Obsidian Platform Whitepaper

Version 1.1

1. Vision

The inalienable right to privacy is a legal tradition found in more than 150 national constitutions worldwide. Still, this right is increasingly in peril as state and private organisations become more hungry for data and communication meta-data for sometimes legitimate but frequently illegitimate or criminal reasons.

Privacy and secrecy is always a double-edged sword and you cannot really have it both ways. The Obsidian Project aims to offer unrivalled private communication by marrying a secure messenger application with a cryptographic coin that enables a decentralised communication network. This provides resilience against attacks on the communication servers by replacing them with decentralised nodes which anyone can host, and thus receive Obsidian coins as compensation.

The decentralised secure communications network is therefore owned and operated by no single entity, but instead by thousands of humans all over the world thereby rendering attacks on hosts ineffective to the network status. Communication meta-data cannot be gathered at one central point, as it is scattered over thousands of hosts all over the world making it very hard to work out who is talking to who, even when parts of the internet are under surveillance.

The Obsidian Project thus takes the power of existing secure messaging services one step further, by fundamentally changing the architecture from a server-centric network to a decentralised network that is owned and run by its users, and financed with the Obsidian coin. The WhatsApp and Facebook mobile messenger applications alone process 60 billion messages per day. It is our dream to make each of these messages much more private than they currently are, with our Obsidian Secure Messenger line of mobile applications.

2. Technical Overview

The Obsidian Platform coalesces blockchain and secure anonymous messaging and consists therefore of two main parts:

- The Obsidian Coin (ODN)
- The Obsidian Secure Messenger (OSM)

The Obsidian Coin, currently in development, is based on the STRAT coin by Stratis, which is in turn based on Bitcoin. It will be kept in sync with the latest features from Bitcoin, including

features such as the SegWit scaling solution. Our use of the Stratis C# code base makes us more efficient and relieves us from the burden to create a state-of-the-art coin on our own.

The Obsidian Secure Messenger (OSM) is based on so far unpublished prior work of one of our developers who is leading the messaging architecture of our project. It is currently available as a working alpha version which should be available for preview in the coming weeks.

At this point, the ODN coin and the OSM messenger are not yet mature and not linked. The initial scope of this project will be the decentralization of the messenger's storage, making the messaging nodes available for hosting by anyone, providing the nodes an ODN fee per message, and offering light wallet functionality in the OSM messenger client to be able to pay for the traffic produced.

3. Technology

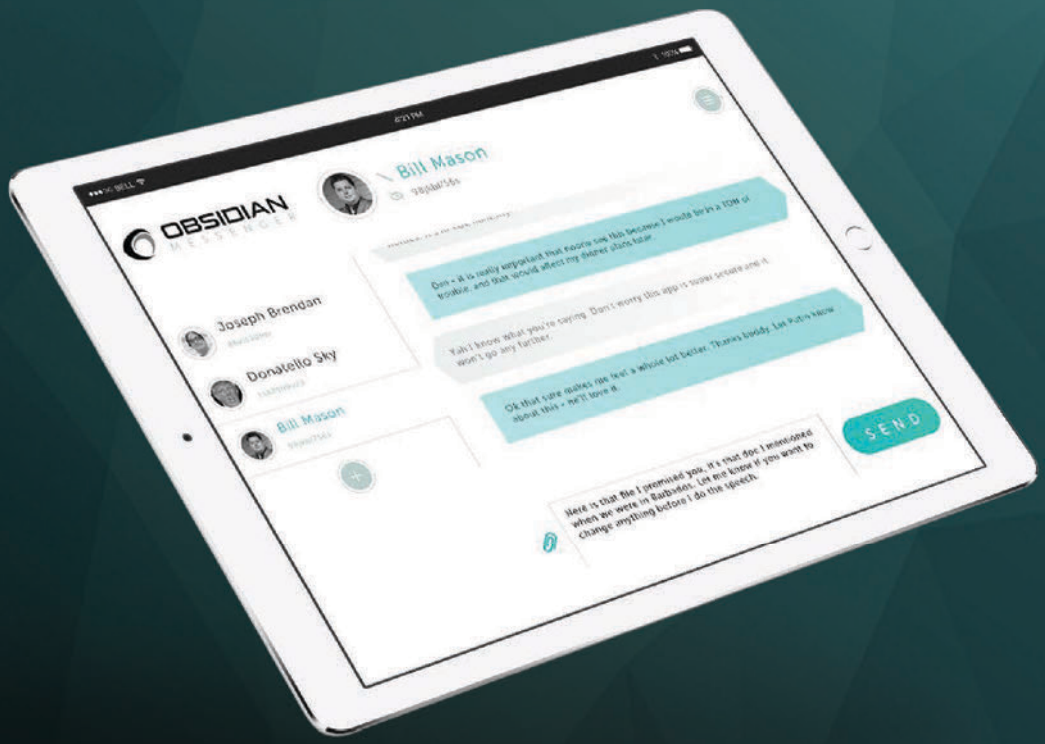
a) Obsidian Secure Messenger (OSM)

OSM is going to be a light client to the Obsidian blockchain which and a messenger app that offers end-to-end-message encryption with perfect forward secrecy (PFS) relying on Elliptic Curve Diffie-Hellmann (ECDH). Obsidian IDs are 10-digit identifiers protected with Curve25519 signing keys. OSM has no user accounts or connection to an email address or telephone number. They cannot be related to any personal data per se. For message transport, we envision a secondary parallel network to enable faster-than-blockchain message exchange within the application, including large payloads like images and files. Messages will be buffered by specialized nodes that anyone can run, earning fees in ODN. These nodes will temporarily store the end-to-end encrypted messages, and/or binary files, until the specific recipient is online to receive the payload. Messages are encrypted on origin and decrypted only when they arrive at the intended destination. The intermediate nodes cannot open these messages without brute-forcing them (256 Bit symmetric encryption). Furthermore, buffered messages are automatically dropped after a short time by the network, freeing resources. While messages will be cached on the application client's frontend in an encrypted state, with an option to remove them, they are deleted on the backend.

b) Platform Specifications

The Obsidian coin (ODN) is built on a C# codebase using sources from the NBitcoin/ NStratis project and the Stratis Bitcoin Full Node implementation. It runs under the .NET Core technologies, therefore making it developer-friendly and capable of running on various operating systems such as Windows, different versions of Linux, and more recently some Mac OS X versions.

User Interface designs for OSM mobile applications.



c) Obsidian Node Types, Master Nodes, Staking (rewards)

The fully developed Obsidian Platform will establish different node types, i.e. programs that interact with the blockchain and/or messages.

Light nodes/SPV wallets. These are simple GUI-based interfaces into the blockchain that store the minimum possible information in their hard storage in order to keep them useable and to keep their value stored. Light nodes depend on the existence of the full nodes in order to stay in synchronization with the network. A light wallet can be a self-contained app, used to send and receive payments. A OSM messenger app with payment functionality would also be an example of a light node.

Full nodes. They store the complete blockchain and protect consensus in the blockchain payment network. The requisites for a full node are enough disk space for the blockchain and an intermittent connection to the Internet in order to keep themselves up to date. They are used by the light nodes in order to enable their payment functionality. As ODN is a Proof-of-Stake coin like STRAT, the full nodes receive a reward for verifying blocks, the staking reward. The total staking reward across all nodes in the network reward is 10% per year and is distributed randomly among staking nodes, where the amount of coins owned by a 'staker' increases the probability to earn the block's reward. The net result should give holders of ODN who run a full node a 10% interest on their owned ODN coins. As the initial supply of ODN is approximately 98 million coins, it also means 9.8 million new coins are produced every year, which can be seen as inflation. Nevertheless, this is needed to make people run nodes, as this is the infrastructure needed by all stakeholders.

This model (10% staking rewards for staking-enabled full nodes) will also be, according to our planning be followed for the first 2-3 years at most-until block rewards can be reduced or eliminated in favour of a transaction/message fee based incentive model, used by more specialised 'Masternodes'.

Masternodes. In the course of development, the initial Full Nodes will see a specialization, namely on securing the blockchain and providing payment services for light clients and buffering OSM messages. Upcoming alpha versions of these more specialized nodes will be called Masternodes. E.g. messaging Masternodes should comply with the requisites of a 24/365 presence with as little downtime as possible, good performance, sufficient storage space and bandwidth. Advanced blockchain Masternodes might also have to meet a certain quality of service to be as useful as needed for mobile wallets. This is why we can announce but not further specify the conditions and requirements of Obsidian Masternodes. We need to develop and measure via careful testing first to get the parameters correctly determined. We cannot overpay or underpay or make the requirement of locked coins too high or too low because that would result in an unbalanced network and put its functionality at risk. That is, we cannot say at this time with certainty the exact number of locked-up coins an Obsidian Masternode will require and what the reward in terms of staking and/or tx/message fees will be. The current estimate from our developers of the number of coins required is 10,000 ODN, but we reserve the right to change this value before the Masternodes launch for a number of reasons: costs of running the node, responsibilities of the nodes and affordability have to be balanced to provide for a large, and ensuring a global network that is up to the demands of satisfying the needs of our platform.

4. Initial Coin Offering (ICO), ICO Pre-sale, and Distribution

The crowdsale will end when either all 58.8 million coins being offered for exchange are sold for the fixed exchange rate detailed below, or in 35 days from the start of the pre-sale. There will be an initial coin emission of 98 million ODN before the ICO. Staking rewards in year one are 10% of the initial amount of coins. We plan to reduce or remove the reward model once we have gathered additional data about the obsidian network economy.

We have fixed the exchange rate at the following amounts:

1 BTC = 21433 ODN
1 ETH = 2192 ODN

The crowdsale will be split into two parts. The pre-sale will last for a period of four weeks. During this time all participants will receive a bonus for their contribution. The bonuses will be applied to the base amount of ODN listed above and will decrease each week in the following schedule:

Week 1 = +20% bonus ODN
Week 2 = +15% bonus ODN
Week 3 = +10% bonus ODN
Week 4 = +5% bonus ODN

ICO Week = 0% bonus ODN

After the ending of the pre-sale period we will launch the ICO period within 24 hours, which will include all unsold coins from the first four weeks.

Please note that participation during the pre-sale period holds a much greater risk (and a greater reward) as Obsidian will not be as far along in it's road map, thus having less working services to showcase. We will release the wallet, reveal the OSM app, and more, to the public during the pre-sale and ICO period.

- 15% ODN (14.7 million coins) will be distributed among the members of the core team.
- 25% ODN (24.5 million coins) will be sent to multiple accounts to be used for direct OSM licensing, integration, and ongoing development. ODN from this group will also fulfill the need for "stock options" to incentivise additional teammates, (2nd tier developers, designers, etc.) marketing, and any other ongoing Obsidian costs. The use of these funds will be decided by the core team via majority vote.
- 60% ODN (58.8 million coins) will be sent to another escrow address and this part will be offered to the interested parties in the ICO and Pre-sale.

After the ICO exchanges all the ODN being offered, the the total distribution model will be as follows:

50% of the final amount raised in the ICO will be divided into two escrow accounts:

- The first one will contain 60% of this capital and it will be used for advertising, marketing, developers, dailyoperational costs of the company and similar expenses. This will also include a monthly salary for the core and 2nd tier members of the team.
- The second will contain 40% of this capital and will be kept as company assets, for ensuing compliance with all the appropriate regulatory agencies.
- The remaining 50% of the final amount raised from the ICO will be divided between the members from the core group.

The final use and distribution of the second half of the ICO final amount will always be decided by majority vote of ICO founders and is intended for funding ongoing Obsidian-related work.

5. Glossary of Technical Terms

- Blockchain - This represents a distributed ledger database, where no single copy exists. Instead of storing data in a monolithic server (or server farm) and make it available to the users through a centralized point of access, distributed ledger technology allows for a more sparse approach, where many redundant copies of the data exists all over the world. The data is stored in blocks, which are chained one to another to keep a logical and sequential registry of the operations of the network.
- .NET Core - This is a Microsoft-created platform that allows a single source code base to be shared among different operative systems. It currently supports Windows 7, 8, 8.1 and 10; Windows Server 2008 R2, 2012, 2012 R2 and 2016; RHEL Linux 7; Ubuntu 14.04, 14.10, 15.04, 15.10, 16.04 and 16.10; CentOs 7; Debian 8; Fedora 23 and 24; OpenSUSE 13.2 and 42.1; Oracle Linux 7, 7.0, 7.1 and 7.2; Linux Mint 17, 17.1, 17.2, 17.3 and 18; and OS X 10.10, 10.11 and 10.12.
- Graphical User Interface (G.U.I.) - A visual representation created by the developers in order to facilitate the manipulation of the data in the application or the presentation of the results of those manipulations.

- Wallet - An application that allows a user to have a public address where other users can send funds or where funds can be sent from in the Obsidian Platform Network. The wallet contains a private key and stores the current state of the user funds expressed in ODN units. Normally, though, the people refers to the G.U.I. as the wallet itself, but this is only a practical case. Wallets without G.U.I. can also be used but the difficulty is bigger because the commands must be manually entered by the user and the results are not easily interpretable. The wallet can also be stored as a paper copy of the master private key, so it can be rebuilt later in a different machine without losing value.

- Cold wallet - This is a way to store the essential information that allows a wallet to be recreated in software form at a later time, while at the same time avoiding having it available (and hackable) through the Internet. When you create a paper wallet, you essentially make a special copy of the wallet main values (private keys) so you can delete the file physically from the computer. Doing this still allows to receive funds (you just need to send people a copy of your address or public key for that) but you cannot use/spend those funds until you activate the wallet again in a node

- Node - A node is a wallet that also is connected to the internet. There can be different types of wallets and nodes, but they're internally equivalent.

- Initial Coin Offering (ICO) - This is a process started by the coin creators in order to make an initial distribution of one part of the available total amount among the interested parties. The contributors to the ICO campaign will receive a certain number of coins proportional to their contribution in BTC or ETH.