Draupnir Proxy Private Key Technology

"In Draupnir We Trust"

Introduction

Proof of ownership is a key feature of any monetary system. Prior to the banking system, **"Proof of Ownership"** was simply what you had in your physical holding. With this system, there is no way to recognize official ownership, so a change of ownership is a simple transfer of gold/silver to another person, either with consent or without (as in the case of a robbery).

With the banking paradigm, **"Proof of Ownership"** is tied to an account number. An account number is simply a numerical identifier that is used to associate a person with a certain quantity of funds. The funds that are registered to the account belong to the person who is linked to the account number on the bank's records. To transfer funds (pre-internet days), a cheque was required as the official form that would authorize the transfer of funds from one account to another, with the owner's signature as proof of **"Authentication"**.

In the current time of the internet, **"Authentication"** and **"Proof of Ownership"** are accomplished electronically with the transfer mechanism being the scanning of a bank card at a counterparty's terminal, and entering the correct pin, only known to the holder.

Cryptocurrencies offer a new financial and economic paradigm by revolutionizing the concept of **"Proof of Ownership"** and **"Authentication"** using **Private keys** and Public addresses (Wallet Addresses). Private keys are central to the Proof of Ownership concept and Public addresses are like bank accounts. They are the numerical identifier for the funds that a person possesses. Public addresses are generated from the Private Key through specialized cryptography algorithms. This process solidifies the ownership of the funds held at the public address with the holder of the private key.

The Public-Private Key pairing is the backbone of the cryptographic finance paradigm. This paradigm provides many benefits to the transaction economy when compared vis-à-vis with the prevailing banking paradigm. It is quintessentially described as centralized finance vs decentralized finance. There are, however, concerns with the cryptography paradigm. These are derivative from the Private key. These problems are detrimental to the growth and adoption of the paradigm.

The **Draupnir Proxy Private Key** aims to solve these issues. By applying Draupnir's technology to the current cryptocurrency ecosystem, it will propel crypto into the next stages of growth: wide spread adoption of cryptocurrencies by the global economy, furthering the lead of the Cryptocurrency model and becoming the dominant financial paradigm.

The **Draupnir Proxy Private Key** is the technology that will enable and accelerate this transformation.

The Problem

"Solana ecosystem hit by hack draining millions in crypto from 8,000 hot wallet". The Verge, 04 August 2022

…"As Drecrypt reports, the transactions are signed with users' private keys, suggesting the attackers have somehow compromised the seed phrase that's used to secure their wallets"

While the Private key is central to and enables the Cryptocurrency paradigm, it is also the most vulnerable part of cryptocurrencies. Seed phrases/mnemonics are intended to add additional protection and help in the event of losing the key, but the above hack shows that it does not provide the needed security to gain people's trust.

The Private key vulnerability exists on two ends of the spectrum: 1) User Application & 2) Enterprise Application

1) User Application Vulnerabilities
   a. The user relies on the Private key for Proof of Ownership and the method of authentication. The Private key allows the user to spend/transfer the funds in his/her wallet. If the user loses the Private key, it will entail a complete loss of access to the funds. If a malicious actor gains access to the Private key, then the funds become those of the malicious actor. Because the Private key is both the mechanism for Proof of Ownership and method of authentication, whoever holds it has access to the funds in the associated wallet.

2) Enterprise Application Vulnerabilities
   b. For an enterprise, the risk revolves around possibly millions of Private Keys. Storing the Private Keys in a database creates the risk of an actor accessing billions of USD/EUR in a central database and increasing the risk-reward ratio - creating justification and incentivizing hacking into the server.
   c. Another option is to store the Private Keys on the user's device. The issue arises again when the user loses their device, or the device becomes compromised.

For the Cryptocurrency ecosystem to grow and have wide adoption as a means of settlement across the world, a protecting and confidence layer of technology must be employed to keep Private Keys from loss and theft, guaranteeing authorized users access to their funds.

This is where the Draupnir Proxy Private Key Technology comes in: it allows the user base to know their Private key is safe from loss and theft, and it is uniquely tied to them and only them. This is how confidence is built.

The Solution

The Draupnir Proxy Private Key provides confidence to the user. By safeguarding the Private Key from loss and theft by forging an unbreakable link to the user's identity and the Private Key and laying the foundation for a legal claim to the funds that reside in a wallet.

The Digital Forge Process is a proprietary (Patent Pending 17/815,667) process that generates the **Draupnir Proxy Private Key** using the user's Private Key. The *Digital Forge Process* uses three identifiable values:

1. Initial Seed String (Slug)
2. Epoch Differential
3. Digital Forge Set Number

The "Epoch Differential" and the "Digital Forge Set Number" assist during the authentication and the "Initial Seed String" and the "Digital Forge Set Number" help during recovery.

The user's Private Key is only required when generating the Draupnir Proxy Private Key and never again—securing it from any possible exposure.

There are two types of wallets, hot and cold —the level of security ranges from least secure (Hot) to most secure (Cold). Yet, security does not exist if the actual Private Key is lost or stolen.

The **Draupnir Proxy Private Key** can be printed as a QR code, programmed on an RFID tag, or written down on paper. If stolen, it is just a benign number without the other parameters that make up the Draupnir Verification System.

Ultimately, whoever gets the **Draupnir Proxy Private Key** can't leverage it to access the funds since it is not linked directly to their funds in the wallet. The **Draupnir Proxy Private Key** aids in hardening and securing the cryptocurrency ecosystem.

Draupnir assures that the user will always have access to their cryptocurrency accounts and funds.

Conclusion

"Every once in a while a new tech, an old problem, and a big idea turn into an innovation."
……Dean Kamen

The old problem is the creation of a reliable means of exchange that is not inflated away or controlled by a few who only look after their self-interest.

The big idea is the Decentralized Finance paradigm that has given rise to cryptocurrencies. The core value of Decentralized Finance is pushing the power of finance back to the people and away from a centralized system.

The new tech is Draupnir. Initially, Draupnir secures peoples cryptocurrencies using the Draupnir Proxy Private Key. Long term, Draupnir is a set of tools that is revolutionary.

The grand vision is that we can manage our financial system in a decentralized structure - through cooperation and interconnected systems governed by verifiable algorithms and proofs. A system in which anyone can participate and have full faith and confidence in preserving value and wealth without fear of confiscation, theft, or inflation.

We have the tools; it is up to us to make use of this innovation.

All that is needed is "The will to do it".

Brax Kinsey
Brax@draupnirau.com
Inventor of Digital Forge System