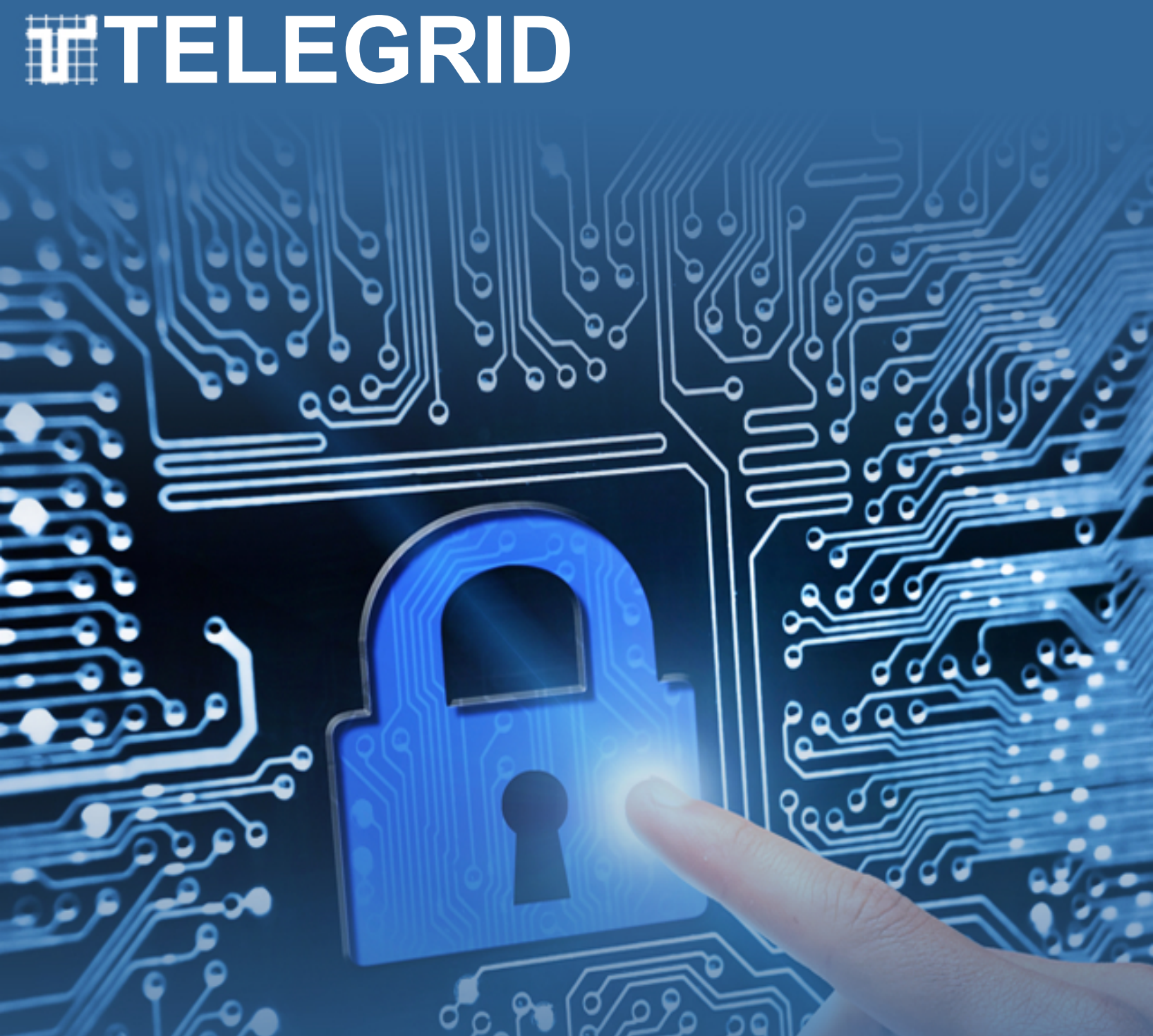
TELEGRID



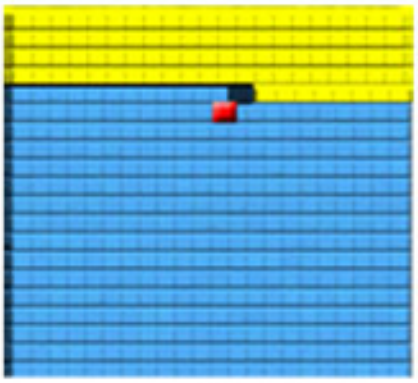
3 Ways Blockchain Can Improve Public Key Infrastructure

TELEGRID

When it comes to the future of technology there are few concepts more exciting than blockchain. Many technologist consider blockchain the precursor of Web 3.0 and the future of secure transactions. The benefits of blockchain technology, that make it ideal for transactional data, are that it is public, distributed, and once information is stored in a blockchain, it is virtually impossible to alter it. Indeed blockchain technology is already being investigated for financial transactions such as wire transfers, micropayments and stock purchases. As a company focused on secure authentication, TELEGRID identified 3 ways blockchain can improve Public Key Infrastructure (PKI).

BLOCKCHAIN BACKGROUND

Blockchain technology consists of a network of nodes which maintain a database of transactions. Each node is essentially an administrator of the network thus making blockchain a decentralized network. The original purpose of blockchain was to keep track of Bitcoins accumulated by users who earned them by solving complex computational problems (a process referred to as “mining”). When miners add blocks to the chain, the new blocks reference earlier blocks. If a user attempted to falsify a transaction, by altering an earlier block, they would have to change all the blocks from that block up to the current one. This would have to occur before any other miners add new blocks. This is virtually impossible and is why blockchain is considered a secure source for transactional data beyond just Bitcoins.



PUBLIC KEY INFRASTRUCTURE BACKGROUND

PKI is a set of policies to create, use, and revoke certificates and manage public key cryptography. Certificates are electronic documents which prove the holder’s identity and include their public key. They are issued and digitally signed by a Certificate Authority (CA). During Transport Layer Security (TLS) communications a server provides its certificate to a client which, when used in conjunction with the server’s private key, provides secure network communications. If mutual authentication is required, the client will also provide its certificate to the server. There are specific elements of PKI that would benefit from the public, distributed, and tamper-resistant features of blockchain. This white paper highlights 3 ways blockchain can improve PKI.

#1 STORAGE OF SERVER CERTIFICATES

The first of 3 ways blockchain can improve PKI is by storing server certificates in the blockchain. This would prevent a man-in-the-middle attack whereby a hacker provides a false server certificate and tricks the client into thinking they are securely communicating with the server. Man-in-the-middle attacks risk exposure of personally identifiable information to hackers.

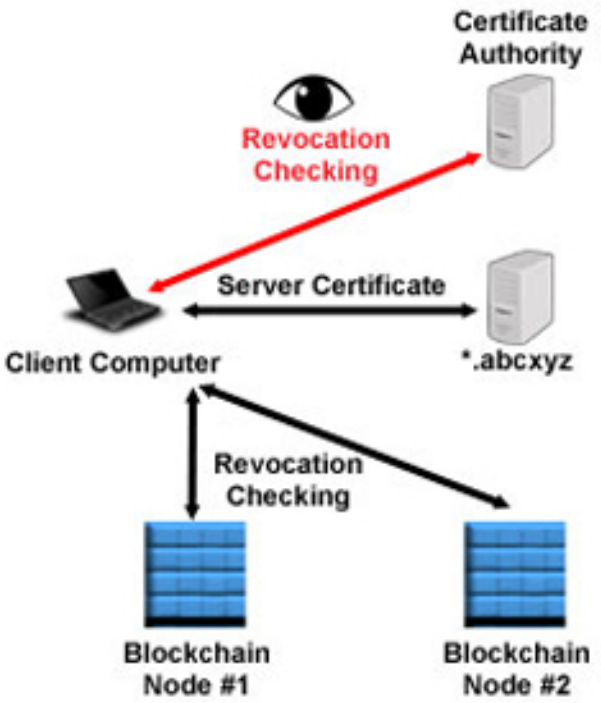
While this should be prevented by checking the CA's digital signature, it is possible for a hacker to acquire a false certificate from a legitimate CA. Indeed, in 2011 the Dutch CA DigiNotar was hacked and, as was reported, the hacker issued themselves a *.google.com certificate. This would have allowed them to eavesdrop on a legitimate conversation with google.com. Authentic representations of server certificates for high traffic sites (e.g., amazon, google, etc.) should be stored in a public and tamper-resistant blockchain so a client can validate the server certificate it receives. The full certificate does not even have to be posted to the blockchain. Alternatively, the CA's posting of the certificate's hash to the blockchain could serve as validation that the certificate was issued by the CA. Since postings to the blockchain are signed by the poster's private key, it is not even necessary for the CA to digitally sign the certificate or hash in the traditional manner.

Security could be further enhanced by allowing for distributed PKIs whereby more than one CA "issues" the certificate and stores it in the blockchain. Allowing more than one CA to post a certificate to the block, as a trusted certificate, means an adversary would have to compromise multiple CAs in order to execute an attack similar to the one on Dutch CA DigiNotar. Linking identity to public key in a decentralized manner is not unlike the web of trust (WOT) concept developed by Phil Zimmerman when he created PGP v2.0 and wrote about the concept in 1992.

#2 DISTRIBUTED REVOCATION CHECKING

The second of 3 ways blockchain can improve PKI is with revocation checking. Revocation checking is the process of a client or server checking the validity of a certificate. Revocation checking is performed via CRL or OCSP at a central location. This creates a network chokepoint and a single point of failure. Additionally, since the certificate is sent in the beginning stages of the TLS handshake, before any encryption is defined, the information it contains is sent in the clear. If a hacker is able to intercept the certificate and see the address of the CA they could perform a denial of service attack on the OCSP responder and shut down the network. Revocation checking can be quicker and more secure if it is distributed globally in a blockchain and close to the client or server that is performing the revocation checking.

Additionally, distributed revocation checking would resolve many of the privacy concerns related to PKI. Certificate revocation checking during session establishment provides a means for the CRL server or OCSP responder to collect information about a client. For example, if a CA issues a certificate to *.abcxyz.com, a client going to *.abcxyz will send the *.abcxyz certificate serial number to the issuing CA's OCSP servers for revocation checking. The CA will then have the ability to collect information (e.g., IP address) on which clients visited *.abcxyz's website. A locally downloaded blockchain for revocation checking would solve the privacy concerns for websites requiring trusted certificates.



#3 CERTIFICATE PATH VALIDATION

The third of 3 ways blockchain can improve PKI is with certificate path validation and certificate trust stores. Root CAs, intermediate CAs, and bridge CAs together form the trust chain. However just because something calls itself a CA does not mean that it is a CA. Hardware and software manufacturers have a lot of flexibility in the selection of CA certificates they pre-install. For instance, in 2015 it was claimed that Lenovo pre-installed a self-signed CA in order to intercept communications and input ads into websites (i.e., man-in-the-middle). If there was a list of trusted and untrusted CA

certificates in a public, distributed, and tamper-resistant blockchain it would provide for more secure certificate path validation.

Imagine opening a newly installed web browser, and instead of having a set of CAs pre-installed by a single corporation, a user could choose to use a publicly validated set of blockchain-enabled distributed CAs. These blockchain based CAs would be under continual review by a coalition of academia, security firms, and corporations with a vested interested in secure web browsing. In addition, the CAs would be required to pass rigorous checks from a distributed set of validation authorities before being posted to the blockchain as trust-worthy CAs. By simply selecting a checkbox during the browser's initial configuration, the browser could download and continually monitor the blockchain's trusted CA list. The system would increase in security over time, given that adversarial attempts to modify the trusted CA list would become increasingly difficult as the chain grows in length.

CONCLUSION

Too often new technologies can only be implemented via "rip and replace". Blockchain technology, on the other hand, is complimentary to PKI. It has the capability to improve the efficiency and security of PKI without altering certificates or how they are validated. The reason is that blockchain's public, distributed, and tamper-resistant nature is perfectly aligned with those of PKI and public key cryptography. This is what makes blockchain technology so exciting for PKI applications.

TELEGRID Technologies Inc.
23 Vreeland Road
Florham Park, NJ 07039
973-994-4440
sales@telegrid.com
www.telegrid.com