**Using Blockchain instead of CA(Certificate Authority)**

**Certificate Authority:**

A Certificate Authority (CA) (or Certification Authority) is an entity that issues digital certificates.

The digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified.

In this model of trust relationships, a CA is a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate.

In the context of a website, when we use the term digital certificate we often refer to SSL certificates. The CA is the authority responsible for issuing SSL certificates publicly trusted by web browsers.

Anyone can issue SSL certificates, but those certificates would not be trusted automatically by web browsers. Certificates such as these are called *self-signed*. The CA has the responsibility to validate the entity behind an SSL certificate request and, upon successful validation, the ability to issue publicly trusted SSL certificates that will be accepted by web browsers. Essentially, the browser vendors rely on CAs to validate the entity behind a web site.

**Examples of CA:**

[COMODO - An ideal choice for any situation](https://comodosslstore.com/?aid=52913899)

COMODO is currently the biggest global innovator and developer of cyber-security solutions, having over 43% of the global market for SSL certificates. The company focuses on providing a wide range of reliable security solutions at very competitive prices.

Other than their low prices, every COMODO SSL certificate comes with a big pack of extra utilities. This added value makes it an especially good fit for small to medium sized companies. Choosing COMODO will get you the highest quality in security, as well as various tools. Thus, you are more efficient when it comes to clients and therefore more likely to increase your sells.

[SYMANTEC - Top-of-the-line security solutions](https://www.thesslstore.com/symantec.aspx?aid=52913899)

SYMANTEC’s certificates are used for the verification and security of more than 1 million websites worldwide. 97 out of the 100 biggest banks of the world trust SYMANTEC’s services. SYMANTEC has also contributed a great deal in the advance of Extended Validation certificates, having issued more EV certificates than any other certificate authority.

In 2012, April, SYMANTEC combined the identifyability of the Norton Secured Seal with VERISIGN’s brand name. Since then, the company’s logo shows up on screens in over 170 countries more than 500 million times a day.

SYMANTEC offers quality in good prices for all!

[GEOTRUST](https://www.thesslstore.com/geotrust.aspx?aid=52913899)

GEOTRUST is another giant in the SSL certificate market. More than 100,000 clients in over 150 countries trust GEOTRUST with their online trading and their brand name on the internet.

GEOTRUST’s wide gamut of certificates and their immediate activation make the company one of the best choices for organizations of all sizes, which are looking for low prices and maximum security.

With GEOTRUST, you can easily have the SSL certificate you want at the price you want.

[RAPIDSSL - Flawless Entry-Level SSL certificates](https://www.rapidsslonline.com/?aid=52913899)

Owned and operated by GEOTRUST, RAPIDSSL’s main purpose is one: To provide one of the most popular DV SSL certificates in the world, renowned for its very quick activation and low price point. To achieve this, the company has developed a proprietary automated verification and registration system that makes the whole process a piece of cake. This makes it perfect for bloggers, personal websites or sites that are just not collecting any crucial information.

All you have to do after purchasing a RAPIDSSL certificate, is confirm ownership of your domain and install it on your web server. So simple! In just a few minutes you have an industry-standard 256-bit Domain Validated encryption on your website.

[THAWTE](https://www.thesslstore.com/thawte.aspx?aid=52913899)

This was the first certificate authority to issue certificates on public entities outside of the USA. In 2000, it was acquired by VERISIGN, having all of the advantages that come with the number 1 choice in security certificates. It is the first company to have secured international domain names (IDNs) and, so far, it has issued over 945,000 SSLs protecting trades and corporate identities in over 240 countries.

This has become the choice of millions of users due to its multilingual support, strong certification practices and user-friendly environment which make it the best value choice among SSL certificates.

TRUSTWAVE

TRUSTAVE’s certificates are used in over 96 countries, by thousands of businesses, retail companies and big financial organizations, many of which are included in the Fortune 500. TRUSTWAVE’s SSLs offer security in internet structures and data transfers, while also providing a full range of services pertaining to credit card transactions. They have been certified by the biggest companies in the credit card game worldwide. TRUSTWAVE is also the only certificate authority to be certified as PCI Forensic Investigator.

**Can Blockchain replace CA:**

No, blockchain is an unnecessary addition to the SSL/TLS public key infrastructure (PKI). Blockchain technology doesn’t solve the problem that SSL/TLS PKI is trying to solve. The problem an SSL CA is trying to solve is matching up the names of persons and businesses, domain names and public keys.

That is, you trust the CA to tell you that traffic to, say, Amazon’s website is going to a domain owned by the Amazon company. That requires varying levels of real life business facts: that the company is registered with the relevant national business registry, that the website is controlled by the same legal entity as the certificate, the domain is owned and controlled by the same, and crucially, that it isn’t *suspicious* (i.e. you shouldn’t be given a certificate for “PayePall”).

A blockchain would ensure that once that trust decision had been made and a certificate issued, that decision would be held in perpetuity and couldn’t be silently revoked without questions. That has some value.

In practice, systems like Let’s Encrypt are handling the Domain Verification side of SSL. The bits of PKI that require actual *trust* can’t be “blockchained away” precisely because the point of PKI is cryptographically representing trust.

A blockchain is *just* a database in this scenario. It doesn’t magically give you reason to trust the data in it matches up with any actual external reality.