DeepOnion

DeepOnion White Paper

DEEPONION TECHNICAL NOTES

PRIVACY IS FREEDOM

Prepared By :
Jimmybob

REVISION 1.0A

*Deep*Onion White Paper

DeepOnion Core Team: **Monocolor**, **Deeper** & **Jimmybob** (Lead Author)

Abstract—This white paper examines the vision of DeepOnion and describes the underlying proprietary blockchain innovations that underpin this new privacy-centric cryptocurrency. Firstly, we define the goals of the project by conducting a thorough assessment of the current cryptocurrency ecosystem. We identify flaws within the current system and present how DeepOnion seeks to remedy these with new technological implementations. Secondly, we introduce our core technologies and provide a detailed explanation as to their rationale, technical specification, implementation, testing and deployment. Finally, we outline our vision for future improvements to the DeepOnion project providing a clear path to success in creating a secure, private and anonymous payment ecosystem.

Index Terms—Anonymity, Privacy, Cryptocurrency, DeepSend, DeepVault, Smart Contracts, VoteCentral, TOR.

1 Introduction

DEEPONION is a hybrid cryptocurrency that implements proof of stake (PoS) and the x13 proof of work (PoW) algorithm. DeepOnion implements the TOR protocol and is natively integrated within the TOR[2] (The Onion Router) network ensuring that all peer-to-peer connections are secure and anonymous. DeepOnion's primary purpose is to protect an individual's identity and privacy by creating an anonymous, secure, scalable, instantaneous and untraceable payment platform.

DeepOnion promotes privacy and anonymity for cryptocurrency users by reducing the likelihood of identification by legal and illegal entities through the incorporation of industry-leading cryptography and anonymity-centric networking protocols. DeepOnion will implement innovate blockchain technologies, such as DeepSend (our hidden payment technology), to obfuscate transactions, making it impossible to trace coin movement throughout the DeepOnion network. This provides a secure, anonymous platform operating over a secure, anonymous network in which users can transfer their wealth, free from observation and scrutiny by the authorities and malicious attackers.

*Deep***Onion**
December 1, 2017

1.1 DeepOnion's vision for the future

DeepOnion strives to become the premier privacy-centric cryptocurrency by improving the current state-of-the-art and introducing novel blockchain technologies. We incorporate the latest privacy standards into our technology stack, such as the inclusion of the latest TOR protocol to ensure that our community members remain secure and anonymous in all aspects of their finances. We further this by adding voting mechanisms such as VoteCentral to allow anonymous, democratic representation of DeepOnion's future development.

We believe that privacy is an inherent right and nobody should have their identity or finances scrutinized by Government entities, Financial Authorities or any other group or individual. Our mission is to create a 100% anonymous cryptocurrency that fulfils the requirements of a modern financial world whilst ensuring that the privacy and anonymity of its users remains intact. We facilitate this through the inclusion of blockchain technology running on the DeepOnion network. DeepOnion is an evolving project that is under constant development in an effort to meet the changing demands on security, privacy and technology and to remain at the leading edge of cryptocurrency advancement.

Most importantly, DeepOnion is a community; a family with a common belief in online privacy and financial obfuscation. A core community is a critical component to the success of the DeepOnion project and we pride ourselves on the many thousands of individuals that already support and promote us in such a short space of time. Together we are stronger, together we are DeepOnion.

2 Current problems in cryptocurrency

Bitcoin (BTC) is currently the dominant cryptocurrency with a market cap and market share of $598B and 37.6% respectively, despite its inherent flaws. To argue this point, it is necessary to elaborate on what BTC lacks and in turn, how DeepOnion will solve these problems.

2.1 Privacy and Anonymity

BTC [1] is built upon a publicly available, SHA-256 bit encrypted, immutable blockchain that is distributed over

• *This white paper is authored by Jimmybob with significant contributions from the aforementioned Deeper & Monocolor, as well as input from members of the wider DeepOnion team.*
E-mail: monocolor, deeper @deeponion.org

Manuscript drafted Oct-Dec 2017; released December 31, 2017.

a decentralised network supported by miners and wallet users. As blockchains are fundamentally immutable, once a wallet address is tied to a human identity, perhaps through a crypto exchange or commercial vendor, it is irrevocably compromised with respect to privacy, and that user's anonymity can never be regained without losing their remaining BTC tied to that address and generating of a new one. This would be the equivalent of having a public record of your bank statement showing all transactions that have transpired that is available for the entire World to see.

An empirical demonstration of this phenomena is witnessed when one considers exchanging BTC into FIAT via an online exchange (and vice versa). A typical scenario can be conceptualised as:

1) A user creates an account with the exchange and registers their personal details to facilitate the exchange of currency
2) A BTC address is generated by exchange and linked to your personal identity
3) The user send funds from their anonymous BTC wallet (or FIAT bank account) to their identity verified exchange wallet
4) The user performs a trade

The unfortunate outcome of the above process is that your once anonymous BTC address is now irrevocably linked to your identity. This means that the exchange is able to verify exactly how many BTC you have in both addresses (your once anonymous BTC address and your newly created one) and furthermore, to whom you are sending and receiving BTC. Alarmingly, if the exchange is required to share its customers' details to law enforcement agencies or Government bodies, they too now know your identity and how many BTC you posses in your wallet and the addresses of those you have interacted with.

An empirical demonstration of this ability to track the blockchain is visualised through the recent Wannacry ransomware [10] outbreak that infected millions of computer systems throughout the world. The ransom required to decrypt an infected machine's files was requested in BTC and the wallet address was therefore made public, thus available for tracking as well. In the following months, it became increasingly difficult for the group responsible to exchange their BTC for FIAT as every time the BTC moved to another wallet it could be tracked within the blockchain. Whilst many may argue that this is a positive feature given that it was a criminal act, consider the following perfectly legal scenario. Imagine a negotiating position during a tender agreement. If a competitor was able to track your financial investments by obtaining a list of your suppliers and contractors through blockchain exploration, this would provide valuable insight into your finances and undermine your negotiating position. This could lead to outbidding, corporate takeover as well as a full disclosure of all previous investments and business relations. This would be catastrophic for most businesses and probably one of the key reasons preventing BTC not being adopted by major institutions where privacy is a fundamental principle in financial operations (something that is actually mandated in numerous jurisdictions).

It is clear, therefore, that the level of privacy that BTC affords to its users is wholly inadequate for mass adoption. Therefore, it is glaringly obvious that the often quoted "anonymous" nature of BTC is indeed a fallacy.

2.1.1 Anonymity

Anonymity is another area of weakness for BTC with node traffic being sent in an unencrypted fashion. BTC's peer addresses are clearly visible IP presenting a prime opportunity for targeted attacks and consequently network interruption. This information is trivially obtained through the 'getpeerinfo' command in any of the freely available BTC wallets. Not only is it unsecure to involuntarily disclose the public IP address of your computer wallet without adequate perimeter defences (Adaptive Security Appliances etc), it is considered bad practice. Potential risks include the ability to be able to link a user's wallet address to its IP, further disclosing the identity of the coin holder and possibly resulting in a more sophisticated, intelligence-based attack. Thus, protecting the wallet client's IP address is an imperative action in protecting your identity and safe-guarding your financial assets. These risks are specifically mitigated by DeepOnion's implementation of anonymous TOR IP addresses.

2.2 Scalability and Speed

BTC requires that all nodes on the network cryptographically verify all previous blocks within the blockchain. This requires not only significant computing power and storage space, owing to the size of the blockchain (due to the age of BTC and the number of transactions), but also a significant amount of time to process the entire chain. As BTC relies solely on SHA-256 based PoW to process blocks and mint new coins, there is a limit as to the speed at which transactions can take place, proportionate to the current difficulty and set by design. At present, the confirmation time of a single block is 350 minutes with a high degree of variability. As most services require a minimum of 6 confirmations in order to verify, it many take up to 35 hours to send and receive a payment. This is hardly a payment system fit for the modern world!

3 DeepOnion's Vision

DeepOnion solves many of these problems by integrating a myriad of technologies into the core stack. Firstly, the entire network operates over the TOR network (see 6.1) making it extremely difficult to ascertain a user's identity without the ability to compromise large segments of the TOR network, a process that can be further hampered by the utilisation of Virtual Private Networking (VPN) solutions. This means that it is effectively

impossible to determine where a DeepOnion user is geo-located. BTC on the other hand does not encrypt its traffic, the specific rationale behind proposing BIP 151, thus enabling packet snooping to determine that an IP address is connected to the BTC network. Not only could this have legal ramifications (if BTC is illegal in your jurisdiction), but it also discloses that you are using BTC and who you are connecting to, something that you may wish to keep private and not disclose.

DeepOnion will provide security at multiple levels by adopting several industry-leading standards from the field of cryptography and network security. The following diagram depicts our multi-layered approach to security and anonymity:

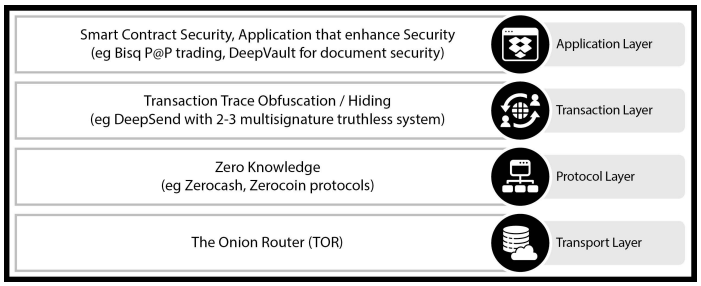

Fig. 1. DeepOnion's Multi-layered Security Model

At the transport layer we integrate the TOR protocol to secure and anonymise network traffic between nodes. In our roadmap, we indicate the addition of zero knowledge proofs [11] (protocol layer), which will obfuscate the origins of ONION transactions to all but the sender but provide sufficient, non-sensitive evidence that the transaction did occur. Transaction traces will be further hidden by implementing our DeepSend technology, which is a completely trust-less system based on multi-signatures [12]. The application layer provides the final stage of security and anonymity by adopting services such decentralised exchanges, marketplaces and other services that only operate in a secure, anonymous, decentralized and cryptographically verified fashion (details to be confirmed at a later date).

3.1 DeepOnion Roadmap

The DeepOnion roadmap (Fig.2) provides a high level overview of upcoming features within the project and their estimated implementation period. Whilst we endeavour to meet these deadlines, it is not uncommon for a project of this magnitude and scope to slip. We have developed contingency plans to mitigate this as effectively as possible and will hire additional developers as and when required. In any event, all delays will be publicly disclosed.

4 DeepOnion Features

The following section details a high level overview of DeepOnion's features before providing a more thorough in depth analysis in section 6. We introduce DeepOnion's

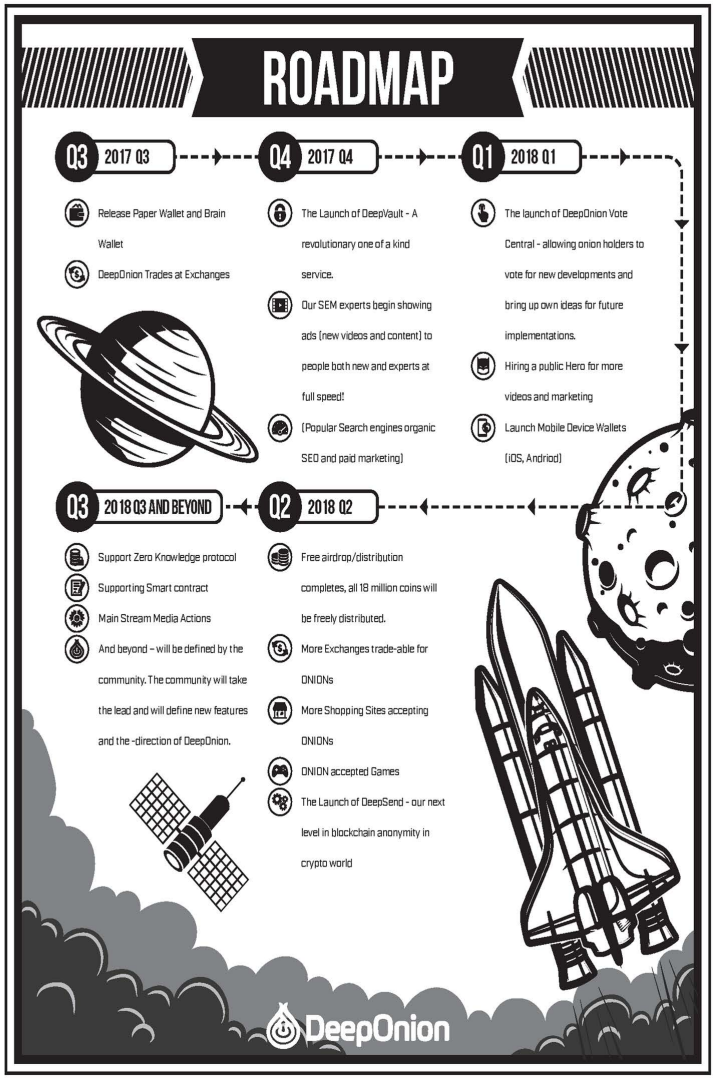

Fig. 2. The DeepOnion roadmap

coin specification, its fair distribution process, along with details regarding the formulation and support tools for our community.

4.1 Specification

DeepOnion is a PoS, PoW cryptocurrency with an emission model of 25 million ONION over 10 years. More specifically, the specification is as follows:

- 5 confirmations per transaction
- 50 confirmations per minted block
- 18 million ONION (90%) will be pre-mined at the genesis block and will be distributed FREELY to the community via airdrop
- 2 million ONION will be mineable by the public
- Connection port: 17570 - RPC Port: 18580

PoW:

- x13 algorithm

- 240s block target
- Difficulty retarget each block
- Initial payout will be 8 ONION per block
- PoW payout will be halved each year until it reaches 1 ONION where it will remain

PoS:

- 60s block target
- Difficulty retarget each block
- PoS interest will be variable per year: 1st year 10%. 2nd year: 5% and subsequent years 1%
- Minimum holding time before PoS generation is 24 hours
- Maximum allowed accumulated coin age is 30 days

4.1.1 x13 Algorithm

As its name suggests, x13 uses 13 rounds of hashing with 13 different hash-functions (including notable names such as blake, bmw, groestl, jh, keccak, skein, luffa, cube-hash, etc.). This makes it one of most secure algorithms in modern cryptography. The x13 algorithm is flexible allowing a selection of hash functions to be selected. This is beneficial as new algorithms can be adopted in light of collisions [13] being discovered in a given algorithm. By its very nature, 13 hashing functions is inherently more secure than the traditional single (SHA-256) employed by BTC.

4.1.2 Emission Model

The emission specification for DeepOnion is as follows:

- PoW 240 sec block target, meaning 15 blocks per hour, or 360 blocks per day
- Each block initially comprises of 8 ONION
  - this payout will halve each year, so the number of minable PoW coins will be:
  - 365 * 360 * 8 * (1 + 1/2 + 1/4 + 1/8 + ...) = **2,102,400**
- Therefore the total number of PoW coins will be **20,102,400** ONION (including 18 million pre-mined at block 1).

PoS generation occurs at 10% during the first year, 5% during the second year, and 1% in all subsequent years. It is estimated that over the space of 10 years, the total generated ONION will be approximately **25 million**.

4.1.3 Network Model

The DeepOnion network operates over the TOR network, providing a highly secure, anonymous method of transaction. DeepOnion clients communicate using TOR addresses, such as bb3ebyhgfkj3jzfd.onion. Onion addresses are self-authenticating addresses meaning that the address itself is a cryptographic proof of the identity of the service, thus preventing it from being spoofed by attackers. Integrating TOR into the DeepOnion technology stack provides a multitude of security advantages to our users, including:

- Added privacy for the device where your DeepOnion wallet is stored (your IP is anonymous and untraceable)
- Cryptographic verification that the network you connect to is genuine (DeepOnion over TOR)
- Freedom from oversight and network surveillance
- Inability for your client to be blocked via a specific IP address
- Enhanced communications integrity and tamper-proofing through encryption

4.2 Distribution

A fair distribution is critical for any new cryptocurrency seeking mainstream adoption. To meet this requirement, DeepOnion offer a free airdrop and additional bounty programme. [The specifics of airdrop can be found in Appendix A].

The rationale behind this method is many fold. A 40 week airdrop period promotes holding of the coin as owners that have previously received their airdrop trust the distribution model and thus wait until its completion in order to maximize their accumulation. PoS provides further rewards for those who are prepared to hold. The longevity of the campaign ensures that new users are given ample opportunity to participate and this boosts the number of members within the community that are holding ONION. A tapered emission of airdrop distribution ensures that as the number of participants grows, the number of airdropped coins is increased (see Appendix A).

A large number of ONION are held within the development and bounty wallets to be utilised when additional recruitment is necessary, either as an advertisement or extra developer venture. Bounties are readily collected as members of the community complete goals set by the development team.

Whilst initial criticism of this distribution model hypothesises the event of a Developer dumping their coins once a critical price is met, it is important to stress the manner in which this threat is mitigated.

- The Founding members of DeepOnion hold 2 million ONION, a figure whose percentage of the overall distributed ONION falls with each week's successive airdrop (week 24 at time of writing).
- Current volume is low, preventing a 'dump' scenario. This is attributed to the airdrop distribution method which promotes holding, ultimately resulting in a low number of ONION on a given exchange.
- The project is open-source (minus the currently protected DeepVault which will be released in due course). Given the size and skill set within the community it would be possible to fork with minimal disruption.
- A dump of this nature categorically defies the work ethic of the development team and the future vision for the DeepOnion ecosystem.

4.3 Community

DeepOnion's strength stems above all else from its massive community, reputation and support of its network.

There are many cryptocurrencies available that fall short of mainstream adoption due to their small user base and lacklustre promotion. We clearly understand how vital the social aspect is and from inception have always placed the community formation with the utmost importance. We have furthered this by introducing a Voting platform to ensure that our users can shape the future of the DeepOnion project.

To ensure that we fulfil this requirement we have created a plethora of social media outlets and supporting technologies. Perhaps most notable is our Official forum available at https://deeponion.org which forms the heart of our community and the platform itself boasts many features that are not present on other forum software. We are also prominent on several proprietary platforms such Twitter, Reddit & YouTube which we use in advertisements and community projects boasting a large following.

Our strategy has been extremely successful and to date we have one of the largest and most popular threads on the established BitcoinTalk.org forums. This level of exposure is highly beneficial and we will continue to purse this social outlet. Most importantly, it reflects peoples' sentiments towards the DeepOnion project and their willingness to be involved, support and participate.

4.3.1 Forums

The Official DeepOnion forums are our community hub and are used both as a social interaction platform and also to coordinate our 'call to arms' in promotional events. The official forums have witnessed exceptional growth over the past 6 months and is one the pivotal reasons behind DeepOnion's continued success.

Our forums are available at https://deeponion.org and registration is open to all. Please visit us to find out more about DeepOnion and to ask our excellent, friendly community any questions you may have. You will be amazed at the number of talented, diverse individuals we have within our community and we welcome you to join us.

5 Examination of Technologies

DeepOnion's strength lies in its multi-faceted approach to security and privacy manifested by the myriad of technologies incorporated into its blockchain and wallet. Whilst DeepOnion incorporates a number of recognised technologies witnessed in other currencies (we adopt current best practice), it also boast a number of proprietary solutions that further the state-of-the-art and offer additional privacy, anonymity and security.

In order to discuss this further it is necessary to understand the common terminologies that all blockchain cryptocurrencies share.

5.1 Blockchain

A blockchain can effectively be defined as "a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. By design, blockchains are inherently resistant to modification of the data" [3].

Utilising a blockchain in a currency is an effective solution to many problems facing existing financial systems. The blockchain provides an immutable public ledger containing all transactions that have transpired on the network in its entirety. This creates the ability to verify any transaction since the coin's inception (with obvious privacy trade-offs as described in 2.1) making conflict resolution a simple task.

5.1.1 Blockchain Scalability

As the blockchain is a continuous ledger of all transactions, it is important to understand the concept of throughput. With Bitcoin and Ethereum, their maximum throughput is 4 and 7 transactions per second respectively. This limitation is due to their blocksize (the amount of data [records of transactions] that can be stored in each fixed block size - 1MB) and block time (the average time it takes to process a block's hash and add it to the blockchain). As you may be aware, this can result in BTC transactions taking well over 24 hours to complete, a fundamental flaw in a supposedly instant payment system. DeepOnion improves this situation many fold by including PoS, larger blocksizes and faster block times. This provides a theoretical throughput of 62.5 transactions per second as detailed here:

1) The average transaction size is about 500 Bytes. The DeepOnion blocksize is 1.5MB, so each block can hold approximately 3000 transactions.
2) DeepOnion is a mixed PoW/PoS coin, PoW interval is 240 second on average, but PoS is a lot more frequent, target at 60 sec. This means our theoretical combined block time is 48 seconds (240 / 5).

To verify this, we checked last 24 hour's blocks, this is what we get:

- block 223460 occurs at Nov 25, 2017 11:59:36AM
- block 225285 occurs at Nov 26, 2017 11:59:05AM

This means:

3) we have 1825 blocks in 24 hours, which means our average block time is 47 second, which perfectly matches our designed target block time.
4) Thus, we have one block per 48 seconds, which can handle 3000 transactions. This means that DeepOnion can handle a maximum transaction rate of: 3000/48 = 62.5 tx/second.

This is almost 10x the throughput of Ethereum and proves that DeepOnion is more effective, scalable and suitable for mass adoption as a cryptocurrency.

DeepOnion's transaction speed can be further increased by the future implementation of 'lightning network' [8] technology, this could theoretically make the transaction speed the same, if not faster, than the VISA

network (approx. 56k/sec [8]). These fast speeds combined with TOR anonymity will make DeepOnion the perfect payment platform.

5.2 Cryptocurrency

A cryptocurrency (or crypto currency) is a digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets [4].

Bitcoin was the first decentralized cryptocurrency released in 2009 by Satoshi Nakamoto.

5.3 Decentralization

Decentralization is the process of distributing or dispersing functions, powers, people or things away from a central location or authority [5].

With respect to cryptocurrencies, decentralization is defined as the removal of a central processing authority (much like the aforementioned VISA). Instead, each node (typically wallet or miner) on the network independently verifies, via a processes of cryptographic hashing functions, each block within the blockchain.

The benefit of this approach is that it increases the level of security on the network and greatly reduces the reliance on trusting the payment processor. In order to compromise the network, you would have to effectively compromise 51% of the network. This is not feasible given the global distribution of nodes, different protocols and operating systems. The network also benefits by having every node able to verify new block. DeepOnion takes this a step further than BTC by introducing PoS, another form of mining and verification, and results in the necessity of having to compromise an even greater share of the network across two channels (effectively impossible).

Whilst verifying each transaction affords maximum security, it is also the reason why transactions take a considerably longer time than traditional payment methods. Technologies such as 'lightning network' are one approach to solving this scaling option but each time you take transactions off the core chain you are reducing security as the number of verifications is reduced. Exactly much security (certainty) or how many confirmations are required is a complex problem and one that is currently the focus of various projects such as BTC and Ethereum.

6 DeepOnion Innovation Technologies

Having defined the commonalities behind all cryptocurrenices in section 5, it is necessary to introduce the novel blockchain technologies that DeepOnion will implement in order to meet the changing demands in the cryptosphere and the necessity to improve privacy and anonymity beyond current efforts.

DeepOnion is cloned from Supercoin, an anonymous coin with stealth transactions facilitated by coin mixing processes. Supercoin provides a solid base from which to build and improve upon. The following sections will detail DeepOnion's novel blockchain implementations and the rationale behind their selection.

6.1 TOR

Tor is defined as a "circuit-based low-latency anonymous communication service. This second-generation Onion Routing system addresses limitations in the original design by adding perfect forward secrecy, congestion control, directory servers, integrity checking, configurable exit policies, and a practical design for location-hidden services via rendezvous points. Tor works on the real-world Internet, requires no special privileges or kernel modifications, requires little synchronization or coordination between nodes, and provides a reasonable trade-off between anonymity, usability, and efficiency" [2].

This provides the perfect platform from which to build an anonymous cryptocurrency on. At the time of writing, DeepOnion is currently upgrading to the latest 0.3 protocol to introduce the latest and most secure, anonymous features to our wallet and to protect our users. It is important to stress that all connections from the DeepOnion wallet are made over the TOR network. At no point is your public IP address exposed.

6.2 DeepSend

DeepSend is a transaction-side security feature designed to obfuscate transaction traces within the blockchain (a problem we earlier identified with BTC). This is distinctly different from our TOR integration, which secures and anonymises network traffic at the transport layer.

DeepSend comprises of a number of technologies such as:

- **Zero knowledge** technologies by Zerocash and Zerocoin: such as ZCash and ZCoin
- **CoinJoin** technologies, either with centralized mixers (such as masternodes) or random mixers (Seen in Dash and SuperCoin)
- **Ring signatures** by CryptoNote: such as Bytecoin and Monero

Each technology has both pros and cons. For example, in Zero Knowledge technologies you must burn and "mint" new, unrecognizable coins each time which requires additional space on the blockchain. DeepSend is currently planned to be a CoinJoin/Mixer technology based on trustless multi-signature technologies and thus will provide cutting edge anonymity and privacy. To conceptualize, consider the following scenario:

1) Person A wishes to pay $x to Person B
2) Instead of Person A paying it directly to Person B, thus publicly disclosing the transaction to all (currently occurring in BTC), Person A pays Person C, and Person C pays Person D, etc. Finally after n iterations, Person Z pays Person B

3) As such, all payments between Person A and Person B are guaranteed by multi-signatures, and none of the addresses linked to individuals
4) This is because Person C receives money from Person B, but pays Person D using a different and unrelated address. This makes it practically impossible (given enough iterations) to reverse trace the transaction.

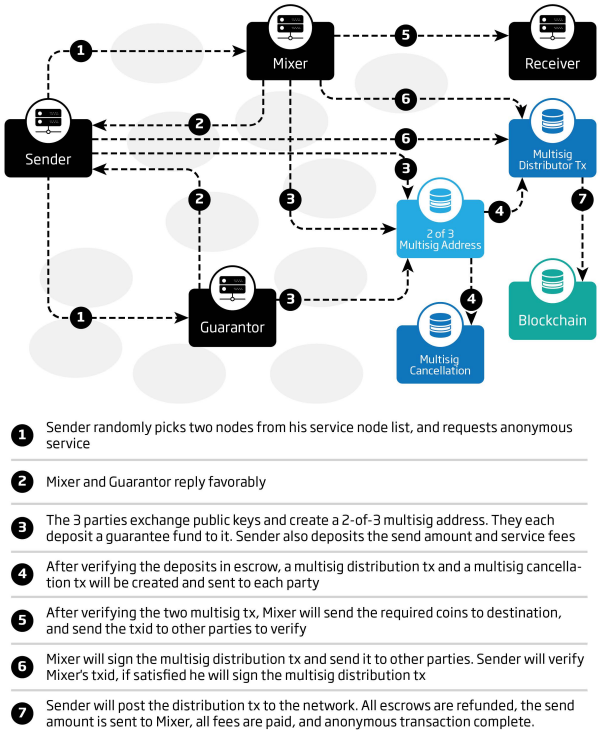

Fig. 3. DeepSend Transaction: Ofuscation through CoinJoin & Multi-signature

[9]

6.3 DeepVault

DeepVault is an immutable information store that is held within the DeepOnion blockchain. More specifically, DeepVault allows DeepOnion members to store file validation credentials (hashes of files) within the blockchain. This has obvious benefits as it allows users to verify a file's integrity over time. Therefore, if the hash of the file changes, it proves that the file has been altered or corrupted. This tool will be invaluable in checking whether your important documents are secure and have not been tampered with. Legal documents are an obvious use for this feature as it would enable a person to verify that the document, and thus content, has not been altered either maliciously, erroneously or through file corruption. Think of this as an expansion of smart contracts where conditions or integrity are validated through cryptography.

- A video demonstration of DeepVault has been kindly produced by @themonkii [6]
- A manual for those unable to view the video is also available [7]

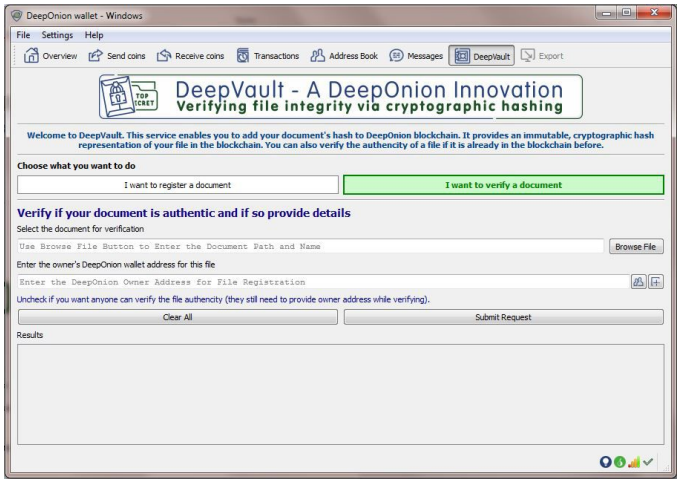

Fig. 4. DeepVault - DeepOnion wallet

DeepVault is seamlessly integrated into the DeepOnion wallet and is highly intuitive. This novel feature provides a pragmatic solution to the long held problem of simple file validation. DeepVault improves the hashing process and file verification processes by providing a number of simple to use benefits:

- The hash of the file is generated using a GUI that is embedded within the DeepOnion wallet
- The hashing process uses the secure and trusted SHA-256 algorithm
- DeepVault protects the hash of the file within an immutable blockchain. This means that the hash itself is safe from alteration
- The file verification can be locked to the user preventing others from validating the file

We think that DeepVault is an important tool in aiding our users to safeguard and protect themselves in the digital era. The ability to verify your files' integrity has innumerable benefits and can be applied almost all scenarios.

DeepVault will be expanded in Q1 2018 with the deployment of a non-wallet based solution hosted in the cloud. This will allow a web-based interface in which to secure your files. Details will be released soon.

6.4 Mobile Wallet

The DeepOnion mobile wallet will make its debut on the Android operating system early in 2018. The wallet will afford similar functionality to the desktop experience (final features to be confirmed) and will naturally operate over the TOR network, protecting your identity whilst on the move. DeepVault is an important feature of the mobile wallet allowing you to protect your documents on the fly, an important feature and a natural application for protecting your photos.

Furthermore, users will be able to view their transactions, address book, access VoteCentral and naturally send and receive ONION.

We're currently in the initial stages of hiring an iOS developer to bring the DeepOnion mobile wallet to Apple devices. Be sure to check our official forums and newsletter to keep up to date with this development.

The wallet will be branded in line with our website to promote an homogeneous user experience for our community across all platforms. User experience is an important element of our mobile wallet and will be undergoing extensive testing to ensure that the operation of the wallet feels natural to anybody, regardless of your experience of cryptocurrencies.

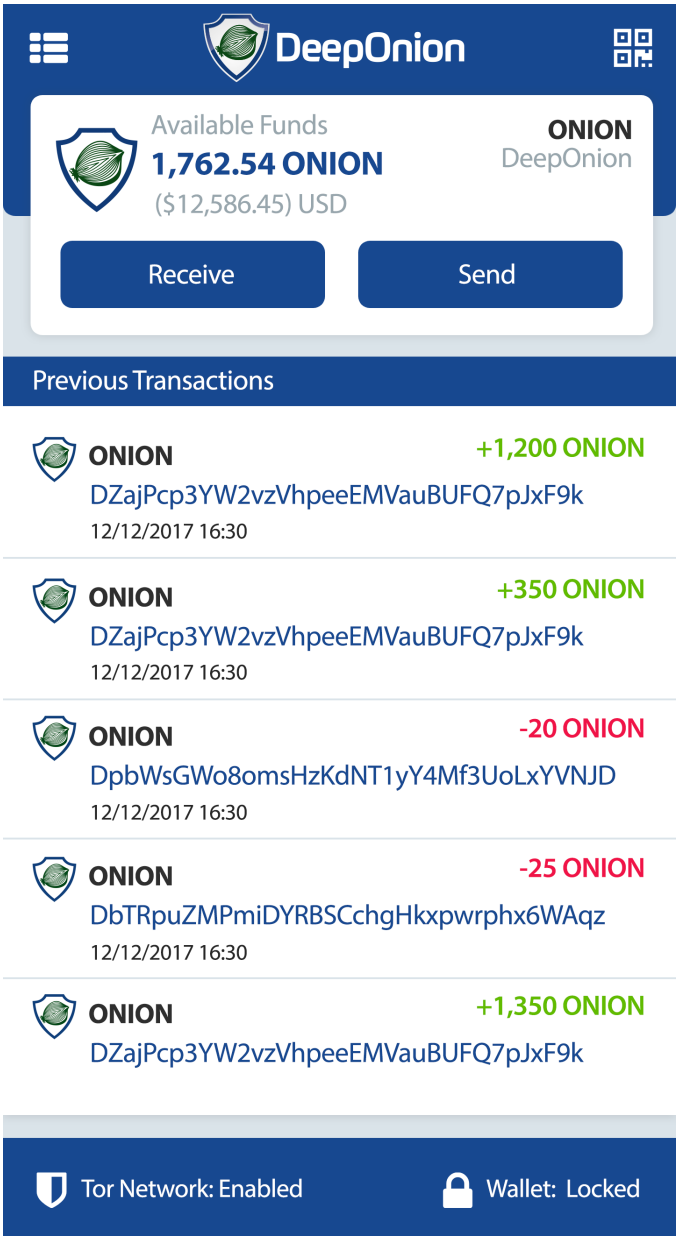

Fig. 5. DeepOnion Mobile Wallet

6.5 VoteCentral

VoteCentral is an open voting platform built upon blockchain technologies that will enable the DeepOnion community to vote on the suggested proposals and tasks submitted by community members regarding the future direction of the DeepOnion project. This platform enables DeepOnion members to have an impact on the community decisions influencing the direction and expansion of the DeepOnion project.

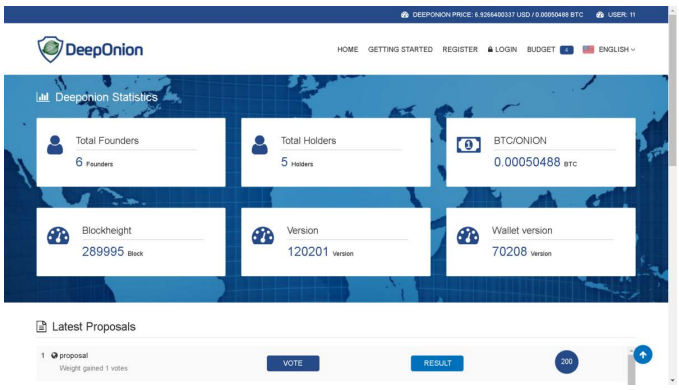

Fig. 6. VoteCentral - Landing Screen (In Alpha)

It has many parallels to existing democratic voting systems in modern politics, except it has the added benefits of blockchain technology to mitigate voting fraud. New directions or community suggestions can be registered through VoteCentral and subsequently evaluated by the Development team, airdrop founders and holders that have ONION balances above the necessary minimum within their wallet.

As we have previously mentioned in our communications, VoteCentral is a layered approach. To imagine this hierarchy, imagine 3 concentric circles:

1) The inner circle (core) consists of our dev team and initial founders.
2) Surrounding this are our airdrop founders who have the right to vote in vote central.
3) Finally, the exterior consists of long-term DeepOnion supporters, and those who have made significant contributions towards the project.

Voting is based on a member's proven contribution to the community (or status granted through long-term support). At this moment, a member's voteweight (voting power) depends on their ONION wallet balance.

VoteCentral has two phases, a centralized solution supported solely by web technologies, a future next phase will be supported by the blockchain. Wallet owners will use this software to vote on community suggested proposals and tasks based on the number of ONION held within their wallets.

During the first phase we ask that participants prove ownership of their ONION wallet by registering a signing message. We can check a member's wallet balance each day and decide that participant's voteweight accordingly with respect to suggested proposals awaiting decision by the Development team or others. Proposals will need to follow protocols and meet stan-

dards that are not yet defined but will be detailed at a later date.

The Development team, Founders, and future Holders registered VoteCentral will have the ultimate decision on which direction the project will take but each circle of members will each be able to express their sentiments.

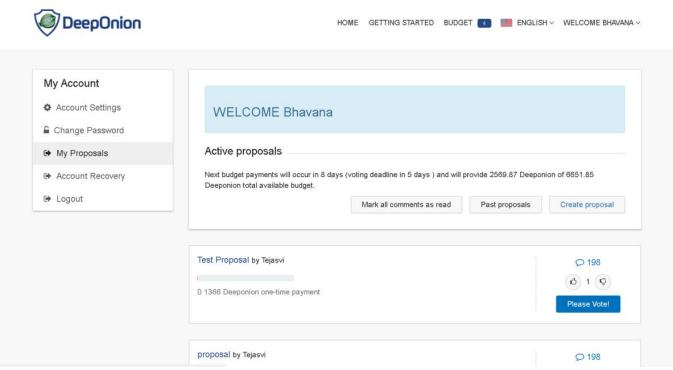

Fig. 7. Viewing and Creating Proposals - (In Alpha)

We have grand ambitions with VoteCentral and wish to establish a 'living organism' whereby we accept or reject decisions based on a process of robust analysis and evaluation supported by community sentiments and weighting in a democratic fashion. We select the best and most popular proposals/tasks from VoteCentral and use these to guide the future expansion (Domination) of the project. You can play a pivotal part in this future and you voice your opinion by proving your commitment to DeepOnion, ultimately rewarding you with an increased voting weight within the project. The stronger we build our Founding community, the better DeepOnion will become.

6.6 DeepPoints

DeepPoints is our community reward programme that enables community members to earn ONION for their contribution towards the project. Our goal is to reward members who regularly contribute meaningful posts and create promotional material for the wider community. The criteria for DeepPoints is flexible and dynamic, a model that suits both the spontaneous realm of cryptocurrenices, along with the rapid development that DeepOnion is currently experiencing. The strength of this approach stems from our ability to adapt and target our whole community towards a specific g o al or objective. This has been successful in many attempts, specifically with respect to exchange listings such as the recent KuCoin and Satoshi Exchange and will no doubt be crucial for our expansion onto the Bittrex and Binance platforms.

For our members, it is quite simple, the more official DeepOnion (Domination) tasks you complete, the more likes, threads and replies (inside of the documented rules and avoiding spam) you accrue, the more DeepPoints you will receive. Importantly, Domination tasks (those designed specifically from the dev/mod team to target a specific objective) reward 5x the standard remuneration of likes and replies.

Within our weekly airdrop, 2% - 10% of the distribution is reserved for DeepPoints rewards. This provides a real opportunity for our community to earn lucrative rewards for their participation, and it is a perfect opportunity for the DeepOnion team to reward our loyal followers.

7 The Future

2017 has been a tremendously successful year for DeepOnion. Not only are we one of the most popular forum threads on BitcoinTalk.org, but we've done that as a community in the space of 6 months. We're seeing continued strong growth of approximately 750 members per week on our forums with strong mining to support our blockchain. With the current roadmap and recent expansion of our development team, 2018 is set to be a record breaking year!

We are contacted daily by major investors, exchanges wishing to list us as well as notable crypto celebrities wishing to involve themselves within the project. It is humbling to see that all the hard work of the Development team and community is paying dividends.

It is important to stress that we will not stop until DeepOnion is the de-facto, privacy cryptocurrency adopted. Our message is spreading, our trade volume and exchange listings grow on a monthly basis and we continue to integrate new blockchain technologies. More impressively, we haven't even begun our advertising campaign as denoted in our roadmap. We're confident that a fully implemented roadmap with celebrity endorsement will surely propel DeepOnion to the forefront of crytpocurrency adoption.

So, here's to 2018, it's going to an exciting year!

- DeepSend
- DeepVault Website
- VoteCentral
- Smart Contracts
- Mobile Wallet
- Advertising campaign
- Celebrity endorsement

Appendix A
Airdrop Specification

Total Premined 18,000,000

- Airdrop Rounds 1-15: 3,200,000
- Airdrop Round 16-40: 6,800,000
  - Round 16-30: 250,000 each
  - Round 31-39: 300,000 each
  - Round 40: 350,000

In addition, to reward participation at the DeepOnion forum community, 10% of each week's airdrop will be

used for events in the DeepOnion forum. The remaining 90% will be directly airdropped as usual.

Bounty Fund: 3,000,000

Currently, the balance stands at 2,600,000 after various bounties, events, rewards and distributions. This fund is used to reward contributions such as articles, videos, significant contributions that help DeepOnion and its community, and also to support potential new merchants that choose DeepOnion.

Founders reward: 2,000,000

Development fund: 3,000,000

e.g. for smart contracts, and other new feature development. The usage of this fund will be determined by the community via VoteCentral.

ACKNOWLEDGMENTS

The DeepOnion team would like to thank our community and all those who have purchased or supported us throughout our journey so far. It is you that make this project what it is today. We have the technology and the vision but it is you who helps us distribute this into a workable ecosystem where we all benefit from anonymous, private financial transactions in a world increasingly dominated by pervasive digital espionage. Thank you and please continue to support us.

The DeepOnion team would also like to extend their gratitude to the ongoing work of their diligent Moderator team who continually excel in meeting the requirements of the project and the community (even through the festive period!).

A special thank you to @Impressive and @DogLover for the provision of graphics included within the white paper.

REFERENCES

[1] The Bitcoin Project. 2017. *Bitcoin is an innovative payment network and a new kind of money.* Available at: https://bitcoin.org Last Accessed: 31/12/17

[2] R. Dingledine, N. Mathewson & P. Syverson. 2013. *Tor: The Second-Generation Onion Router*, 2nd ed. Available at: https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf.

[3] Economist Staff *Blockchains: The great chain of being sure about things*. Available at: https://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable, 31/10/2015.

[4] A. Greenberg. 2011. *Crypto Currency*. Forbes.com. Available at: https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html. Retrieved 12 December 2017.

[5] *Definition of decentralization*. Archived 2013-01-26 at the Wayback Machine., Merriam-Webster Dictionary, accessed February 4, 2013.

[6] theMonkii. 2017. *DeepVault Tutorial Video*. Available at: https://deeponion.org/community/threads/deepvault-video-guide.3780/.

[7] Jimmybob. 2017. *DeepVault Tutorial Manual*. Available at: https://deeponion.org/community/threads/tutorial-deepvault.3868/.

[8] J. Vermeulen. 2017. *'Bitcoin and Ethereum vs VISA and PayPal'*, Available at: https://mybroadband.co.za/news/banking/206742-bitcoin-and-ethereum-vs-visa-and-paypal-transactions-per-second.html Last accessed: 28/12/17.

[9] SuperCoin. 2016 *'SuperCoin's Revival'*. Available at: https://bitcointalk.org/index.php?topic=1351548.0 Last Accessed: 28/12/17

[10] Wikipedia. 2017. *wannacry* Available at: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack Last Accessed: 01/01/18

[11] M. Green. 2014. *'Zero Knowledge Proofs: An Illustrated Primer'*. Available at: https://blog.cryptographyengineering.com/2014/11/27/zero-knowledge-proofs-illustrated-primer/ Last Accessed: 01/12/17

[12] Bitcoin Wiki. 2018. *'Multisignature'*. Available at: https://en.bitcoin.it/wiki/Multisignature Last Accessed: 01/01/18

[13] Wikipedia. 2018. *'Collision Attack'*. Available at: https://en.wikipedia.org/wiki/Collision_attack Last Accessed: 09/10/17