# Don’t Let Blockchain Technology’s Security Loopholes Go Unnoticed

Do you assume, for instance, that private ‘permissioned’ blockchains are secure? You’re wrong.

January 11, 2019 6 min read

Opinions expressed by *Entrepreneur* contributors are their own.

At the start of 2018, the International Data Corporation published a report forecasting $2.1 billion in global spending on blockchain solutions for the near future. In July, the research firm followed up with another spending guide, which estimated that blockchain spending would exceed $11.7 billion by 2022.

**Related: Blockchain Technology Can Be Critical to IoT Infrastructure Security**

That forecast is beginning to bear out: Today, blockchain technology continues to appeal to the global corporate institutions looking to fundamentally change the ways in which they handle transactions and manage data.

That appeal makes sense, considering blockchain’s time-stamped, distributed and irreversible benefits. Overall, the technology boasts transparency, reliable tracking, reduced costs and the ability to eliminate intermediaries. It is, therefore, no surprise that financial giants like Bank of America are looking to blockchain to create more efficient financial transactions for consumers and businesses alike. More examples? The global giants Walmart and United

Bank of Switzerland are working with IBM to develop blockchain-based finance platforms.

Still, there is a caveat to these positive developments: With cryptocurrency — blockchain's most popular financial application — continuing to witness sharp highs and lows — confidence around the technology isn't where it was a year ago. On one side, we have blockchain enthusiasts who swear by the technology; on the other are those raising serious concerns about the various cryptocurrencies, such as regulatory uncertainty and overall trust.

**Related: Thanks to Blockchain, Decentralization — and Data Security — Are the Future**

According to a study conducted by PWC last summer, 45 percent of respondents cited "trust" as the biggest barrier to adoption of the technology.

That brings us to the present. And, today, the large number of hacks and thefts, coupled with lax regulatory policies, have not only crippled the crypto economy, but also led people to question the immutability and security of blockchain. So, the obvious conclusion is that while the blockchain is secure in and of itself, it can very much be compromised at the point of access.

What constitutes those security vulnerabilities? Here's what you need to know about permissioned blockchains, crypto wallets and crypto exchanges as well as how these security gaps can be hardened for greater security.

# What makes cryptocurrencies and crypto exchanges vulnerable.

A whopping $9 million is stolen from crypto wallets every day. From DAO to GDAX and Mt. Exchange to Zaif, even the best of exchanges can't protect themselves from being hacked. As of

June last year, $1.1 billion had already been stolen in cryptocurrencies in 2018.

Why do crypto wallets and crypto exchanges continue to fall victim to crypto hacks? The answer is that hackers are adept at manipulating the vulnerabilities that lie within our devices, and within us, as the humans using them. Hackers are increasingly using malware to attack the devices that we use to interact with crypto wallets and exchanges.

Because most people continue to rely on a 30-year-old anti-virus technology to combat threats to their devices, security is falling short. Every four seconds, hackers release a new string of malware, and by the time an antidote is created, another malware has been generated to take its place.

**What we need instead** is a proactive solution that protects devices inside out with features such as keystroke encryption, anti-clickjacking capability, anti-screen capture and strong password protection.

Only then can we stay a step ahead of the hackers who are continuously coming up with newer, more sophisticated ways to attack wallets and exchanges by gaining access to our devices.

# What makes private (permissioned) blockchains vulnerable.

Contrary to common perception, there are inherent vulnerabilities in the private blockchain. A blockchain essentially works as a shared record of information that multiple parties can reference, observe and make additions to. Unlike public blockchains, where anyone can participate in the network, conduct transactions and maintain the shared ledger, *permissioned* blockchains can be accessed only by those with express authority to the network.

This means that multiple parties can reference, track and

alter transactions within a private blockchain, as long as they are authorized to enter it. Each transaction within this shared record is digitally signed, to ensure its authenticity and integrity.

Enterprises looking to deploy permissioned blockchains work with the assumption that only authorized users can access those transactions and that only a legitimate transaction can be permanently added to the record, making the transactions untouchable.

Unfortunately, that assumption is wrong. What these enterprises don’t consider is that malware could be secretly attached to a legitimate transaction made by an authorized user. This move could then become permanent, just like all the other data stored on the now-infected blockchain.

**To prevent permissioned blockchains from being compromised, we need** to employ a combination of new and existing technologies. For example, tried and tested transaction verification assurance, such as out-of-band authentication, could ensure that only verified transactions would be permanently added to the permissioned blockchain.

In addition, content agents that scan everything entering blockchain could ensure that malware not make its way into the blockchain. Furthermore, each blockchain could benefit from specific rules and policies in place dictating what blockchain users with express authority to access the network could or could not do.

Such goals could be accomplished via a policy engine capable of encoding rules and corporate policies into the blockchain.

## Leveraging blockchain’s promise and

# potential

While blockchain has inherent security issues, industry players with the foresight and capability to leverage the power of blockchain technology should in no way feel discouraged.

In fact, blockchain's numerous use cases can be and are already shaping up to be a hard reality. However, innovators and entrepreneurs looking to adopt the technology should go in with a thorough understanding of the security issues involved and embark on their blockchain journey by first ensuring that proactive measures are in place to combat the risks. Here are a few pointers to help prepare those looking to implement the technology, especially in payments:

• **Blockchain and cryptocurrency are here to stay.** While still in the early stages, these technologies are quickly becoming part of the fundamental fabric that businesses will use to gain a competitive edge. So, as an entrepreneur, you should become a zealous student and learn all you can about this expected change.

• **Develop a strong cybersecurity posture and practice it all the time, especially when dealing with cryptocurrencies.** Crypto-hackers are relentless at developing new schemes to steal crypto. So, remember that a good carpenter will always "measure twice and cut once." Apply that same preventive practice to your own daily computing habits.

**Related: Sick of Passwords? Here's How Blockchain Can Help, and Enhance Cybersecurity, to Boot.**

• **Embrace the future of blockchain and crypto**. Get involved, talk to others about these changes; go to local meetings; and become a proactive part of this new evolution.

https://www.entrepreneur.com/article/325992