now.

The sections that follow outline the most important milestones we intend to deliver in 2018. The team already has an established track record of meeting or beating our milestones. As discussion, debate, and design continues within the Phore core development team and the Phore community, we will refine and update these plans. It is likely with their feedback we will add other features and upgrades to Phore throughout the year.

Q1 2018 Milestones

Blockchain Technology

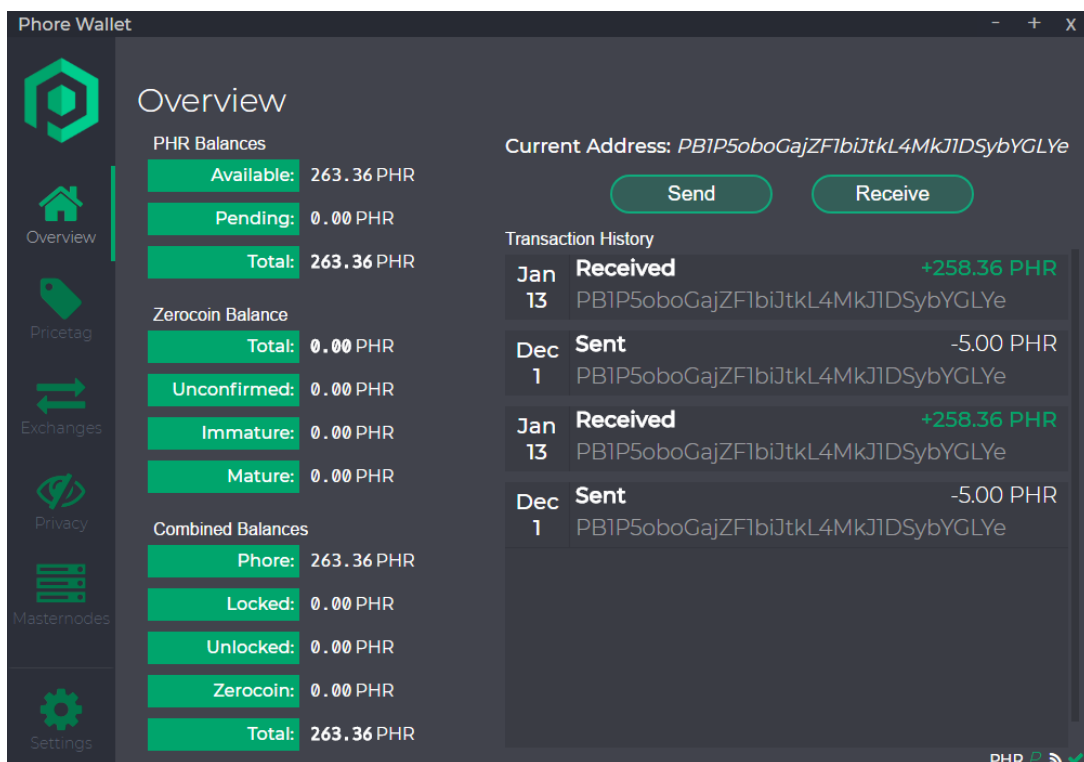
Integration of Phore into the marketplace is the focus during this quarter. Ongoing review and maintenance of the core code will be conducted. In addition, initial testing and implementation of the segwit ahead of the full adoption that will occur in the next quarter.

Web Wallet and Android Wallet Release

One part of the Phore vision is to make Phore available to as many people as possible, and to be easy to use. To that end, two new wallets will be introduced in Q1 2018:

The Android Wallet will be a mobile wallet available for download from the Google Play Store and provide a secure and speedy mobile connection with the Phore blockchain. We also plan to incorporate two-factor authentication (2FA) into this wallet as well as the full Phore desktop wallet to provide users with an additional layer of security to protect your Phore.

The Web Wallet will provide a platform for online hosted Phore wallets, which will allow a more convenient option for people to store Phore without having to run a full Phore wallet on a laptop or mobile device.



Screenshot of an early version of the new wallet UI

Wallet and Core Upgrades

The Phore core development team will be continually maintaining and updating Phore's code to ensure that the currency and wallets are safe and secure. This will continue throughout 2018. During Q1 we will also be making updates to support future 3rd party wallet integrations with support for hardware wallet integrations coming later in the year.

Masternode Setup Automation

While Phore has provided an excellent guide and technical support to users wanting to set up and run masternodes, we recognize that the setup process could be more automated than it is today to make it easier to use. The Phore team will be developing a more automated, simpler method for setting up Phore masternodes.

Phore Budget Governance Website

We will be rolling out a website that interacts with the Phore blockchain to transparently show the Phore budget proposals, voting, and status of the budget process. This will add transparency and ease of use by taking information that previously was

Phore Marketplace Launch

An open-beta will be released in early-mid Q1 with the final version being launched towards the end of Q1.

Phore Developer Team Expansion

To achieve Phore's ambitious vision for 2018, we will be adding experienced developers dedicated to development of the Phore core blockchain technology, products and services, both as part of the Phore core team as well as increased developer participation within the Phore community. We are already in discussion with several talented developers about joining the Phore team and this will continue through Q1 2018.

As part of this expansion, we will start a paid internship program, which will help us develop and attract the best blockchain graduates from universities around the world.

Continued Team Recruitment

Further specialists will be recruited to Phore, focusing on skills in developing and implementing Smart Contracts, as well as a Micro-Lending and investment expert for Phore Labs.

Q2 2018 Milestones

Segregated Witness (SegWit) Activation

Segregated Witness changes the format of transactions on the blockchain, separating the witness data (scriptSig and scriptPubKey) into a separate from the rest of the transaction data that is covered by the transaction ID (txid). Without Segregated Witness, it is possible that the witness data could be altered slightly

by a node on the network, or one of the signers could change their signature. The same amount of coins would be paid to the same addresses, but the transaction ID would change.

By separating the witness data from the data that the txid hash covers, it prevents the transaction from being malleable, and brings a number of benefits:

- Writing wallet code is simplified. One of the most convenient ways for wallets to track their spend transactions is to look them up the transaction ID. When the txid can change, wallets need to write extra code to deal with that possibility.
- Spending outputs from unconfirmed transactions becomes more reliable. If Transaction A pays an output, and transaction B spends that output, it is possible that the witness data from the first transaction will change, altering the txid, and depending on the sequence of events it could invalidate transaction B. SegWit prevents this from happening.
- Increased transaction throughput and scaling. Phore is already very fast and efficient at transaction processing with a 60 second block time and a 2MB maximum block size. SegWit counts the witness data as $\frac{1}{4}$ of its actual size, allowing more transactions to be included in each block and increasing scalability and performance.
- Solving the transaction malleability problem makes adding sidechains, similar to the Lightning Network, become less complex to write and more efficient in their use of blockchain data.
- Smart Contracts also become easier to design, review, and monitor.

These last two benefits are very important to Phore's vision. Later in 2018 we will be introducing a Phore smart contract platform, and we are planning to use a sidechain as part of the smart contract blockchain architecture. SegWit activation sets the stage for this new platform.

iOS Mobile Wallet / App

With more mainstream interest in cryptocurrency multiplying by the day it is important that Phore introduces a mobile wallet for the iPhone and iPad, which facilitates use by the large amount of Phore holders on iOS, bringing it to parity

with Android. The process for creating and distributing this through the Apple Store is more complicated than Google Play, which is why the release has been scheduled to take longer.

Creation of The Phore Foundation

An institute will be set up within Phore to develop long-term e-commerce solutions, investments, partnerships. Its aim is to strengthen and sustain Phore, allowing it to quickly react and pivot to challenges in the future. Phore Labs, part of the Phore Foundation, will work as an incubator/seed investor, primarily identifying potentially cutting-edge digital services and products. These will be sourced from individuals, universities, start-ups, and cooperatives around the world.

Q3 2018 Milestones

Smart Contracts

Smart Contracts will bring Phore to an entirely new level of capabilities. Phore will no longer be just a cryptocurrency—it will still have that as its foundation, and on top of that, Phore users will be able to write, compile, and execute complex decentralized applications (dApps) that will run entirely on the blockchain and be fully integrated with the Phore blockchain.

In some of the simpler use cases we have in mind, Phore Smart Contracts will allow the Phore Marketplace to support much more flexible terms for things like escrow and other terms surrounding purchases, making the marketplace more secure and reduce the chances that someone will not fulfill their part of the

transaction. While the marketplace will have an arbitrator capability from the initial launch, smart contracts could potentially make arbitrators obsolete and unnecessary. Similarly, for Crowdfunding, a smart contract can be written for the crowdfunding campaign that will programmatically control the collection and escrow of funds collected, and either distribute them to the successful campaign owner when the necessary level of funding is reached within the prescribed time frame, or automatically refund the Phore to the contributors if the necessary conditions are not met.

The Phore Smart Contracts platform will be much more powerful than this. More advanced use cases could include entirely new decentralized business models running on the Phore smart contracts blockchain. A decentralized cryptocurrency exchange, trustless prediction markets, ride or home sharing applications, or countless other services ranging from tiny apps all the way to complete businesses could take advantage of the decentralization, advanced programmatic control, privacy features, security, performance, and resilience of the Phore architecture.

The first major architectural upgrade we will be making to support Smart Contracts will be building in support for sidechains. This provides a number of advantages over trying to add smart contract functionality directly to the Phore main blockchain (mainchain). When Satoshi Nakamoto created Bitcoin, he realized that optimizing a coin for one use case necessarily cuts off the ability to optimize for a different use case—making a fast, private, and scalable currency blockchain looks very different and makes different tradeoff decisions compared to a very flexible and robust smart contracts blockchain. Sidechains removes this limitation by allowing Phore coins to traverse from the Phore mainchain to the Phore Smart Contracts sidechain, and later come back to the Phore mainchain. By

doing this, each chain can be optimized for its particular use case, without needing to make compromises on the other blockchain. It also can help solve some of the issues we've seen in the early days of Smart Contracts, including the DAO and Parity exploits that Ethereum users dealt with in 2017.

It's important to note as well that support for sidechains opens up the ability for Phore to add other sidechains that are optimized for other use cases as well—smart contracts will be the first.

Phore will be able to move from the Phore mainchain to a two-way pegged Phore Smart Contracts sidechain to fund smart contract transactions. On the mainchain, it will appear that the funds have been sent (deposited) to a special address that is controlled by the miners of the Phore Smart Contracts blockchain, so from the Phore mainchain standpoint it will appear very much like a normal Phore transaction. A few times a year, withdrawals will be allowed from the smart contracts sidechain back to the Phore mainchain, with a long notice period and voting to approve each withdrawal in advance of the withdrawal date.

This infrequent withdrawal schedule allows plenty of time for the miners of the smart contracts blockchain to examine what is happening with each smart contracts transaction, and to disallow and deal with any attempts to exploit the system before any real damage is done. The only way an exploit could succeed would be for the majority of miners on the smart contracts blockchain to want it to succeed.

While such an infrequent withdrawal schedule may appear to be very inconvenient to someone who wants to use a smart contract and get their Phore coins delivered quickly, the architecture we are proposing deals with this by using instant atomic swaps between the Phore smart contracts sidechain and the

Phore mainchain—and this is one of the primary reasons we are building support for atomic swaps into Phore.

We will release more details on the specific implementation of Phore sidechain support as it becomes available. For anyone who wants to dive into the technical details, most of the enhancements we will be making are described in the following references from the Drivechain Project and some of the Blockstream co-founders:

<https://blockstream.com/sidechains.pdf>

<https://github.com/drivechain-project/docs/blob/master/bip1-hashrate-escrow.md>

<https://github.com/drivechain-project/docs/blob/master/bip2-blind-merged-mining.md>

Once we have the ability to use sidechains, we will build the Phore Smart Contracts blockchain as the first Phore sidechain.

The Phore Smart Contracts platform will allow Phore users to write smart contracts that include programming functions, state variables, and even external data as part of a complex transaction. It includes a client interface that will provide a smooth user experience to set up a Phore Marketplace Escrow transaction or a Phore Crowdfunding campaign, and allow various actions to be taken while the transaction takes place (e.g., release funds to seller, issue refund to buyer). The first smart contracts to be created on the Phore Smart Contracts platform are likely to be those that directly enhance and secure the functionality in the Phore Marketplace and Crowdfunding applications. Phore users will be able to write and compile their own smart contracts using high level languages to enable other applications and business models.

We will be building a number of core components to support Smart Contract functionality, building from and enhancing existing smart contracts

implementations, most of which originated as forks from Ethereum. These components will include:

- Tools and interfaces such as:
 - GUI (wallet and/or browser)
 - Clients
 - JSON RPC
 - dApp frameworks
 - Compilers
- Smart Contract Protocol that will support such things as:
 - P2P networking
 - Node discovery
 - Encrypted handshake and transport
 - Virtual Machine container
 - Smart contracts blockchain (mining, contracts, transactions, accounts)
- Decentralized storage
- Decentralized messaging

Our focus will be to deliver a solid minimum viable product (MVP) of smart contract functionality for alpha and beta testing, gathering feedback at every stage from the Phore community about the specific features they want to see in the platform when it is launched. Wherever possible we will be building in additional privacy features, such as leveraging zk-SNARKS zero knowledge proofs to enable private smart contract processing, in addition to the integration we will have with the privacy features already built in to the Phore cryptocurrency.

Like sidechains, we will develop more detailed technical white papers to explain the Phore implementation as we move forward. In Q3 we expect to be conducting Alpha and Beta testing, targeting an official launch in Q4.

Atomic Swap Implementation

Phore will be adding support for atomic swaps, initially as one of the core features needed for effective sidechain support for smart contracts. We will also be looking for ways to support direct atomic swaps between Phore and other leading cryptocurrencies as a way of making Phore more accessible and available.

Decentralised Crowdfunding

There have been many recent examples of major crowdfunding websites shutting down campaigns and being accused of political or other bias in choosing which projects are allowed to get funding on their platforms. We understand the reputational risk this sort of issue poses to a centralized crowdfunding company, and we think this makes a great argument for a decentralized, private crowdfunding application that does not require a company to grant permission to use their platform, or be subject to censorship based on political or other affiliations. We think this will be a huge benefit not only to projects needing funding, but also to those who want to support a certain cause or project without facing scrutiny based on their contributions.

Phore Crowdfunding will be completely decentralized, backed by the privacy of Phore cryptocurrency, and will be integrated directly into the Phore Marketplace. Projects looking for funding will be able to add information to describe their projects and the various options for contributions, and publish them on the Phore Marketplace. Users can then browse through crowdfunding campaigns and choose to contribute if they wish, utilizing the privacy features of zPHR if they don't want anyone to know the funding came from them, and optionally sharing

only the information the project needs to send the product when it is ready, and only to the campaign that needs the information, not to a centralized source that could be hacked or otherwise leak the information to others. Since there is no centralized platform or company involved, there will be drastically lower fees involved in a Phore Crowdfunding campaign.

Click and Collect Marketplace Vendor Pilot Programme. Location TBC

Traditionally 'offline' vendors in a city, which is currently under discussion, will take part in a month-long project, which allows buyers in the vicinity to place orders online through the marketplace and collect their goods in person later at their convenience.

Q4 2018 Milestones

Smart Contract Implementation

As described in the Q3 section of the roadmap, we will be launching the Phore Smart Contracts platform during Q4. This will include initial implementations of several smart contracts that will directly enhance the options and user experience in the Phore Marketplace and Phore Crowdfunding, and will also open up usage of the smart contracts to all Phore users.

Mobile App Development

Refinement of mobile apps for both iOS and Android. We will be looking to expand the features and functionality available on both mobile wallets to take advantage of more of the advanced features of the Phore platform.

VR/AR Marketplace Enhancement – Beta Testing

Open Community Pilot Programme of a parallel Marketplace site with VR/AR enhancement for those with and without headsets, seeking the ultimate, immersive buying and selling experience.

Click and Collect Incorporation into Marketplace

Incorporation of full-service that was piloted in Quarter 3, allowing local pickup of physical goods, following purchase on the online marketplace. It is expected that initial roll-out will cover 3-5 cities, with more widespread coverage planned for 2019.

Phore Labs Investment

Up to 10 Digital Products and Services will receive investment. These investments will be made in the form of Phore currency, and participants will sell exclusively through the Phore marketplace online for a fixed minimum period before being allowed to sell their product locally offline.

The Phore Foundation will invest in projects to help them reach market and then reinvest profits from the sale of these into further Lab projects.

2019 Goals

The Phore team has a lot of ideas on where Phore would go next in 2019 and beyond, ranging from additional mobile capabilities, full launch of VR/AR features, Phore Labs projects, partnerships with other projects, companies, and individuals, and even additional Phore sidechains.

However the team knows from past experience how valuable community feedback is to guiding a product's vision to meet the needs of that community. We highly value that input and want to stay agile and responsive and ready to work on the features that will most enhance the value of Phore.

Phore Core Team

Since our inception (late October 2017), we have experienced rapid growth in many areas, the team being one of them.

Phore began as a rebrand of KTK, with one lead developer; Phroshi and a total of five advisors (the official title - these were not merely advisory roles). Being restless by nature however, we've had to expand upon this in order to match our ambitions.

Over the past three months or so, our team has grown so much that we now boast over 25 official members. This number will continue to grow as we find people who we feel will aid in the progression of Phore.

Current Team Roster

Co-CEO :

Anthony Alleyne - Ubermaster (UK)

Thomas Ambler - Sage (UK)

CTO :

(Anonymous) - Moonshot (US) : Full Stack Developer

Head of Operations :

Shant Kel Khatcherian - Shanto (CA)

Developers :

(Anonymous) - Phorshi (UK) - Founder + Lead Developer

Julian Meyer (US) : Core Developer

(Anonymous) - Jacob (US) : Part Time Developer

(Anonymous) : Iced (NL) - Part Time Developer

Advisors :

Shunsuke Kurita - Liray-Unendlich (JPN)

Harrison Fischberg (US)

(Anonymous) - Toby (CA)

(Anonymous) - King (US)

(Anonymous) - Hman (US)

Legal :

(Anonymous) - Willich (UK)

(Anonymous) - Margo (US)

Marketing :

Pamela Paige - ThePinkCrypto (US) - Head of Marketing

Ramon Freriks - Ramon (NL) - Senior Marketer / Front End Developer

Ilies Graffion - La_Moquette (FR) - Graphics

Snatch (GER) - Social Media

Milky (GER) - Social Media

Communications / Operations Management :

Flipster (UK)

Branding and Partnerships :

Crypto_NL (NL)

Video Content Producer :

Zak.R (UK)

Vendor Relations :

CryptoJoe (US)

Research :

Keyser (US)

Community Management :

Jesse (US)

Further information regarding the team can be found at: phore.io/team

Phore is actively seeking to hire more staff and developers to strengthen the team on a regular basis as it continues to expand and evolve on a daily basis.

Join the Phore Community

We have already made tremendous progress launching the Phore coin and building the community, and the response has been incredible. More people are joining and contributing to our success every day.

2018 is going to be a very exciting year in Phore's development into one of the best advanced, secure, and flexible privacy cryptocurrencies available, with a strong ecosystem of applications and services to match.

Phore has an ambitious roadmap to achieve our vision, and we welcome you to join the community. If you have ideas on how to make Phore better, we want to hear them. We want everyone to contribute to improving Phore using the skills they have to offer, whether it's development, user interface design, spreading the word about Phore to your Youtube followers, or debating the direction of Phore's roadmap, budget, and design decisions.

Take back control of your money. Download the Phore wallet from our website, and stop by the Phore Discord and join the community today.

Links

Official Website

phore.io

Discord

<https://discordapp.com/invite/Aucncz5>

Bitcointalk

<https://bitcointalk.org/index.php?topic=2307909.0>

Bitscreener

<https://bitscreener.com/coins/phore>

Slack

<https://phore-project.herokuapp.com>

Twitter

<https://twitter.com/phorecrypto?lang=en>

Facebook

<https://www.facebook.com/Phore-1996158580662988/>

Github

<https://github.com/phoreproject/Phore>

Block Explorer

<https://chainz.cryptoid.info/phr/#>

Third Party Masternode Sharing Service

<https://www.hostmns.net/phore-pool>

Exchanges and Metrics

https://www.cryptopia.co.nz/Exchange/?market=PHR_BTC

<https://coinsmarkets.com/trade-BTC-PHR.htm>

<https://coinmarketcap.com/currencies/phore/>

<https://www.coingecko.com/en/coins/phore#panel>

<https://bitcointalk.org/index.php?topic=2307909.200>

<https://scrypto.io/s/mns-phore/>

Forum

<https://forum.phore.io>

AMA - Nov 11th, 2017

<https://medium.com/@fishfishfish313/phore-ama-ask-me-anything-on-november-11th-2017-f69ecb91eb1>

Facebook Fan Group

<https://m.facebook.com/groups/249350618927881/>

Bitcointalk Fan Page

<https://bitcointalk.org/index.php?topic=2461070.0>

Telegram

https://t.me/joinchat/F0zLDwzFC8r91eem6x_cBQ

Crypto Delver

<https://cryptodelver.com/coin/phore>

Masternodes.online

<https://masternodes.online/currencies/PHR/>

Masternodes Pro

<https://masternodes.pro/stats/phr>



© Phore 2018