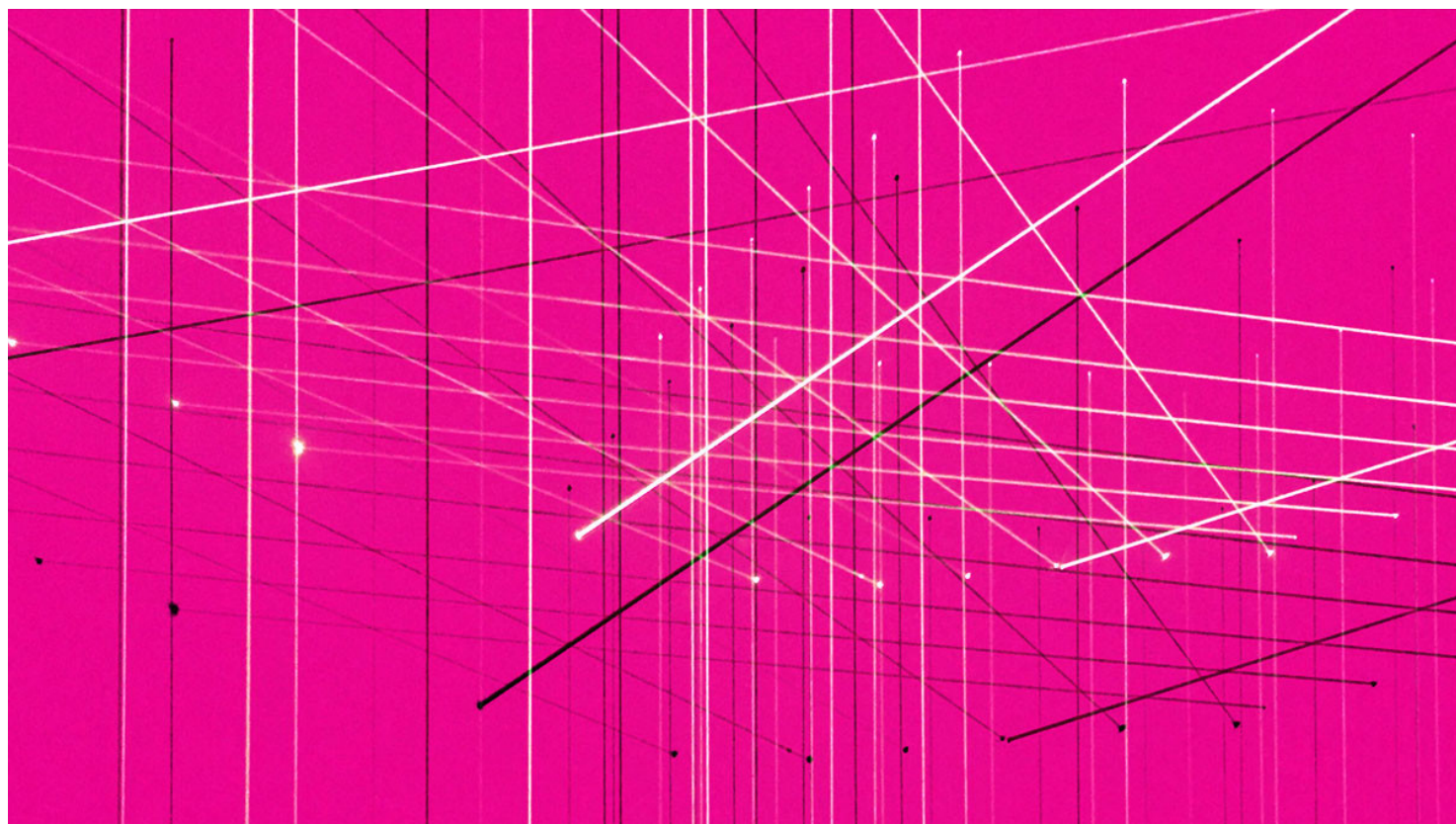


# How Safe Are Blockchains? It Depends.

by Allison Berke

MARCH 07, 2017



Blockchain, the distributed ledger technology underlying bitcoin, may prove to be far more valuable than the currency it supports. But it's only as valuable as it is secure. As we begin to put distributed ledger technology into practice, it's important to make sure that the initial conditions we're setting up aren't setting us up for security issues later on.

To understand the inherent security risks in blockchain technology, it's important to understand the difference between public and private blockchains.

## How Blockchain Works

Here are five basic principles underlying the technology.

### 1. Distributed Database

Each party on a blockchain has access to the entire database and its complete history. No single party controls the data or the information. Every party can verify the records of its transaction partners directly, without an intermediary.

### 2. Peer-to-Peer Transmission

Communication occurs directly between peers instead of through a central node. Each node stores and forwards information to all other nodes.

### 3. Transparency with Pseudonymity

Every transaction and its associated value are visible to anyone with access to the system. Each node, or user, on a blockchain has a unique 30-plus-character alphanumeric address that identifies it. Users can choose to remain anonymous or provide proof of their identity to others. Transactions occur between blockchain addresses.

Bitcoin relies on a public blockchain, a system of recording transactions that allows anyone to read or write transactions. Anyone can aggregate and publish those transactions, provided they can show that a sufficient amount of effort went into doing so, which they can demonstrate by solving a difficult cryptographic puzzle. The process by which a network of nodes confirms the record of previously verified transactions, and by which it verifies new transactions, is known as a consensus protocol. In the bitcoin system, because no user is implicitly trusted to verify transactions, all users follow an algorithm that verifies transactions by committing software and hardware resources to solving a problem by brute force (i.e., by solving the cryptographic puzzle). The user who reaches the solution first is rewarded, and each new solution, along with the transactions that were used to verify it, forms the basis for the next problem to be solved.

#### **4. Irreversibility of Records**

Once a transaction is entered in the database and the accounts are updated, the records cannot be altered, because they're linked to every transaction record that came before them (hence the term "chain").

Various computational algorithms and approaches are deployed to ensure that the recording on the database is permanent, chronologically ordered, and available to all others on the network.

#### **5. Computational Logic**

The digital nature of the ledger means that blockchain transactions can be tied to computational logic and in essence programmed. So users can set up algorithms and rules that automatically trigger transactions between nodes.

This decentralization and relative freedom of access has led to some unexpected consequences: Because anyone can read and write transactions, bitcoin transactions have fueled black market trading. Because the consensus protocol is energy consuming, the majority of users operate in countries with cheap electricity, leading to network centralization and the possibility of collusion, and making the network vulnerable to changes in policy on electricity subsidies. Both of these trends have led to an increased interest in private blockchains, which could ultimately give businesses a greater degree of control.

Primarily used in financial contexts, private blockchains give their operators control over who can read the ledger of verified transactions, who can submit

transactions, and who can verify them. The applications for private blockchains include a variety of markets in which multiple parties wish to participate simultaneously but do not fully trust one another. For example, private blockchain systems supporting land and physical asset registries, commodities trading, and private equity distribution are all being tested. As these systems develop and evolve, they, too, may encounter unexpected consequences, some of which will have repercussions for the security of the system and the assets it

manages or stores. As in software and product development, considering security at an early stage alleviates the difficulty of making fundamental changes to a product to address a security flaw later on.

## **Security Starts with Network Architecture**

One of the first decisions to make when establishing a private blockchain is about the network architecture of the system. Blockchains achieve consensus on their ledger, the list of verified transactions, through communication, and communication is required to write and approve new transactions. This communication occurs between nodes, each of which maintains a copy of the ledger and informs the other nodes of new information: newly submitted or newly verified transactions. Private blockchain operators can control who is allowed to operate a node, as well as how those nodes are connected; a node with more connections will receive information faster. Likewise, nodes may be required to maintain a certain number of connections to be considered active. A node that restricts the transmission of information, or transmits incorrect information, must be identifiable and circumventable to maintain the integrity of the system. A private blockchain underlying commodities trading may grant more-central positions in the network to established trading partners, and may require new nodes to maintain a connection to one of these central nodes as a security measure to ensure it behaves as expected.

---

**INSIGHT CENTER**

**Business in the Era of Blockchain**

**SPONSORED BY ACCENTURE**

How technology is transforming transactions.

---

Another security concern in the establishment of network architecture is how to treat uncommunicative or intermittently active nodes. Nodes may go offline for innocuous reasons, but the network must be structured to function (to obtain consensus on previously

verified transactions and to correctly verify new transactions) without the offline nodes, and it must be able to quickly bring these nodes back up to speed if they return.

## **Consensus Protocols and Access Permissions in Public vs. Private Blockchains**

The process used to get consensus (verifying transactions through problem solving) is purposely designed to take time, currently around 10 minutes. Transactions are not considered fully verified for about one to two hours, after which point they are sufficiently “deep” enough in the ledger that introducing a competing version of the ledger, known as a fork, would be computationally expensive. This delay is both a vulnerability of the system, in that a transaction that initially seems to be verified may later lose that status, and a significant obstacle to the use of bitcoin-based systems for fast-paced transactions, such as financial trading.

In a private blockchain, by contrast, operators can choose to permit only certain nodes to perform the verification process, and these trusted parties would be responsible for communicating newly verified transactions to the rest of the network. The responsibility for securing access to these nodes, and for determining when and for whom to expand the set of trusted parties, would be a security decision made by the blockchain system operator.

## **Transaction Reversibility and Asset Security in Public vs. Private Blockchains**

While blockchain transactions can be used to store data, the primary motivation for bitcoin transactions is the exchange of bitcoin itself; the currency’s exchange rate has fluctuated over its short lifetime but has increased in value more than fivefold over the past two years. Each bitcoin transaction includes unique text strings that are associated with the bitcoins being exchanged. Similarly, other

blockchain systems record the possession of assets or shares involved in a transaction. In the bitcoin system, ownership is demonstrated through the use of a private key (a long number generated by an algorithm designed to provide a random and unique output) that is linked to a payment, and despite the value of these keys, like any data, they can be stolen or lost, just like cash. These thefts are not a failure of the security of bitcoin, but of personal security; the thefts are the result of storing a private key insecurely. Some estimates put the value of lost bitcoins at \$950 million.

Private blockchain operators therefore must decide how to resolve the problem of lost identification credentials, particularly for systems that manage physical assets. Even if no one can prove ownership of a barrel of oil, the barrel will need to reside somewhere. Bitcoin currently provides no recourse for those who have lost their private keys; similarly, stolen bitcoins are nearly impossible to recover, as transactions submitted with stolen keys appear to a verifying node to be indistinguishable from legitimate transactions.

Private blockchain owners will have to make decisions about whether, and under what circumstances, to reverse a verified transaction, particularly if that transaction can be shown to be a theft. Transaction reversal can undermine confidence in the fairness and impartiality of the system, but a system that permits extensive losses as a result of the exploitation of bugs will lose users. This is illustrated by the recent case of the DAO (Decentralized Autonomous Organization), a code-based venture capital fund designed to run on Ethereum, a public blockchain-based platform. Security vulnerabilities in the code operating the DAO led to financial losses that required Ethereum's developers to make changes to the Ethereum protocol itself, even though the DAO's vulnerabilities were not the fault of the Ethereum protocol. The decision to make these changes

was controversial, and underscores the idea that both public and private blockchain developers should consider circumstances under which they would face a similar decision.

## **Weighing the Rewards**

The benefits offered by a private blockchain – faster transaction verification and network communication, the ability to fix errors and reverse transactions, and the ability to restrict access and reduce the likelihood of outsider attacks – may cause prospective users to be wary of the system. The need for a blockchain system at all presupposes a degree of mistrust, or at least an acknowledgement that all users' incentives may not be aligned. Developers who work to maintain public blockchain systems like bitcoin still rely on individual users to adopt any changes they propose, which serves to ensure that changes are only adopted if they are in the interest of the entire system. The operators of a private blockchain, on the other hand, may choose to unilaterally deploy changes with which some users disagree. To ensure both the security and the utility of a private blockchain system, operators must consider the recourse available to users who disagree with changes to the system's rules or are slow to adopt the new rules. The number of operating systems currently running without the latest patch is a strong indication that even uncontroversial changes will not be adopted quickly.

While the risks of building a financial market or other infrastructure on a public blockchain may give a new entrant pause, private blockchains offer a degree of control over both participant behavior and the transaction verification process. The use of a blockchain-based system is a signal of the transparency and usability of that system, which are bolstered by the early consideration of the system's security. Just as a business will decide which of its systems are better hosted on a more secure private intranet or on the internet, but will likely use both, systems requiring fast transactions, the possibility of transaction reversal,

and central control over transaction verification will be better suited for private blockchains, while those that benefit from widespread participation, transparency, and third-party verification will flourish on a public blockchain.

Allison Berke is the executive director of the Stanford Cyber Initiative.

This article is about TECHNOLOGY

 FOLLOW THIS TOPIC

Comments

Leave a Comment



POST


6 COMMENTS

Toby Adams 3 months ago

An organization dedicated to hacking services, helping people recover their stolen coins, binary options schemes, stolen bitcoin, litecoin and so on...look onto DarkWeb. They came through for me in great time. visit darkwebsolutions dot co for more on this

REPLY

1  0 

 JOIN THE CONVERSATION



## **POSTING GUIDELINES**

We hope the conversations that take place on HBR.org will be energetic, constructive, and thought-provoking. To comment, readers must sign in or register. And to ensure the quality of the discussion, our moderating team will review all comments and may edit them for clarity, length, and relevance. Comments that are overly promotional, mean-spirited, or off-topic may be deleted per the moderators' judgment. All postings become the property of Harvard Business Publishing.