



11 hours ago | Sterlin Lujan (<https://news.bitcoin.com/author/sterlinlujan/>) | |

Coinbase Receives Patent for New Bitcoin Security Measure

(<https://news.bitcoin.com/wp-content/uploads/2017/08/Coinbase-Receives-Patent-for-New-Bitcoin-Security-Measure.jpg>)

San Francisco-based exchange, Coinbase, just received a patent

([http://patft.uspto.gov/netacgi/nph-Parser?](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetacgi%2FPTO%2Fsearch-bool.html&r=1&f=G&l=50&co1=AND&d=PTXT&s1=coinbase&OS=coinbase&RS=coinbase)

[Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetacgi%2FPTO%2Fsearch-](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetacgi%2FPTO%2Fsearch-bool.html&r=1&f=G&l=50&co1=AND&d=PTXT&s1=coinbase&OS=coinbase&RS=coinbase)

[bool.html&r=1&f=G&l=50&co1=AND&d=PTXT&s1=coinbase&OS=coinbase&RS=coin](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetacgi%2FPTO%2Fsearch-bool.html&r=1&f=G&l=50&co1=AND&d=PTXT&s1=coinbase&OS=coinbase&RS=coinbase)
base) for a security methodology for storing, distributing, and using private keys.

The U.S. Patent and Trademark Office (USPTO) approved and published the patent on August 15.

Also read: Italian Authority Fines Onecoin Promoters 2.6 Million Euros
(<https://news.bitcoin.com/italian-authority-fines-onecoin-promoters-2-6-million-euros/>)

Custodians are the Heart of the Security Methodology

Coinbase

The security protocol enables custodians to use a key ceremony application that encrypts bundles of passphrases for safe storage. The protocol also provides the ability to transfer and share private data via Coinbase.

The patent (<http://pdfpiw.uspto.gov/.piw?Docid=09735958&homeurl=http%3A%2F%2Fpatft.uspto.gov%2Fnetacgi%2Fnph-Parser%3FSect1%3DPTO2%2526Sect2%3DHITOFF%2526p%3D1%2526u%3D%25252Fnetahhtml%25252FPTO%25252Fsearch-bool.html%2526r%3D1%2526f%3DG%2526l%3D50%2526co1%3DAND%2526d%3DPTXT%2526s1%3Dcoinbase%2526OS%3Dcoinbase%2526RS%3Dcoinbase&PageNum=&Rtype=&SectionNum=&idkey=NONE&Input=View+first+page>) explained the protocol. It read, "A key ceremony application creates bundles for custodians encrypted with their passphrases. Each bundle includes master key share. The master key shares are combined to store an operational master key. The operational master key is used for private key encryption during a checkout process. The operational private key is used for private key decryption for transaction signing in a payment process. The bundles further include TLS keys for authenticated requests to create an API key for a web application to communicate with a service and to unfreeze the system after it has been frozen by an administrator."

More About the Invention/Key Ceremony Methodology

The secret behind Key Ceremony (<http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnethtml%2FPTO%2Fsearch-adv.html&r=55&f=G&l=50&d=PG01&s1=bitcoin&p=2&OS=coinbase&RS=bitcoin>) technology is the ability to distribute security data to a variety of custodians. According to the patent text, the program also uses an application programming interface (API) that allows for easy use of the technology via Coinbase's servers. Custodians then carry out a process of using the key ceremony application.

Furthermore, the concept/methodology allows for web applications to make secure checkout and payment of customer funds. The patent page elaborated, saying, "The invention also provides a method of transacting bitcoin including receiving by a web application prior to receiving a request for payment, a request for address, requesting, by the web application, an address from a service, receiving, by the service, the request for address, generating, by the service, an address and a private key in response to the request for address."

Previous Coinbase Patents

This security methodology patent, however, is not Coinbase's only patent. The company has had numerous patents filed. Bitcoin.com wrote (<https://news.bitcoin.com/things-bitcoin-companies-try-to-patent/>) about previous patents.

*"Coinbase also filed a patent
([http://appft.uspto.gov/netacgi/nph-Parser?
Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-
adv.html&r=55&f=G&l=50&d=PG01&s1=bitcoin&p=2&OS=coinbase&RS=bitcoin](http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=55&f=G&l=50&d=PG01&s1=bitcoin&p=2&OS=coinbase&RS=bitcoin)) for a 'computer system for making a payment using a tip button.' The application describes a system by which "bitcoin can be sent to an email address,' and a 'tip button rewards content creators for their efforts.' Also described is a bitcoin exchange enabling 'users to set prices that they are willing to sell or buy bitcoin and execute such trades.'"*

Do you think Coinbase will benefit from this patent? What do you think about the legitimacy of patents? Let us know in the comments section below.

Images courtesy of Shutterstock and Coinbase

At Bitcoin.com there's a bunch of free helpful services. For instance, have you seen our Tools (<http://tools.bitcoin.com>) page? You can even lookup the exchange rate for a transaction in the past. Or calculate the value of your current holdings. Or create a paper wallet. And much more.

(<https://news.bitcoin.com/author/sterlinlujan/>)

Sterlin Lujan (<https://news.bitcoin.com/author/sterlinlujan/>)

Sterlin Lujan is a journalist, editor, speaker, anarchist, and essayist. He has been involved with cryptocurrency and Bitcoin since 2012. Sterlin is especially interested in the intersection of psychology and cryptography. He has written on behavioral economics in regards to innovative technology, and was one of the first to write about the emerging field of cryptopsychology on bitcoin.com.



(<https://www.facebook.com/psychologicanarchist>)



(<https://www.reddit.com/user/SterlinLujan/>)



(https://www.youtube.com/channel/UCeUJZngyFcacT_N96vocK5w)