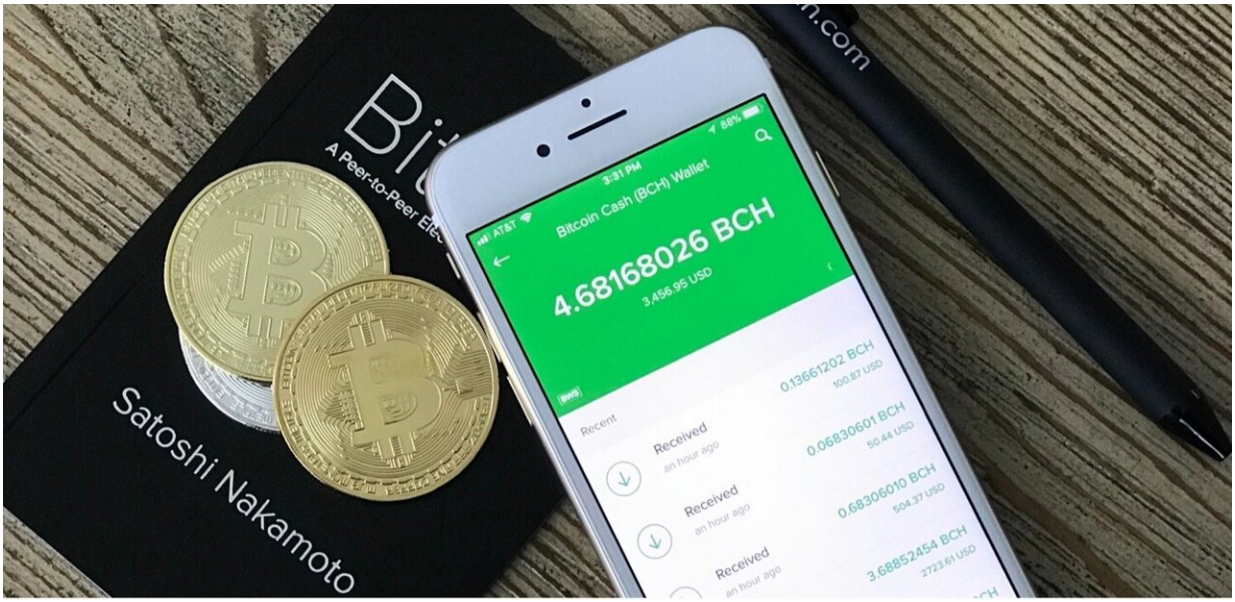
Making Bitcoin more secure

May 5 2021



"More than 90% of users are unaware of whether their wallet is violating this decentralized design principle based on the results of a user study," researchers said. And if an app violates this principle, it can be a huge security risk for the user. Credit: Creative commons via Pxhere

A computer science engineer at Michigan State University has a word of advice for the millions of bitcoin owners who use smartphone apps to manage their cryptocurrency: don't. Or at least, be careful. Researchers from MSU are developing a mobile app to act as a safeguard for popular but vulnerable "wallet" applications used to manage cryptocurrency.

"More and more people are using bitcoin wallet apps on their smartphones," said Guan-Hua Tu, an assistant professor in MSU's College of Engineering who works in the Department of Computer Science and Engineering. "But these applications have vulnerabilities."

Smartphone wallet apps make it easy to buy and trade cryptocurrency, a relatively new digital currency that can be challenging to understand in just about every way except one: It's very clearly valuable. Bitcoin was the most valuable cryptocurrency at the time of writing, with one bitcoin being worth more than $55,000.

But Tu and his team are uncovering vulnerabilities that can put a user's money and personal information at risk. The good news is that the team is also helping users better protect themselves by raising awareness about these security issues and developing an app that addresses those vulnerabilities.

The researchers showcased that app—the Bitcoin Security Rectifier—in a paper published for the Association for Computing Machinery's Conference on Data and Application Security and Privacy. In terms of raising awareness, Tu wants to help wallet users understand that these apps can leave them vulnerable by violating one of Bitcoin's central principles, something called decentralization.

Bitcoin is a currency that's not tied to any central bank or government. There's also no central computer server that stores all the information about bitcoin accounts, such as who owns how much.

"There are some apps that violate this decentralized principle," Tu said. "The apps are developed by third parties. And, they can let their wallet app connect with their proprietary server that then connects to Bitcoin."

In essence, Bitcoin Security Rectifier can introduce a middleman that

Bitcoin omits by design. Users often don't know this and app developers aren't necessarily forthcoming with the information.

"More than 90% of users are unaware of whether their wallet is violating this decentralized design principle based on the results of a user study," Tu said. And if an app violates this principle, it can be a huge security risk for the user. For example, it can open the door for an unscrupulous app developer to simply take a user's bitcoin.

Tu said that the best way users can safeguard themselves is to not use a smartphone wallet app developed by untrusted developers. He instead encourages users to manage their bitcoin using a computer—not a smartphone—and resources found on Bitcoin's official website, bitcoin.org. For example, the site can help users make informed decisions about wallet apps.

But even wallets developed by reputable sources may not be completely safe, which is where the new app comes in.

Most smartphone programs are written in a programming language called Java. Bitcoin wallet apps make use of a Java code library known bitcoinj, pronounced "bitcoin jay." The library itself has vulnerabilities that cybercriminals could attack, as the team demonstrated in its recent paper.

These attacks can have a variety of consequences, including compromising a user's personal information. For example, they can help an attacker deduce all the Bitcoin addresses that wallet users have used to send or receive bitcoin. Attacks can also send loads of unwanted data to a user, draining batteries and potentially resulting in hefty phone bills.

Tu's app is designed to run at the same time on the same phone as a wallet, where it monitors for signs of such intrusions. The app alerts

users when an attack is happening and provides remedies based on the type of attack, Tu said. For example, the app can add "noise" to outgoing Bitcoin messages to prevent a thief from getting accurate information.

"The goal is that you'll be able to download our tool and be free from these attacks," Tu said.

The team is currently developing the app for Android phones and plans to have it available for download in the Google Play app store in the coming months. There's currently no timetable for an iPhone app because of the additional challenges and restrictions posed by iOS, Tu said.

In the meantime, though, Tu emphasized that the best way users can protect themselves from the insecurities of a smartphone bitcoin wallet is simply by not using one, unless the developer is trusted.

"The main thing that I want to share is that if you do not know your smartphone wallet applications well, it is better not to use them since any developer—malicious or benign—can upload their wallet apps to Google Play or Apple App Store," he said.

More information: Yiwen Hu et al, Security Threats from Bitcoin Wallet Smartphone Applications, *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy* (2021). DOI: 10.1145/3422337.3447832

Provided by Michigan State University