Blockchain Isn't as Unbreakable as You Think

Stuart Madnick

Working Paper CISL# 2019-21

November 2019

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

MITSloan
Management Review

Blockchain Isn't as Unbreakable as You Think

Before exploring ways to use blockchain in business, managers should know where its vulnerabilities lie.

Stuart Madnick

• Reprint #61216 • https://mitsmr.com/2Kic91g

Blockchain Isn't as Unbreakable as You Think

Stuart Madnick

Before exploring ways to use blockchain in business, managers should know where its vulnerabilities lie.

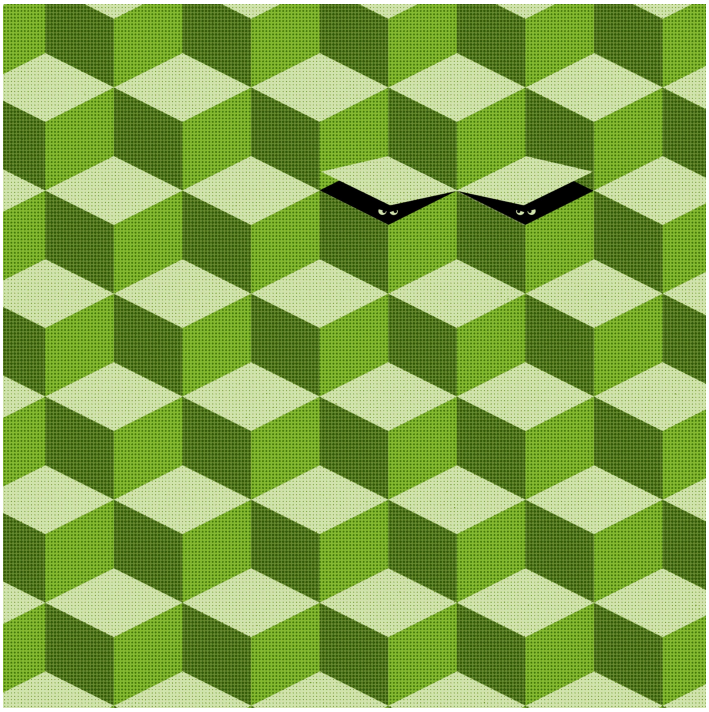

Image courtesy of Dan Page/theispot.com

Sometimes it seems as if everyone has bought into the hype: Industries as far-flung as real estate and diamond sales [1] have embraced blockchain without entirely knowing what it is or how its most vaunted features might fail or have unintended consequences. Blockchain assures users that once information has been stored, it can never be deleted or falsified. This means that when people in finance, say, pore over the history of a transaction, they feel content in the knowledge that illegalities have nowhere to hide. It means that people in the supply chain of a product trust that they can check its provenance without fear that misinformation has been slipped in along the way. In essence, blockchain promises not just complete data security but also something more intangible: that we will never be conned. Is it really so important that we understand what's under the hood?

The truth is that blockchain is not as secure as it is believed to be, and its features can rebound in unfortunate ways. In research I conducted with Jae Lee, described in detail in his graduate thesis [2] and a forthcoming paper for the Cybersecurity at MIT Sloan (CAMS) initiative, we cataloged 72 breaches reported between 2011 and 2018. These breaches cost users a grand total of more than $2 billion. Many of these breaches were possible because blockchain is actually vulnerable in some of the same ways that conventional, centralized record-keeping systems are. The rest are even more troubling, because bad actors were able to exploit the very features that make blockchain revolutionary: transparency, distributed control, anonymity, and immutability. In this article, we will look closely at both categories of vulnerabilities so that organizations can weigh the risks and decide whether to make use of blockchain.

Old-Fashioned Chinks in Blockchain's Armor

Blockchain is widely viewed as unbreakable because advanced cryptographic techniques are used to encode the

data and ensure that it is not altered. But there are vulnerabilities to be exploited. Let's focus first on the ones that have long been present in more conventional systems as well.

Private keys. Much like traditional passwords, private keys must be written down, whether on paper or in a digital wallet, because they are such large numbers. Once they're written down, of course, they can be found. A cocky bitcoin owner actually printed his blockchain key as a QR code on his T-shirt just to see what would happen. This is what happened: Someone took a photo of him and used it to drain his account. [3] (Before you laugh at his foolishness, ask yourself if you've ever scribbled a password on a sticky note.) In another breach, a TV news anchor showed viewers a Bitcoin that was being gifted, and a Reddit user scanned the digital QR code with his phone and nabbed the funds for himself. [4]

Software flaws. The blockchain itself is essentially just data. To add information to the blockchain or make use of the existing information requires software code — and, like any software, it can have flaws. In fact, it often has more flaws than you would usually expect to encounter. In the distant past, I worked as a software developer for IBM. There was typically a six-month delay between the time I completed an update to the system and the date it was made available to users because a quality assurance (QA) group needed time to run extensive tests. That kind of due diligence is increasingly a thing of the past.

The early applications of blockchain, such as Bitcoin, were relatively simple, mostly involving the transfer of funds. The open source code was stable for long periods of time. Users didn't need to be professional software developers — they just needed to know how to download the open source code. Newer applications are much more complicated. The transition happened incrementally but rapidly enough that QA did not keep pace. Furthermore, because of fierce competition, there is enormous pressure to rush to market, which can make QA seem like a nuisance.

As a result, there are often subtle flaws in the writing of blockchain system software. Consider the Ethereum hack, where an intruder discovered a programming mistake and used it to move money into his or her account. (More about this case a bit later.) In another instance, flaws were introduced by developers rushing to meet new regulations actually aimed at *improving* security. The changes were not carefully reviewed, the flaws were exploited, and money was stolen. The cost of this lesson in irony was roughly $60 million. [5]

New Weaknesses Specific to Blockchain

Some of the things that make blockchain so attractive also make it vulnerable. Let's revisit the four prized values mentioned earlier.

Transparency. The logic goes that blockchain software is sound precisely because so many people can see it and verify that there are no flaws, like a Wikipedia entry everyone is double-checking for accuracy. Unfortunately, this also means a bad actor can study the code and uncover flaws no one else has noticed yet.

Distributed control. A traditional, centralized system simply stops if the computer fails. In a blockchain system, the software operates simultaneously on such a preponderance of servers that even if one or more servers fail, the system continues running. That has obvious benefits. But it also means there is no central on-off switch, and, to put it plainly, there are times when you need to shut things off. The U.S. Securities and Exchange Commission, for instance, mandated the creation of "circuit breakers" after the May 6, 2010, flash crash that saw the S&P 500 drop 8.6% in a single day. The system now automatically shuts down trading if there is a sudden, steep market decline. [6] In contrast, blockchain systems are not intended to ever stop.

Even if an attack is discovered on a blockchain system, servers around the world still operate. In the example of the software flaw on the Ethereum system, in particular the smart contract for the distributed autonomous organization (DAO), there was no way to stop the intruder from continuing to siphon off money. The ad hoc solution, such as it was, was to have a group of "good guys" use the same flaw to siphon off the money faster than the "bad guy" and then return as much money as possible to its rightful place.

Blockchain's transparency may have made matters worse during the race against the clock. There was an active public blog, mostly used by smart contract developers, where suspicions about possible flaws were posted for over a month. The blog probably aided the attacker in learning about the suspected flaw and how to exploit it; furthermore, by monitoring posts, the attacker knew when the hack had been discovered and, hence, when it was time to disappear. In the end, about $50 million was stolen. Based on the blockchain principle that "code is law," the DAO attacker in an open letter to the community claimed that the stolen funds were legal compensation in light of binding smart contracts. The attacker threatened to take legal action against any attempt to invalidate what he or she did. Other such cases have been reported, including the Komodo hack. [7]

In a centralized system, the hierarchy makes clear who is in charge of security. As for a decentralized system like blockchain, it's useful to keep in mind that the Wild West was also decentralized.

Anonymity. Blockchains use cryptography that pairs a publicly available key and a private one. Public keys are widely distributed, while private keys are kept secret. One result of that presumed anonymity is that blockchain systems, such as Bitcoin, are popular for illegal transactions, such as ransomware payments, making them effectively untraceable.

To the extent that blockchain systems provide anonymity, [8] another downside is worth considering: If you lose your private key, you've lost access to your account forever. When bank patrons misplace the keys to their safety deposit boxes, banks can resort to a master key, a locksmith, or a crowbar. There is no such override on your blockchain account. Take the case of Gerald Cotten, CEO of cryptocurrency exchange QuadrigaCX, who died unexpectedly in India from complications related to Crohn's disease early in 2019. As a result, no one can access customer funds because no one knows the passwords to the digital wallets on his computers. More than $137 million in virtual currencies are at stake, [9] and 10 other such examples have been reported. [10] Because most people would not be eager to admit to such devastating carelessness, the actual number of cases is most likely higher.

Immutability. We have discussed the upsides to the fact that (according to the rules users agree to uphold) data in a blockchain can never be removed or altered. But what happens if and when a system is used to record something a person would rather not have follow them until the end of time? What if a blockchain were used for criminal records and someone wanted their record expunged? It would be impossible. Thanks to the European Union's General Data Protection Regulation, anyone living in the EU has the right to request that information about themselves be erased once it is no longer needed. In a blockchain world, they couldn't exercise that right.

Now let's consider a very different example. All kinds of extra data and commentary can be included in the blockchain and, like everything else, will live on in perpetuity. A group of "artists" took advantage of this feature by adding a text image they dubbed Permanent Phallus to the Ethereum blockchain. (Being artists, they even signed it.) As a result, every one of the thousands of Ethereum servers has a penis in its blockchain.

If that sounds harmless, consider a more troubling case study. In 2019, child pornography images were found in the Bitcoin Satoshi Vision ledger. [11] The browser was shut down and a filter put in place, but actually removing the content from the ledger would require agreement among all of the blockchain servers — which is no small feat. So, in the meantime, the users of that blockchain might be violating child pornography laws.

How You Can Reduce Risk

The mishaps and catastrophes described above were mostly the result of carelessness and poor decision-making. In many cases, management assumes that because the cryptographic techniques used in conjunction with blockchain systems are unbreakable, there is no need for any concerns about security. As I often say, you can get a stronger lock for your door, but if you are still leaving the key under your mat, are you really any more secure? [12]

However, it is possible to mitigate the following risks:

Password/key exposure. Most organizations have programs to educate people about protecting their traditional passwords. Managers must establish similar procedures for blockchain keys.

Software flaws. The development of blockchain system software must be treated with the same level of care that professional software developers have established for conventional systems. In the case of the Ethereum breach, it was later decided that an independent software testing firm was needed to review and verify software before it was put into use. Managers everywhere must insist on this before using a blockchain system in their businesses.

Transparency. Reducing the number of software flaws is a start. But other approaches could make extreme transparency less problematic. For Facebook's proposed Libra cryptocurrency, the transparency would be limited to individuals or organizations that have been screened. [13]

Distributed control. Some form of an on-off switch could be incorporated into the blockchain's software. This would require a willingness to be flexible about the traditional "never stop" principle of blockchains.

Anonymity. There are at least two issues here: How can the owner and the private key be recorded safely, and how can we ensure that a private key is never lost? Solving these problems would mean that users have somewhat less anonymity, which might be in order in any case, since regulators already worry about blockchain abuses like money laundering. Here's a stab at a solution: Anyone seeking to use a given blockchain (and to be assigned public/private keys) must be vetted first, and a record of the owner and the private key must be kept in a secure location. If a system like this were put in place, lost keys could be recovered even in the case of a CEO's unforeseen death. Alternatively, management could require that all passwords be stored in a company safe. If the owner of that digital wallet were unavailable, the password could be retrieved.

Immutability. Ideally, managers could agree on how and when data could be removed from a blockchain, though this is likely to be a hard sell given that users regard immutability as an almost sacred principle. A slightly less effective solution would be to prevent undesirable content from getting onto the blockchain in the first place. Some applications allow for unrestricted commenting, which is what led to the so-called Permanent Phallus text image mentioned earlier. Elsewhere, organizations are already taking the obvious step of defining the application such that it does not need such unrestricted content and/or requiring that there be a filter that analyzes and excludes undesired content.

There are great advantages to blockchain systems, [14] but it would be a mistake to overlook their pitfalls. Managers must either minimize the likelihood of abuse or make a conscious decision that the risk of abuse is remote enough to be tolerable.

One notion that Lee and I hope to dispel with our research is that blockchain technology is impervious to human interference. Yes, blockchain represents advances in encryption and security, but it's still vulnerable in some of the same ways other technology is and has new vulnerabilities all its own. Human action or inaction still has significant consequences. It's also important to realize that there are many types of blockchain systems available to managers. In a way, it's like deciding whether you want to buy a less expensive car without extra safety features or a pricier one that you can drive with a greater sense of security. The safety features you might want to choose if you decide to make use of blockchain are the measures highlighted in this article.

About The Author

Stuart Madnick is the John Norris Maguire Professor of Information Technologies in the MIT Sloan School of Management, a professor of engineering systems in the MIT School of Engineering, and codirector of Cybersecurity at MIT Sloan (CAMS).

Acknowledgments

This research was supported, in part, by funds from the members of the Cybersecurity at MIT Sloan (CAMS) consortium.

References

1. C. Mims, "Why Blockchain Will Survive, Even if Bitcoin Doesn't," The Wall Street Journal, March 11, 2018, www.wsj.com.

2. J.H. Lee, "Systematic Approach to Analyzing Security and Vulnerabilities of Blockchain Systems," working paper 2019-05, MIT Sloan School of Management, Cambridge, Massachusetts, February 2019.

3. J. Young, "Bitcoin Researcher Has Bitcoins Stolen From Private Key on Shirt," Bitcoin Magazine, Nov. 13, 2015, https://bitcoinmagazine.com.

4. A. Feinberg, "A TV Anchor Tries to Gift Bitcoin On Air, Is Immediately Robbed," Gizmodo, Dec. 23, 2013, https://gizmodo.com.

5. W. Suberg, "Bitfinex Hack: U.S. Regulation 'Prevented Cold Storage Use,'" Bitcoin.com, Aug. 3, 2016, https://news.bitcoin.com.

6. M. Jarzemsky and M. Driscoll, "New Circuit Breakers Would Have Halted 'Flash Crash,'" The Wall Street Journal, June 1, 2012, https://blogs.wsj.com.

7. C. Cimpanu, "Cryptocurrency Startup Hacks Itself Before Hacker Gets a Chance to Steal Users Funds," ZDNet, June 6, 2019, www.zdnet.com.

8. In reality, blockchain systems provide pseudonymity rather than anonymity. That is because nodes (users) in a blockchain system are disguised but still need to fully or partially identify themselves to interact outside the system — for instance, when they register in a cryptocurrency exchange. Princeton University researchers found that 53 out of 130 web merchants that accept cryptocurrency have routinely leaked end users' identifiable data in the form of a cookie (also known as a session ID).

9. M. Kan, "Cryptocurrency Exchange Locked Out of Funds After CEO's Death," PCMag.com, Feb. 1, 2019, www.pcmag.com.

10. N. Eriksson, "10 Dramatic Stories of People Who Lost Their Bitcoin Private Keys," Coinnounce, Feb. 12, 2019, https://coinnounce.com.

11. "Child Abuse Images Hidden in Cryptocurrency Blockchain," BBC News, Feb. 6, 2019, www.bbc.com.

12. S. Madnick, "How Companies Can Create a Cybersafe Culture at Work," The Wall Street Journal, May 29, 2018, www.wsj.com.

13. S. Levy and G. Barber, "The Ambitious Plan Behind Facebook's Cryptocurrency, Libra," Wired, June 18, 2019, www.wired.com.

14. E. Griffith, "187 Things the Blockchain Is Supposed to Fix," Wired, May 25, 2018, www.wired.com.

What Makes Blockchain Different

To understand why blockchain's highly touted features are so prized by users, let's compare a blockchain system with a traditional, centralized record-keeping system, like the one your bank might use to keep track of your balances.

FEATURE	TRADITIONAL SYSTEM	BLOCKCHAIN SYSTEM
Transparency	The database holding the account ledger is locked away in the bank's central computer system. Likewise, the software used is carefully guarded and not generally available to the public.	The blockchain ledger becomes highly visible by being distributed and copied onto hundreds, or even thousands, of computers operated by many different organizations. The software is made publicly available because it needs to run on all these servers.
Distributed Control	The central computer processes all the transactions and makes the necessary alterations to the account ledger.	Each copy of the blockchain ledger has a server that processes it. The same software is used across servers, and the consistency of all copies is assured via a verification process.
Anonymity	Usually, you need to identify yourself when you open a bank account. You're also asked to choose a password to access your account.	Each user has a private key, and that's all that is needed to operate on the blockchain. The private key is a 256-bit number (approximately 78 digits) and likely impervious to being guessed.
Immutability	When you make deposits or withdrawals, your balance changes. Separate transaction records may be kept, but they are not a part of the account ledger.	Nothing is ever changed or deleted in a blockchain — only additions are allowed. The account balance at every point in time is preserved.