horizontal line

Decentralized CA

**The core encryption protocol of the internet made secure, for the first time in history.**

# OVERVIEW

TLS is the foundation that the internet relies on for security. It’s what secures all data between major websites and its users. Including critical data such as credit card information, banking information, passwords, emails, and more. For obvious reasons this system must be impossible to break. Sadly this is not the case today.  
  
Current certificate infrastructure is built with legacy approaches that have serious security flaws. The entire TLS protocol is built on top of the trust of a few centralized authorities.

This inherent weakness in security has resulted in countless compromises throughout history.

It is illogical that these old and unsecure approaches to validation have not been disrupted and by not doing so everyone is putting their own security at risk.

Decentralized CA is a revolutionary approach to certificate validation that will cause a permanent paradigm shift in how certificates are issued and validated by decentralizing the entire process with proven blockchain technologies.

**This will be the first implementation of blockchain technology with intrinsic value by default**

Decentralized CA will be a totally open source project, readable, auditable, and modifiable by everyone in the world. There will be no central points of command or decision making. All decisions will be left up to the community based on this foundation and vision.

# Goals

1. Develop a decentralized validation system on top of proven blockchain technologies to establish a permanent and unmodifiable ledger of certificates.
2. Develop plugins across all devices and applications that link into this system and allow users to use SSL certificates validated by Decentralized CA. Starting with major browsers such as google chrome, firefox, etc.
3. Get direct adoption and implementation into major browsers by default once this is established as the sole standard of certificate validation. Major browsers instead of checking with centralized authorities will check the decentralized ledger to establish validity by default. At this point our mission will have been a success. Decentralized CA will be the only way that certificates can be validated.

# High Level Design

The core of decentralized CA will be based off of proven blockchain technologies such as Bitcoin to establish a secure and unmodifiable ledger of data. This is foundation that we will use to store and validate certificates.   
  
Here is an overview of the beautiful self regulating, and dynamically scalable design.

## Coin Issuance

Coins will be issued using standard and proven blockchain technologies via a proof of work system. We will implement a very ASIC resistant protocol to ensure that mining is within the reach of ALL users using just basic computer equipment. The goal is to make sure that ANYONE can issue a certificate for their website with NO cost by simply mining for a short period of time on basic hardware.

## Certificate Issuance

To issue a certificate a user must use a specified amount of coin. This has a dual purpose. 1) It limits the amount of certificates issued to ensure that they are being used for legitimate purposes.

2) It naturally removes coins from the system forever. This means that inflation will never be a concern to the value of the system and we will not need to implement a limited supply of coins.

The price to issue a certificate, and the number of coins issued can be easily reconfigured upon agreeance by the community and consequential fork.

## Certificate Validation

To ensure that a user issuing a certificate is the true owner of the specified domain there will be a decentralized confirmation system. That is to say that there will be a string of text that the user must upload to their website and this existence must be checked and validated by thousands of decentralized sources to ensure it is correct before certs are put into the permanent ledger as trusted. The validation string is based off of the dynamic block chain data.

## Certificate Revocation

Certificates can be permanently revoked by using the same authentication process as the certificate validation. Once a certificate has been revoked, it will be permanently invalid. The user must issue a totally new certificate and validate it with a totally new string.

## Certificate Authenticity

Certificate authenticity will be established similarly to how it is done today, except for the key difference that instead of checking with a centralized authority the browser will check the decentralized ledger to see if the certificate is valid.

With this the certificate will contain several guarantably true pieces of information: Certificate Age ( How long ago the certificate was validated. The longer the more secure. This will allow users to know with certainty that the certificate they have is absolutely legitimate) and whether or not the certificate has ever been revoked.

# Conclusion

Ultimately the vision is simple and easy to understand. As Da Vinci said: Simplicity is the ultimate sophistication.

# Challenges

The biggest challenge is developing a system where can we have a decentralized agreement upon the validation of a certificate. This is where I see the most risk to security.

Ultimately the blockchain aspect of this means that even if a cert is wrongly issued the age will show to users and be deemed not secure.

Concern: Government operator or someone with millions of dollars wants to issue an invalid certificate. They make the request and using millions of machines around the world they will all vote that the certificate is valid. We will need a way to address this. Regardless even in this case security is not compromised due to the underlying design of the system. Browsers can be programmed to only trust certificates after X days of issuance (similar to confirmations of a transaction on other coins)   
  
A recently issued certificate can be similarly view to a transaction with very few confirmations.