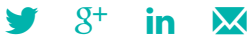SERGEY NIVENS - FOTOLIA

Experts wade through hype to shed light on blockchain security

💬 1

↗

by
Francesca Sales
Site Editor

🐦 g+ in ✉

Along with the hype, there have been plenty of questions around blockchain technology, particularly regarding blockchain security. A panel of experts takes on these concerns.

THIS ARTICLE COVERS
Risk management »

RELATED TOPICS
Automating compliance
BC
Business records managem
Enterprise cloud compliance
Information technology gov

LOOKING FOR SOMETHING ELSE?

📄 Industry gurus tackle blockchain privacy and digital identity

📄 Managing cybersecurity and supply chain risks: The board's role

📄 Data protection requirements start with firm grasp of GRC needs

🏷 **TECHNOLOGIES**

Cryptography   Database transaction processing   Finance & accounting
Use cases & examples

There has been a lot of hype of late about the potential far-reaching benefits of blockchain technology, a decentralized database for storing transaction records. And behind that excitement is a lot of promise: The tamper-proof technology behind bitcoin and other cryptocurrencies has the potential to change how business gets done in a plethora of vertical industries such as financial services, real estate, insurance and healthcare. Even national governments are pursuing the possible advantages of blockchain for country-wide initiatives: Estonia is working with a blockchain startup to secure its citizens' 1 million electronic health records with the technology.

Alongside the voices that have touted its potential use cases, however, there have been those that have raised thorny questions about various aspects of the blockchain system, especially blockchain security. Recent events, such as the theft of 3.6 million Ethereum coins from Slock.it's DAO (decentralized autonomous organization) fund, have also brought to light the potential flaws of this much-discussed technology.

Audience members at a blockchain session at the recent MIT Sloan CIO Symposium voiced some of these concerns. Here is how a panel of blockchain experts addressed their questions.
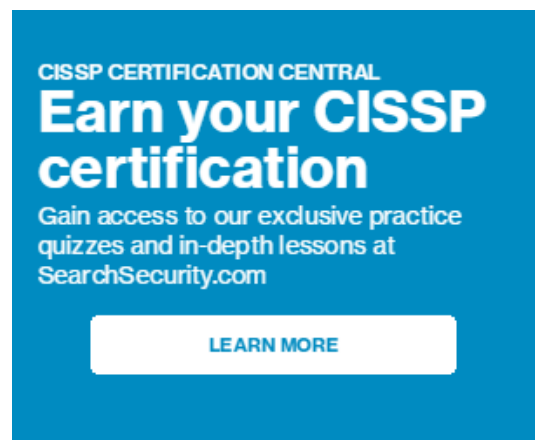
What data actually gets put on the blockchain and how much control do users have over it?

In a public blockchain system, users' information is not stored on the blockchain but rather with a third party such as Amazon. What's put on the

network is a cryptographic hash of the transaction information in each "block" of the blockchain (blocks are collections of data regarding transactions made within a set time period). Panelist Anders Brownworth, principal engineer at blockchain-based payments app company Circle, said the hash proves that a user made the transaction at a certain point in time without revealing user information. Transactions are validated by miners, which are systems on the network that solve complex transaction-related algorithms and are afterward rewarded with a certain number of bitcoins for each block on the blockchain.

"You're not going to put absolutely everything on the blockchain because it doesn't make sense for everyone to have a copy of absolutely everything," said Brownworth, whose company has raised $60 million in funding and recently expanded to China.

Peter Nichol, a healthcare expert at PA Consulting Group, said that the hash is used to verify transactions and functions like an access control.

"A lot of the [standards] that you're already familiar with, like NIST and others that already control the level of access to information, can still be applied," he said.

⬛ Are blockchain use cases and blockchain security benefits overhyped? How secure is it, really?

Brownworth acknowledged that blockchain is overhyped and that a truly secure and tamper-proof blockchain record system is still theoretical. But after seeing the code behind the technology, Anders believes it is inherently secure.

Search the TechTarget Network

"We're not hanging our hat on a governmental agency or a certain group of people; we're hanging our hat on the full faith and credit of math, of cryptography. That works for me a lot better than a group of people," he said.

Brownworth added that the nature of the database itself speaks to blockchain's security: It relies on its miners constantly trying to crack the correct hash inside a peer-to-peer network, using their hardware and software, to solve a block and access its information -- essentially what amounts to a brute force attack.

"What they do is take this attack and they turn it into a benign force so that instead of attacking the network to obliterate it, [it] rewards them with some financial gain from doing that," Brownworth said, adding that one way to measure the technology's security is that its "$7 billion bounty" -- how much the entire system is worth -- has yet to be claimed.

But even if the blockchain system is purportedly secure, what about user vulnerabilities? One audience member brought up the recent breach of the computer systems of up to 12 banks linked to Swift, a global financial system. The hack was possible because of a stolen private key.

> **We're not hanging our hat on a governmental agency or a certain group of people; we're hanging our hat on the full faith and credit of math, of cryptography. That works for me a lot better than a group of people.**

Anders Brownworth
principal engineer, Circle

Brownworth admitted that blockchain isn't necessarily immune to social engineering attacks, but that doesn't mean there's anything wrong with the code.

"Stealing credentials and making valid requests on the network, signed by valid credentials ... that's not a direct attack against the encryption [itself]," he said. Cryptography, he said, is more trustworthy than people who have to remember and hold onto private keys.

Matthew Utterback, co-founder of Rex Mercury Inc., agreed, saying that people don't wholeheartedly trust banks for this reason.

"Everybody I work with has direct experience with a bank failure. We obviously need to educate people on ... their private keys. But being able to have this open source valuation [that blockchain has], yeah we can look at the code, and [seeing that], I sleep better at night," he said.

Check out part two of this discussion on blockchain security and privacy: Experts discuss how blockchain can be applied to electronic health records and how to balance privacy and digitization.

Francesca Sales asks:

Do you think blockchain's security benefits are overhyped?

0   Responses   **Join the Discussion**

➥ Next Steps

Industries look beyond the financial benefits of blockchain

Will blockchain compliance rules hinder innovation?

U.S. Congress considers blockchain security concerns

This was first published in June 2016

⬎ Dig Deeper on Risk management and compliance

ALL ▲	NEWS	GET STARTED	EVALUATE	MANAGE	PROBLEM SOLVE

New Jersey CTO targets compliance, security standards

Industry gurus tackle blockchain privacy and digital identity

As IoT and big data increase cyber risks, industry on the defensive

Cybersecurity insurance policies gain popularity as threats persist

Load More

💬 **1 comment**

Oldest ▼

Share your comment

☑ Send me notifications when other members comment.

Register or Login

E-Mail

email@techtarget.com

Username / Password

Username

Password

Comment

By submitting you agree to receive email from TechTarget and its partners. If you reside outside of the United States, you consent to having your personal data transferred to and processed in the United States. Privacy

Sharon Fisher — 30 Jun 2016 11:49 PM

It's difficult for me to believe that governments are actually going to let blockchains operate with impunity. It sounds an awful lot like a parallel currency system, and I don't think they're going to go for that. Look at how the states have been flipping out over online poker and fantasy sports.

Latest TechTarget resources

SearchCIO

Blockchain market outlook: Hype vs. reality

There are predictions that the blockchain market will change the nature of business transactions. But how much of that is hype? ...

Google snaps up startup in push to master computer vision

The future of computer vision looks bright following a string of tech acquisitions in the field, most recently by Google. Also in...