PHANTOM

Private Smart Contract Platform

Version 1.1

info@phantom.org

Abstract. Privacy designed to protect the integrity of a peer-to- peer transaction or contract is essential in a world where our privacy seems to leak with the power of any government or hacker having the ability to use back doors to view our activities.[1] The purpose of cryptocurrency in its root is to create a peer-to-peer cash system[2] designed to give the power back to the people separate from intermediaries and centralized entities while being cryptic to protect the transactions privacy. Blockchain has served its purpose to be a trust less ledger where data cannot be forged or altered and consensus can be met so that a transaction can take place which has therefore created a handful of worldwide solutions. Smart Contracts give users the ability to interact through a segment of pre- defined configurations to allow the transactional purpose and selected purpose to be executed without doubt. Privacy driven cryptocurrencies[3] have given the power of privacy back to the people while maintaining consensus. However, the combination of these elements is essential to create a platform and protocol designed for meeting these solutions without having the need to use them individually. Enabling the ability to where a smart contract is trust less with the blockchain to meet consensus and remain decentralized, but viewable to only those who are the intended parties is essential to create a value of security, privacy, and trust without compromising performance and decentralization. PHANTOM will be designed to be a network protocol that will allow deployment of private smart contracts and currencies with capabilities to build encrypted, autonomous, decentralized applications.

1. Introduction

Designing a network where its core functions illustrate the support for user privacy is important to building an ecosystem of solutions surrounding anonymity. The power of Ethereum is the fact that it is one of the most widely used smart contract platforms using the infamous Ethereum Virtual Machine.[4] Smart contracts have been designed with unique properties designed to create decentralized applications (dApps) and a variety of other use cases such as voting, record keeping, digital identities, IoT, real estate, auctions, gaming and more. The fact of the matter is, as much as these use cases are applicable, there is an issue of keeping the data private to the parties since the information being transacted is open and all publicly viewable on the blockchain. [5] All transactions and data that runs through Ethereum is publicly viewable to all participants and users of the network. Scaling the system to become interoperable with other blockchains and use a method of consensus that allows for a more efficient system is not exactly in the road map of Ethereum [6]. Realizing these protocol realities, there is a dire need of a platform where users can reap the benefits of running a decentralized application such as a lending system, but maintain the privacy needed to keep the transactions discrete between the parties involved. PHANTOM allows these smart contracts to become privately placed within the ledger where its deployment and code can be seen by the nodes to be verified valid, however the transactions running through the smart contracts will remain encrypted with the ability to be viewed by those only holding the secret view keys within their wallets.

Ethereum currently allows the ability of tokens to be created within its network by running them through a ERC20 protocol [7]. While these tokens may be unique to size, functionality within the smart contracts decentralized applications, and by name, they all operate within the frameworks of Ethereum which lack privacy to their usage and the transactions running through them [8]. Withstanding the fact of these issues, the feasibility to transact within the Ethereum network and its popularity has given these platforms the comfortability to operate on it. However, Scalability lacks for these tokens as well as they rely on the infrastructure of Ethereum.

PHANTOM's Blockchain, which is forked from ARK, gives an operator the tools needed to build a compatible ecosystem while not being stuck to hold all the frameworks of the parent design. Instead of creating tokens on the network to perform the same framework mechanism that it has, there is an ability to launch your own ready-made blockchain. [9] These blockchains are already built with interoperability and allow the communication between PHANTOM and ARK based blockchains based on the ARK Smart Bridges [10]. This will allow companies to create specific applications that can communicate privately within their own network but also communicate with other blockchains that have the Smart Bridge [11] protocol as well. For example, let’s say you wanted to execute a smart contract running on Blockchain B but hold an asset from Blockchain A. You could send the instructions through a Smart Bridge right within the wallet to execute the event. The code in the blockchain B is always scanning and listening for a Smart Bridge transaction and will collect this data and trigger the function to issue a contract however the relay of the data would remain private using a PHANTOM based blockchain.

2. PHANTOM Experience

PHANTOM will be designed to give a dynamic user interface to make the processing of transactions and deployment of smart contracts seamless all within the client. The clients will be available on multiple platforms such as Linux, Windows, MacOS, and mobile. These clients will all be able to perform the same functionalities of a full node. We will be creating a web interface as well similar to MyEtherWallet [9], that will give users the ability to use the transactional features of PHANTOM all from a web based device if they are unable to install a client. Users will be able to deploy a ready-made blockchain by utilizing ARK's technology and PHANTOM's privacy protocol that operates on-chain.

It's important to have a great user experience because as we are trying to build worldwide adoption of cryptocurrencies and blockchain technology. We have to understand that not everyone is technically acute or has a deep knowledge of the space. There are a great number of individuals, companies, and businesses that see the ultimate benefit of incorporating these factors but lack the basic understanding or procedural guidance on knowledge implementing the protocols. PHANTOM has been designed to not only give advance users a private smart contract platform, but a simple user interface to create adoption of its technology to the average new user. The PHANTOM client, whether as an application or web based interface, gives the user a seamless portal of tools such as per-designed private smart contracts to meet a wide array of use cases. They are able to view private contracts through a built-in viewer within the application as well to make the user experience simple. The PHANTOM client will also host a decentralized peer-to-peer exchange marketplace designed for users to transact with one-another without the need of a centralized third party handling the transaction while running the transactional data through the private two-tier network. The focus on a private decentralized network will give the ultimate experience to the user to execute functions are that complex in design yet with a simple interface while trusting an on-chain protocol. With the use of relayers we- will create a high-throughput trading platform designed with on-chain settlement.

Accessing Smart Bridges will allow cross-chain interoperability and communication so that users can interact with other blockchains and still utilize the PHANTOM protocol to keep transactional data private that bases through the blockchain. These Private Bridges gives the ability of data to be used on other PHANTOM based standalone blockchains but remain private.

3. PHANTOM Hard Fork

A hard fork is when a protocol changes its code for the purpose of scaling, implementing, or fixing an issue. [12] Creating a hard fork will allow the launch of a custom protocol that will operate the PHANTOM blockchain. PHANTOM's network launch consists of a two part hard fork from Ethereum's Centra ERC20 token and ARK. Centra's ERC20 Platform was designed as a utility token to financial services tools utilizing cryptocurrencies. ARK has been designed to create a governed decentralized system utilizing a delegated proof-of-stake consensus to make blockchains interoperable and scalable with ease. The economic realities that are causing this hard fork has to do with the Centra project being unstable at the moment due to the challenges the platform is facing and has contributed code from Centrachain over to PHANTOM.

The hard fork will be designed to eliminate any challenges the community is facing due to the centralization of the original company. By allowing a decentralized network to be formed we are creating a community driven ecosystem that is governed by the users. The Phantom Foundation will only be giving technical support to protocol and assisting the ecosystem in adopting the platform and utilizing the currency conversion engine for dedicated products. Users do not have to do anything with their ARK or CTR tokens. We are contacting exchanges to be able to either enable trading, withdrawals, or make an announcement on the status of the fork. Users who have tokens in private wallets will not have to perform any changes as well. Once the network's mainnet is launched we will publish a detailed guide on how to claim your XPH.

We are first restoring balances on a previous block due to events that happened to the CTR Token. This will allow a restoration of those balances to continue to move the project forward. Based on the CTR balances from block 5363360 (April 1st) from the Ethereum blockchain those CTR Token balances from block 5363360 will be credited a 4:1 XPH/CTR ratio. There will be a snapshot of Ethereum's CTR balances and ARK Balances on August 30th, 2018 at 00:00 UTC (Block determined soon). Those users will receive a 2:1 Balance of XPH to CTR and ARK holders will receive a 3:1 XPH to ARK balances as well. For purposes of understanding the supply of XPH there will be approximately 1,007,554,954 XPH on our genesis block. 600,000,000 XPH are being distributed to CTR addresses, ~407,554,954 to ARK addresses.

4. Consensus & Protocol

PHANTOM uses Ark[13] for the point of governance, consensus, interoperability, and scalability while running a two-tier system to enable the use of Private Smart Contracts with a private smart bridge. Unlike blockchains that rely on Proof of Stake where they need all coin holders to secure the network, PHANTOM will use Ark's Delegated Proof of Stake model. The top 51 delegates whom are voted in by the network are responsible for up keeping the network. They will confirm blocks and receive XPH rewards and transaction fees. For every 1 XPH, it will equal one vote in the network for delegates, which effectively contributes their own XPH quantity to that delegate. The voter will then also receive a portion of the validation that occurs in accordance to their balances contributed. This allows the benefit of a PoS with the governance of the delegates. By effectively putting this into action, it makes achieving a 51% attack much more difficult. In a standard proof of stake model if one user could purchase 51% of the coins they would be able to authorize invalid transactions. However, in the PHANTOM network even if one delegate manages to get 51% of XPH supply he would only be one of the 51 delegates which can vote on a change to remove them to maintain the network. This allows a more decentralized ecosystem to take place. By governing the model this way any bad actors that are required to stake their coins in the network will lose their coins if malicious activity is detected. By having this provision, it creates a serious economic disincentive. By allowing 51 delegates we also give the system a broader reach for users to be able to participate within the network.

Users running the Phantom Core node that wish to become a delegate within the network must first register their account with the PHANTOM protocol. To enable this function the user must deposit 250 XPH per delegate they wish to register. PHANTOM will use a 1 XPH = 1 vote mechanism and the weight of that person's wallet will determine the percentage split. For example, if a user votes for two separate delegates than there is an even 50% split weight between the two delegates. When the election cycle is completed the 51 nodes with the highest number of votes are eligible to produce blocks within the PHANTOM network.

The network will be able to transact on custom fees which will be set by the delegates to determine a minimum fee required to produce a block. It will be the sole duty of the delegates to adjust fees in the same way that Bitcoin miners do currently [6]. Enabling Private Smart Contracts comes at a higher computational cost which will transcribe to a higher fee per size in bytes. The consistency of the network will allow for 8 second block times with a capability of 150 transactions per block. The inflation rate will be set to 5.5% with .25% decreasing every year until we reach a 3% inflation rate. The benefit of this is that other blockchains deploying using PHANTOM will have their own network which won't cloud or clog any of the interoperable blockchains. The block reward will be distributed based on the distribution schedule hard coded into the protocol. 90% goes to Delegates and 10% goes to the treasury pool where delegates can vote on budget allocation for the network. Additional features that are being implemented into the PHANTOM blockchain are the use of multi-signatures that will allow multiple private keys to enable a transaction and multi-payments to help batch transactions to help with reduced fees in the network such as for exchanges. These features are being forked from ARK 2.0 and will be implemented into PHANTOM on launch.

5. Private Smart Contracts

Blockchain has led to the ability to create protocols that help the transfer of data and value through global consensus in a trustless ledger. The fact that it allows us to operate in a system that we believe is trustless we need to however trust all the nodes in the network. Privacy is a huge gap, so we have designed a protocol where we can reach consensus and transact privately to execute a series of predefined agreements in a smart contract.

Now what if the two parties want to do a trust less transaction that has predefined parameters and get the benefit of blockchain but keep their transactions private? The PHANTOM protocol enables that the contract remains public to the nodes to verify its validity within the network but the transactions be encrypted that it's only viewable to the parties involved with a view key. The purpose of PHANTOM is to make these transactions private. When a business or corporation wants to do a transaction via smart contract and they look to Ethereum to do it, they essentially hit a wall when they want to maintain the privacy that they need. If you look at centralized applications that do private business such as Facebook, Banks, Lenders, Apple etc., would they make their databases public? No, they value their clients' privacy and that is one element that is important in any application business model dealing with another party. Using blockchains have brought immerse value into commerce based transactions and are solving a wide array of use cases but we are missing a big part in solving the privacy issues that go along with a public ledger.

To ensure that consensus is still met and that the network is decentralized nodes will still verify the contract and run the code that processes the transaction. However, creating this protocol also makes it so when a Private Smart Contract is deployed the nodes themselves cannot see the encrypted transaction data.

5.1How Phantom Can Solve Problems?

For example, we have tons of Blockchain Based Data Marketplaces now that have emerged to create a decentralized marketplace. However, the reason why they have not been successful is because once the information is sold and transferred it essentially becomes useless and can be resold time and time again as it is now public data. By utilizing PHANTOM, the protocol is designed to allow nodes to verify the existence and validity of these smart contracts that operate decentralized applications but transmit the transactional inputs and outputs in an encrypted fashion where only the peer to peer user can view it with a secret view key.

Now imagine all of the companies running Decentralized Applications on identity based ideas such as Civic. The concept makes sense where we are utilizing an unforgeable ledger to identify individuals and the respective records that go along with it. However how that data is stored in the blockchain is public and takes away the privacy and security of the individuals identity. Running a PHANTOM protocol decentralized application would allow the data transacted through this smart contract to verify the identity remain encrypted so that it hides sensitive information but utilizes the blockchain to validate their identities.

5.2How does a Node perform its duties?

Delegates are responsible for governing and validating the Private Smart Contracts. These nodes are responsible to store a one-time deposit in XPH that manages the validity of the contract. If a node cheats while computing the Private Smart Contract, then other nodes in the network can dispute this transaction automatically and execute an arbitration process to determine whether or not the node was being honest. The node then will loose and be penalized if the computation is proven dishonest which gives the nodes a disincentive to act malicious. This allows the system to be governed and truthful and creates a de-incentivized plan for malicious nodes.

6. Encrypted Transactions Through Private Smart Contracts

When data is actually transacted through these private smart contracts the information is essentially split between different delegates and they compute functions together without leaking any information through other nodes. Therefore, no single party except the sender and recipient would know the transactional data and the data within these validating delegates is meaningless. Every full node must submit a security deposit within the contract to ensure these transactions are being validated and transmitted properly. Running these transactions on a delegated proof-of- stake network ensures that the transaction is performed at an optimal rate of speed as well in comparison to a standard proof-of-work blockchain. We have seen Enigma's secret contract that operates through their network [14] but these protocols are all off-chain and require the trust of a third-party system running your computations. PHANTOM, with the help of Smart Bridges, allows interoperability of private smart contracts while remaining on-chain and meeting optimal transaction output speed. This feature is already built into the protocol and as other Blockchains deploy as a standalone service they will have the PHANTOM privacy protocol built into it. Users who are using PHANTOM as a stand-alone blockchain will benefit of being able to use these private smart contracts within the network and all running on the blockchain without the data having to be integrated to a third-party protocol.

As we move into the era where companies, governments, and even countries [8] are beginning to make the use of blockchains, we need to make sure we protect the integrity of private and sensitive data. For example, PHANTOM will allow a large institution to build a decentralized application through a smart contract and be able to plug sensitive data like internal numbers, social security numbers, and more without anyone being able to see this data except the intended parties while maintaining a distributed and decentralized platform. Using this as a commercial platform will allow other businesses to deploy a ready-made blockchain using ARK's technology and PHANTOM's privacy protocol and there is huge potential for credit, finance, health, and identity businesses to use this technology.

7. Private Smart Bridge

Smart Bridge Technology is a means of connecting blockchains designed by Ark. In order to do this, a snippet of code needs to be embedded in the target blockchain, Ark calls this an Encoded Listener.[15] The encoded listener is very easy to deploy on any blockchain and the AFT is making themselves available to help implement it.

Private Smart Bridge allows users to trigger events on compatible blockchains (those who have added the Encoded Listener to their core code or deployed a standalone PHANTOM blockchain). Using the XPH token, you can send transactions and trigger actions on any blockchain but allow the PHANTOM protocol to relay those transactions privately. Because Ark can be bridged with any blockchain and if you factor in the use of privacy within this technology utilizing the PHANTOM protocol the use cases are endless. Let's say you want to issue a record entry on the Factom (FCT) blockchain (Factom is a platform for data storage and record- keeping). Provided that the FCT blockchain is compatible with Smart Bridge, you would simply open your Ark wallet, navigate to the Smart Bridge tab, enter the correct information and instructions for the FCT blockchain, then click send and you're done. The FCT blockchain will receive and process your transaction accordingly. Now we take that one step further and implement a second layer within the current protocol so that the actions happen on chain and are already pre- programmed in the listeners. This will essentially allow the cross-chain interoperability of blockchains with the use of submitting encrypted data so that the parties sending and receiving the data remain private.

You may be wondering why you would even need a Smart Bridge as it seems as though it's just a "middle-man." The point of the Smart Bridge is to be a hub for all your blockchain needs. If a Smart Bridge didn't exist, the FCT entry we just walked through would require you to buy FCT tokens to complete. With a Smart Bridge, you only need to own the native token to make the transaction and you never need to leave the platform while being able to utilize this transaction privately. Imagine if all (or at least a substantial number) of blockchains were Smart Bridged together. The actions you could carry out via your wallet would be potentially endless. Whether you want to instantly convert XPH to BTC or unlock your front door, or change your thermostat, Smart Bridges could allow you to connect to the Internet of Things (IOT) all from the wallet interface. Private Smart Bridges allows you to do everything mentioned above but keep the transactional portion of the data private. When companies and business launch a PHANTOM based blockchain in the future these listeners are already pre-coded in to make a network of interoperable blockchains all possible from inception. These blockchains will have the capability to use Private Smart Bridges to with a wide array of use case such as the ability to share sensitive data such as health care records from one blockchain to another, execute a series of data transfers for private institutional companies, enable the transfer of value and functions while maintaining anonymity, and more.

8. Conclusion

The PHANTOM blockchain project has been developed to bring privacy use cases to life by utilizing a community to drive the project. The decentralization of its protocol allows for the operators to control the destiny of the system. By giving power to the people we are also giving them a network to help grow the system to bring economic growth and awareness to the project. Having an interoperable blockchain opens doors for those who want to customize their project and use a privacy based module to interact with others in the ecosystem. PHANTOM gives the power back to the people.

References

1. Edward Snowden, Leaks exposed US spy program, 2014, https://www.bbc.com/news/world-us-canada-23123964
2. Satoshi Nakamato, Bitcoin White Paper, 2007, https://bitcoin.org/whitepaper.pdf
3. Top 5 Privacy Based Cryptocurrencies, 2018, https://itsblockchain.com/5-privacy-cryptocurrencies/
4. Gavin Wood, Ethereum Yellow Paper, 2014, http://gavwood.com/paper.pdf
5. Using Blockchain For Public Data, 2018, https://www.iotforall.com/blockchain-applications-using-blockchain-public-data/
6. Ethereum Road Map, 2018, https://github.com/ethereum/wiki/wiki/Releases
7. Ethereum ERC20 Standard, 2016, https://theethereum.wiki/w/index.php/ERC20_Token_Standard
8. Privacy on the Blockchain, 2017, https://hackernoon.com/privacy-on-the-blockchain-7549b50160ec
9. ARK Ecosystem, 2017, https://ark.io
10. What is an ARK Smart Bridge, and how does it work?, 2017, https://blog.ark.io/what-is-the-ark smartbridge-and-how-does-it-work-1dd7fb1e17a0
11. Smart Bridge Technology, 2016, https://blog.ark.io/smartbridge-technology-by-ark-ab3e97a081db
12. What is hard fork?, 2017, https://www.investopedia.com/terms/h/hard-fork.asp
13. Ark White paper, 2017, https://ark.io/Whitepaper.pdf
14. Engima, 2017, https://enigma.co/enigma_full.pdf
15. ARK Authentication Listeners, 2018, https://medium.com/@arkaces/aces-completes-ark-authentication-listeners-for-ark-bitcoin-ethereum-and-litecoin-ff98c1c792cf