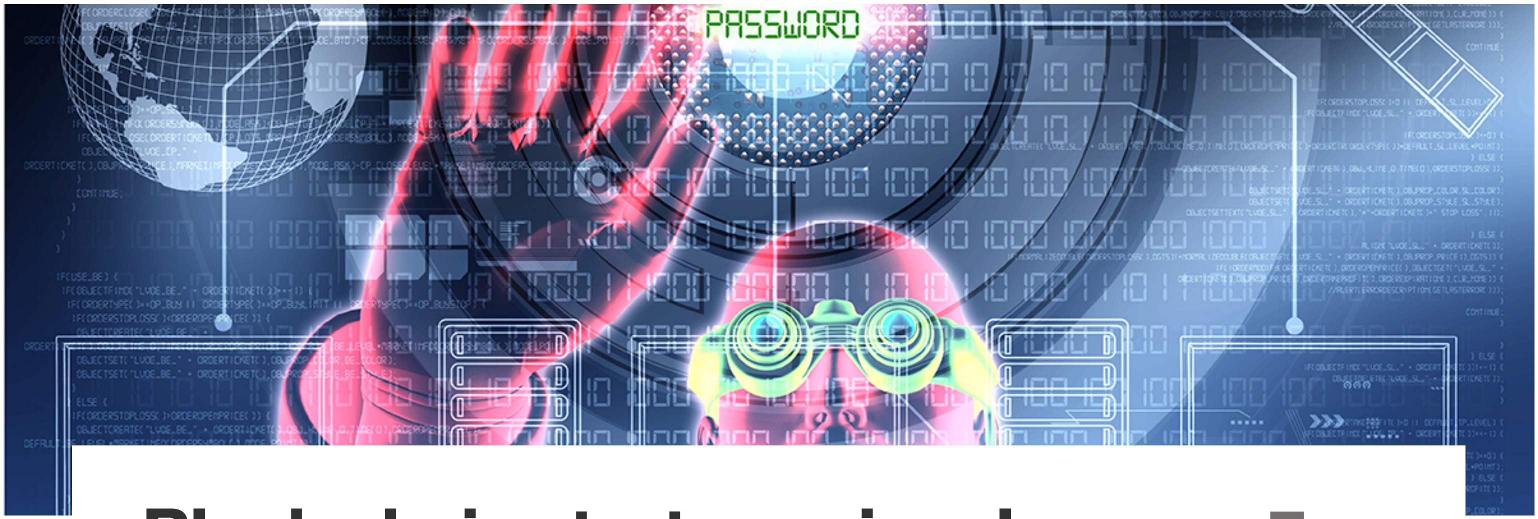
NMEDIA - FOTOLIA



# Block chain startups signal new approaches to data integrity

by
Robert Richardson
Editorial Director

Bitcoin 2.0 is fueling technology development and services. The block chain mechanisms that secure the Bitcoin network hold real promise for security.

THIS ARTICLE COVERS
Data Security and Cloud Computing

LOOKING FOR SOMETHING ELSE?
The big data challenge: What's in store for

TECHNOLOGIES
APIs Data integrity Network security New & emerging

RELATED TOPICS

Data Analysis and Classifica
Data Loss Prevention
Database Security Manage
Disk Encryption and File En
Enterprise Data Governance
Data breaches and ID theft

NoSQL security

technology

+ Show More

Download

This article can also be found in the Premium Editorial Download:

Information Security magazine: Malware analysis beyond the sandbox:

In this Article

- Public history of transactions
- Alternate chains
- Dig Deeper

Related Content

**The transaction that lasts forever**
– SearchSecurity

**Australian police raid home of alleged Bitcoin ...**
– ComputerWeekly

**Bitcoin mining**
– WhatIs.com

Sponsored News

**As Security Threats Increase and Diversify, New Defenses and Strategies Are ...**
–Dell

**A Threat Intelligence Service Case Study: The Escelar Trojan**
–Palo Alto

See More

Vendor Resources

**CIO Decisions – July 2016, Volume 54**
–SearchCIO.com

Looking for a radical way to bolster all three points of the classic security CIA triad? Lucky for you, there’s Bitcoin.

Specifically, there are two concepts lurking in the Bitcoin phenomenon that are considerably more important than the currency itself: the decentralized transactions database, or block chain, and the idea of “programmable currency,” which really is more about adding a scripting API to extend the block chain construct than it is about money.

The direction this scripting capability will take isn’t clear yet. A startup called Ethereum is well underway with its own programming language, Ethereum Script, and a platform for developers to create decentralized applications based on smart contracts (without the middleman). Another startup called Counterparty offers peer-to-peer financial tools specifically tied to Bitcoin.

When it comes to the Bitcoin block chain, it’s already crystal clear that there are big potential wins for security.

# Public history of transactions

If you're aware of Bitcoin, you're familiar with the idea that so-called Bitcoin miners harness high-speed computational processing power in an effort to solve mathematically difficult problems to secure and verify transactions, and create Bitcoins. (Miners earn transaction fees and subsidies -- paid in Bitcoins, of course.) A new block is written every ten minutes, extending the chronological block chain, which is shared among nodes on a peer-to-peer network using the Bitcoin protocol. But it's more complicated (and far more elegant) than that.

The block chain is a series of data records -- time-stamped transactions -- stored in a database. The hash of each block (beginning with the "Genesis block") is used to link to the next so that there is a single forward pathway through the blocks: This is the "chain." Each new block is broadcast in near real-time all across the Internet, with almost every miner (or node) maintaining a current copy of the transactions log.

When a Bitcoin transaction occurs, the previous transaction's hash and the public key of the next owner are digitally signed with the current owner's private encryption key. If you want to transfer your Bitcoin (that is, buy something), you have to have your secret key. No key, no possession.

Once an entry is written into the block chain, it cannot be altered without regenerating the previous blocks. (In other words, data can be *added* to the transactions database, but it cannot be removed.) This prevents double-spending and ensures the forward linking of the block chain.

> **There are two concepts lurking in the Bitcoin phenomenon that are considerably more important than the currency itself.**

Therein lies the security angle. If a company were to store its general ledger in the Bitcoin block chain, a bad apple in the accounting department would be completely unable to go back without detection and alter previous entries to cook the books. Think of the potential impact on fraud prevention.

While it might seem odd to think of storing those kinds of transactions in Bitcoin’s block chain, in fact, you can store pretty much any sort of data. And people have occasionally done so, though admittedly with a bit of a “toying with the system” approach. There’s a picture of Nelson Mandela in the block chain, for instance.

There’s even a model hacker exploit (tip of the hat to Ken Shirriff’s blog):

```
<script>window.alert("If this were an actual exploit, your mywallet would be empty.")</script>
```

Note that the exploit had to do with a client program called MyWallet, not with the Bitcoin technology -- one definite issue in the Bitcoin economy is that wallet programs that store private keys have to remain unhacked.

## Alternate chains

Now, writing to the Bitcoin block chain isn’t free. It is actually a little pricey if you start thinking about storing megabytes, so no one’s likely to use it for directly storing their logs. But the concept of a decentralized database whose records are “secured” by 10,000 computers can, of course, be extended to other block chains. A startup called Factom is working this angle.

As Peter Kirby, the president of the Austin-based company, put it: “It turns out that having permanent, immutable, tamper-proof data is a really big deal for anybody who does record keeping, anybody who cares about their data being written once and never changed and never tampered with.”

Factom is just gearing up, but eventually will let its customers write to a separate block chain that’s more suitable for data entries. Cleverly, however, it ties those entries back to the Bitcoin block chain by storing a hash of each new Factom in the next Bitcoin block added to the chain. The hash can be used to verify the time of the Factom transactions and that the Factom block hasn’t been tampered with.

There are other startups doing this, too. Storj is beta testing a distributed cloud storage service that uses block chain technology. MetaDisk is a file sync app built atop the Storj block chain infrastructure. BlockCypher is building a cloud block chain platform with APIs that make it easier for developers to build applications based on this technology.

There’s more than just secure recordkeeping lurking here, however. Digital assets can be controlled just like Bitcoins (which are, after all, digital assets themselves), so digital rights management may well wind up with a whole new look and new capabilities (such as easily transferring ownership of your music collection -- just try reselling stuff you bought through iTunes).

I can’t help but think that there will be direct applications of block chain technology to the security space (beyond immutable records). I don’t have the killer block chain security app figured out yet, but I’m sure, all the same, that non-fungible developments spinning out of Bitcoin will be fascinating to watch from a security perspective.

**About the author:**
*Robert Richardson is the editorial director of TechTarget’s Security Media Group. Follow him on Twitter:* @cryptorobert.

This was first published in June 2015

## Dig Deeper on Data Security and Cloud

# ↘ Computing

ALL | NEWS | GET STARTED | EVALUATE | MANAGE | PROBLEM SOLVE

### How to achieve secure file sync and share

### A secure sync-and-share tool can provide powerful file protection

### The big data challenge: What's in store for NoSQL security

### Encryption key management: Should keys still be stored in the cloud?

Load More

## 0 comments

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

## SearchCloudSecurity

### Cloud apps failing EU GDPR privacy regulation compliance so far

Cloud apps and cloud customers face challenges in complying with the EU GDPR as the new data protection regulation is set to take...

### Top AWS security features organizations need to know about

As cloud security becomes more essential, Amazon security features become more important. Expert Matthew Pascucci takes a look at...

About Us

Contact Us

Privacy Policy

Videos

Photo Stories

Guides

Advertisers

Business Partners

Media Kit

Corporate Site

Experts

Shon Harris CISSP training

Reprints

Archive

Site Map

Events

E-Products