Hugin Messenger Whitepaper

Introduction

Hugin Messenger is a decentralized private messenger and social network with native cryptocurrency payments. WIth it you can engage in secure communications and make untraceable transactions, all without any trusted parties.

There are many private messaging services on the market today, but how private they really are is a point of debate, and often you have to take their promises at face value. Due to parts of their system being closed source, or them having opaque distribution lines, like with Google Play or the Apple App Store[1] you have to trust the developer's competence and intentions. In addition, centralized systems such as Signal, WhatsApp, Facebook Messenger etc are dependent on a specific company's servers and they can become subjected to coercion by third parties, which could lead to shutdowns, forced decryption of private messages, censorship, as well as abuse of power.

Centralized server structures, even if distributed, can fall victim to censorship by authoritarian regimes that shun freedom of speech, such as the case where Signal was censored in Iran, leading Signal to obfuscate their server's origin with the Amazon owned domain name Souq.com. Amazon responded with threats to take down their services at AWS, which could have lead to serious outages, or at worst putting a halt to the network[2].

To build a private messaging service that evades these potential issues altogether, the entire infrastructure for transmission, storage and client-side applications must be based on open source and decentralized technology.

By being decentralized it is possible to protect the network from being censored, taken offline, or somehow being made unavailable, simply because there is no single point of failure - you would have to shut down every node in the network to effectively shut the network down, and even then, new nodes could join the network at any time.

Decentralization also lends another important prerequisite for privacy, which is permissionless operation. In traditional centralized systems, a central authority controls permissions, perhaps forcing you to give up personal information to use the network. In a decentralized system, there is no such authority. Anyone can interact with the network at any time, without limitations other than those - in Hugin's case - consensus rules that govern the network, and those are always the same for all users.

Another positive feature of decentralization is that it can make certain operations a lot less costly, and in turn more scalable. In Hugin Messenger, for example, you can make *true* peer-2-peer calls, where the data is only travelling between you, and your recipient. In a centralized system, that call would be relayed through a centralized server, costing the

[1] https://drewdevault.com/2018/08/08/Signal.html
[2] https://signal.org/blog/looking-back-on-the-front/

centralized entity valuable resources, in turn causing an incentive for it to profit off of the user's interactions with their service. It is feasible that such calls are transcribed, analyzed, and hopefully anonymized, before being sold as data for profit. Hugin is immune to this race to make more profit, as server cost's increase due to user base growth and data volume. This is achieved simply because the data is stored in the peer-2-peer network, the bulk of it only between the affected parties - such as in calls, file sharing and more.

By being open source, users and experts can combine efforts to scrutinize the source code, making sure it's safe and legitimate - a process that has been shown to create the most robust and reliable systems over the decades[3].

Hugin Messenger also lets you seamlessly send value transactions in combination with messages on the same protocol, without needless fragmentation or complexity - in other words; Hugin was born to be a combined messaging service and a tool for transacting money that puts privacy first.

Features

Private messaging

Hugin Messenger is a private messenger that uses military grade encryption to secure messages that are transmitted through the kryptokrona cryptocurrency peer-2-peer network.

With the high security encryption used in Hugin Messenger, it is possible to send private, encrypted messages that can only be read by the sender and the recipient. There are no middlemen that keep any master keys, so there is no way of anyone eavesdropping.

Private video and voice calls

With Hugin Messenger, you can make private peer-to-peer video and voice calls that often beat mainstream services in terms of video and audio quality, as well as in privacy.

File sharing

Hugin Messenger lets users send files of any size without any cost or restrictions, where files are sent completely peer-to-peer.

Social network

Hugin also has a public (and private) boards function where users can discover new communities and users in a way similar to social media platforms but has the additional upsides of being completely decentralized and permissionless.

[3] https://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/oss(10).pdf

Technology

Blockchain

The base layer on which Hugin Messenger operates is the kryptokrona blockchain. Kryptokrona is a cryptocurrency based on the CryptoNote-protocol[4], which was first implemented by the ByteCoin developers, and further developed by the TurtleCoin developers.

CryptoNote is a continuation of the work by Satoshi Nakamoto, that seeks to improve on some problems with Bitcoin such as miner centralization, lack of privacy and fungibility.Unlike Bitcoin, CryptoNote proposes the use ring signatures and stealth addresses to give transactions untraceability, which is something that was required for keeping Hugin Messenger private.Additionally, CryptoNote provides us with an excellent P2P network that can be used to relay messages as well as transactions.

A kryptokrona transaction, simplified, consists of an amount of XKR to send, an address to whom it is sent, and some optional *extra data*. With Hugin Messenger, we send a small amount of XKR along with an encrypted message to the recipient's XKR address. (See fig. 1).

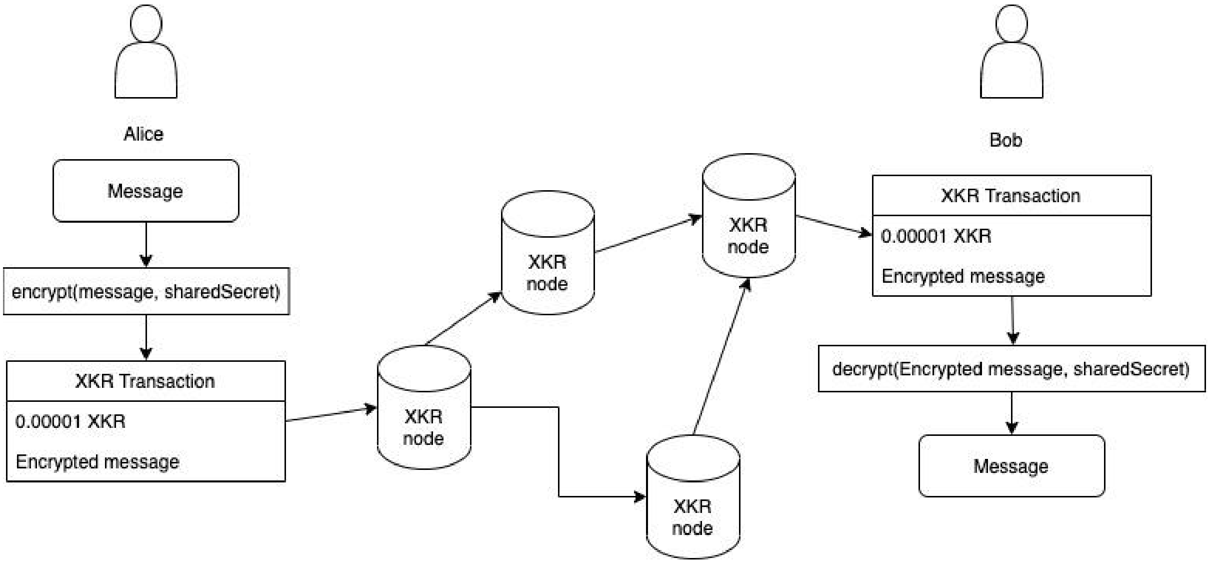

Fig. 1

In the figure above, Alice sends an encrypted message to Bob, which is propagated through the XKR node network, and when it reaches the node Bob is currently connected to, he will try to decrypt it, and if he can, he will have received the message.

[4] https://bytecoin.org/old/whitepaper.pdf

A kryptokrona node is something anybody can host by themselves on cheap hardware such as a Raspberry Pi, which means that Hugin is a federated network where the entirety of the transmission and handling of the messages is completely decentralized and independent of trusted parties or nodes.

The nodes do not know who the messages or transactions belong to, who sent them, or anything else about the contents or nature of the message. This is accomplished by the use of the CryptoNote-protocol in conjunction with asymmetric encryption of the messages.

An online user will receive a new message as soon as it reaches the transaction pool of the node the user is currently connected to, without having to wait the additional ~90 seconds for it to be stored in the blockchain itself.

Transactions containing Hugin Messages are ignored by nodes when creating blocks, and are removed from the nodes memory periodically. When they are removed, the XKR used to send the message is refunded to the sender, and can be used again. In this way you "stake" coins while the data you're sending is being published on the network.

Hugin Boards work similarly to private messages, but instead of every user having their own wallet, members of a board all subscribe to the same XKR address, and send messages to this shared XKR address instead of directly to another user's address.

There is also a distinction between *private* and *public* boards. Public boards are **unencrypted** and function as public discussion forums. Private boards, on the other hand, are encrypted with a shared private key. The downside of this, as compared to private one-on-one messaging, is that if any one person in the group is compromised, the whole group is compromised.

NaCl

NaCl (pronounced "salt") is a new easy-to-use high-speed software library for network communication, encryption, decryption, signatures, etc. NaCl's goal is to provide all of the core operations needed to build higher-level cryptographic tools.[5]

NaCl is a well tested cryptographic library, used by countless projects, that has been audited with flawless results[6].

We use NaCl (specifically the TweetNaCl[7] JavaScript implementation) to secure every private message sent on Hugin, with NaCl's elliptic curve cryptography, that works by first conducting a Diffie-Hellman key exchange, where a shared secret is exchanged by sharing each other's public keys, which are then used to compute the shared secret. This shared secret is in turn used to encrypt and decrypt messages, making them available to the two holders of the shared secret, and them alone.

[5] https://nacl.cr.yp.to/
[6] https://tweetnacl.js.org/audits/cure53.pdf
[7] https://github.com/dchest/tweetnacl-js

In practice, this is done by having a user share their XKR address, along with their public encryption key. For the first exchange in a conversation, the message is encrypted with a sealed box, containing the sender's public key. This first message can be decrypted by the recipient without any knowledge about the sender. This is important, because otherwise it would be necessary to append the sender's public key in clear text, which could be used to track users. With sealed boxes we can make these exchanges indistinguishable from any other message on the network.

Subsequent messages are encrypted with the NaCl box instead, making use of the sender's private key, and the recipient's public key.

For private boards NaCl is also used, but in a different manner. Where private boards use public-private key (asymmetric) cryptography, private boards use simple private key (symmetric) encryption. In practice, this means that private board keys have to be shared in a private channel in order to stay secure, in contrast to the public keys used for private messaging can be shared in public.

WebRTC

WebRTC (Web Real-Time Communication) is a free and open-source project providing web browsers and mobile applications with real-time communication (RTC) via simple application programming interfaces (APIs). It allows audio and video communication to work inside web pages by allowing direct peer-to-peer communication, eliminating the need to install plugins or download native apps.[8]

Hugin Messenger uses WebRTC to establish direct peer-to-peer connections between two users, enabling users to send data to one another off-chain. To make such a connection, however, you first need to make a signalling exchange, i.e. exchange details about how to connect to one another.

In most other implementations of WebRTC a central point is used to share this information, but Hugin simply sends this signaling data (SDP) as a regular encrypted Hugin message. When the WebRTC connection is established, it becomes possible to stream large amounts of data between users, enabling audio and video calls that could not reasonably be stored by every node on the network.

BitTorrent

[8] https://en.wikipedia.org/wiki/WebRTC

BitTorrent is a communication protocol for peer-to-peer file sharing (P2P), which enables users to distribute data and electronic files over the Internet in a decentralized manner.[9]

Hugin Messenger can also send files of any size, and distribute files to a large number of users, by using BitTorrent.

BitTorrent uses magnet links to link to files on it’s network. With Hugin the magnet link is simply sent to another user, and is then downloaded by Hugins built-in BitTorrent-client, which enables seamless and fast file sharing of even the largest of files.

OpenAlias

At its most basic, OpenAlias is a TXT DNS record on a FQDN (fully qualified domain name). By combining this with DNS-related technologies we have created an aliasing standard that is extensible for developers, intuitive and familiar for users, and can interoperate with both centralised and decentralised domain systems.[10]

Hugin uses OpenAlias to make it easier for users to share their details with each other, by connecting a user's Hugin address to a subdomain, such as *hugin.xkr.se.*

Then another user can use a standard DNS lookup to get access to the address details, without having to remember anything other than what closely resembles a standard email-address, instead of the 163 characters long Hugin address.

Tokenomics

Because Hugin requires users to stake XKR in order to interact with the service, this creates an incentive to buy or mine, and hold coins. You “pawn” your XKR every time you send a message, and even if you get your stake back when the message is removed from the transaction pool, the demand for XKR will increase with usage of Hugin Messenger.

Future

Hugin can be seen as a protocol on top of HTTP, a decentralized “dropbox” on which you can publish anything, either for you and your friend, or the community at large. One of our future goals is to bring a comprehensive API to developers, enabling the community to build decentralized apps on Hugin.

Such apps could include, but are not limited to, a live and recorded video and music streaming service, e-commerce services, a trading service for using atomic swaps between

[9] https://en.wikipedia.org/wiki/BitTorrent
[10] https://openalias.org/

XKR <-> BTC. The technology to enable the swaps are already available from COMIT Network.[11]
To sum it up: Hugin can become a scalable Web3.0 protocol where developers can develop virtually any service from the old web, but with the added perks of being decentralized, having privacy-by-default, as well as build in payments, taking the spirit of Hugin and Kryptokrona to the next generation of applications.

Summary

Hugin Messenger uses a slew of useful technology to achieve a completely decentralized, and scalable solution to private online messaging, as well as content publication with built in economic tools to enable tipping, shopping, content subscriptions, and much more.

One of the main goals of this project has been to make it easy for non-technical users to make use of secure cryptography that despite having been around for many years, has not made sense to integrate for corporations that mine data as an imperative part of their business plan.

Although it is true that you can use tools such as PGP to encrypt messages on any platform, but not everyone has the technical knowledge to use these available options. With Hugin, we have automated this process and made it as easy as typing “Hello” and hitting enter.

Of course, a prerequisite to use Hugin is having spendable XKR, but to use Hugin you need a very small amount of XKR that today can be mined with your phone during the nights, and in addition, you get your money back when it is cleared from the transaction pool.

Hugin Messenger is in its essence a resilient and secure, private and untraceable messaging and transaction platform.

At the current juncture clients for Windows, macOS and Linux are available on our GitHub[12], and an Android version is also being developed[13].

Harry Eriksson
info@kryptokrona.se
kryptokrona.se
Fri 3 Sep, 2020

[11] https://github.com/comit-network/xmr-btc-swap
[12] https://github.com/kryptokrona/hugin-messenger
[13] https://github.com/kryptokrona/hugin-mobile