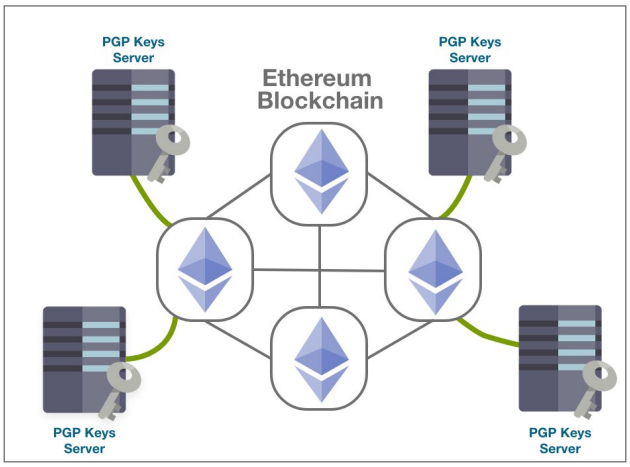
BlockPGP: A new blockchain-based PGP management framework

5 February 2020, by Ingrid Fadelli



Blockchain provides a trusted infrastructure to manage PGP keys server. Credit: Yakubov et al.

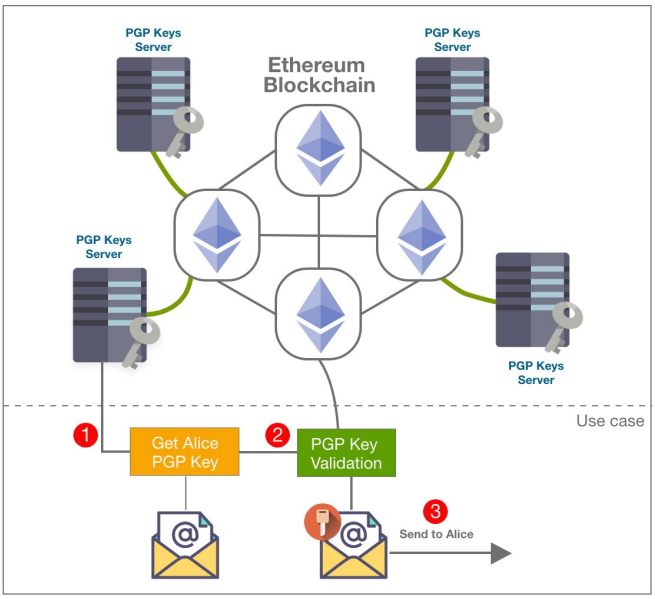
Pretty Good Privacy (PGP), one of the most widely used cryptographic standards, enables safe end-to-end encryption for emails, messages and other data sharing between users. Essentially, PGP works by implementing asymmetric encryption, in which certificates are shared through a network of PGP key servers.

Researchers at the University of Luxembourg have recently developed a new PGP management framework in which the key server infrastructure is implemented using blockchain technology. This new framework, dubbed BlockPGP, was presented in a paper published in the *International Journal of Networking and Computing*.

"We wanted to make email exchange and file exchange via the internet more secure," Alexander Yakubov, one of the researchers who carried out the study, told TechXplore. "If something is wrong with the PGP key or PGP certificate (which ensures the security of file exchange with PGP protocol), our system quickly and efficiently revokes the old PGP key, and more importantly, disseminates information about this key revocation to the majority of PGP users in several minutes."

In their previous work, Yakubov and his colleagues, who are part of the SEDAN research group, explored the potential of using blockchain technology to enhance the security of data exchanges using SSL/TLS certificates, for instance, when communicating via websites opened on internet Explorer, Chrome and other popular browsers. As the results they achieved were very promising, they later sought to apply blockchain techniques to PGP standards, as well.

In most existing PGP key servers, information is disseminated over the course of one or two days. BlockPGP can instead share information encrypted using PGP in minutes, while also eliminating the risks of man-in-the-middle attacks. This unique PGP management framework is based on a private version of leading blockchain platform Ethereum, which was deployed specifically for the system developed by the researchers.



A use case of sending an encrypted email using PGP key to Alice : (1) retrieve Alice's PGP certificate/Key from a public keys server; (2) validate the PGP certificate information using blockchain; (3) encrypt the email with Alice's PGP key and send. Credit: Yakubov et al.

"Blockchain allows our system to relatively quickly distribute information among users and to exclude risk of data manipulation. This is its main advantage over present PGP key infrastructure," Yakubov said. "Current PGP key servers often store revoked certificates, and it is quite difficult to let other users know that a given certificate is not valid anymore. But our approach significantly simplifies this."

Today, many enterprises and individual users communicate with others online, exchanging data on platforms that are managed by third-party companies. Blockchain-based encryption approaches such as the one developed by Yakubov and his colleagues have the potential to change this by distributing or replicating the same data over the internet through a worldwide system that is not owned or monitored by any company, but is instead an independent platform.

"In my opinion, BlockPGP is a good attempt at creating PKI for a PGP-system on blockchain," Oleg Khovayko, chief technology officer at Emercoin and an expert in blockchain technology, told TechXplore. "When trying to develop their own protocol, these researchers used our emerSSH as a reference for comparison. Their outcome (latency reduction, impossibility to block revocation), could thus also be applicable to our systems at Emercoin (emerSSH/emerSSL), as well as to other blockchain systems worldwide."

In the future, the framework developed by Yakubov and his colleagues could be used by enterprises to improve the security of their communications and data exchanges. Should the researchers succeed in persuading PGP users to shift from traditional key servers to their system, their framework could ultimately speed up and simplify the management of PGP certificates considerably.

"There are many research directions that we'd like to explore next," Yakubov said. "For instance, we recently developed a machine-learning algorithm to estimate trust for PGP keys (certificates). Blockchain technology is an active research topic in both industrial and academic settings. Side by side with our partners, we are exploring the benefits of this technology to enrich their portfolio with blockchain based applications. In the same context, our team made a notable contribution in the blockchain scientific community."

More information: BlockPGP: A blockchain-based framework for PGP key servers. www.ijnc.org/index.php/ijnc/ar ... cle/viewFile/217/218

APA citation: BlockPGP: A new blockchain-based PGP management framework (2020, February 5) retrieved 16 May 2021 from https://techxplore.com/news/2020-02-blockpgp-blockchain-based-pgp-framework.html