Public vs. Private Blockchains: 3 Considerations to Help Businesses and Employers Decide the Best Option

Insights
3.01.22

As cryptocurrency continues to enter the mainstream, many businesses and employers are trying to understand how to implement blockchain technology at their organizations – and one of the most important choices they'll have to make at outset is whether to proceed with a public or private blockchain. Whether you are contemplating using a blockchain to strengthen security, eliminate inefficiencies, retool your recruiting and onboarding processes, or compensate employees, there are pros and cons to each choice. Each organization will need to assess their own business needs before making a selection. This Insight will review the prime features of public and private blockchains and provide three considerations to keep in mind before making a choice.

Primer: What is a Blockchain?

As a quick refresher, a blockchain is a distributed (shared) digital ledger that contains an immutable historical record – or chain – of all transactions that have occurred on that blockchain's network. A distributed ledger means that there are multiple versions of the same data that are stored in different places and connected through the network.

A blockchain stores information together in "blocks" of information. When a block reaches its storage capacity, it is closed and linked via cryptography to the prior block and each block is chained in chronological order. This creates the chain of data known as the "blockchain." You can dive deeper into this concept by reading our detailed FAQs here.

The most common reasons businesses and employers might consider using blockchain technology include enhancing security for financial data and sensitive personal employee information, improving the recruiting and onboarding processes, streamlining payroll, or increasing the efficiency and reliability of current audit processes. And the two most common blockchains are public and private blockchains.

Public Blockchains

A public blockchain, such as Bitcoin's blockchain, is "permissionless." This means that the blockchain is visible to anyone and open to public participation. Key features of a public blockchain include:

Copyright © 2025 Fisher Phillips LLP. All Rights Reserved.

- **Access**: Public blockchains are decentralized, which means that anyone can join and participate in the blockchain network. Similarly, anyone can read, write, and see the activities on the public network. A public blockchain does not have a single entity that controls the network.
- **Identity**: Users of a public blockchain are pseudonymous because the users are not identified by typical identifying information. Rather, users of a public blockchain are identified by their wallet address.
- **Speed**: Transactions on public blockchains are slower compared to a private blockchain because of their decentralized governance mechanisms and because of the potentially unlimited number of users trying to facilitate transactions on the blockchain.
- **Governance**: The rules for a public blockchain cannot be set by a single centralized entity. Similarly, there is no single entity that can shut down the network.
- **Security**: A public blockchain is more secure and less vulnerable to hacks. Due to the large number of nodes (computers that have a complete copy of the blockchain) there is not a single point of failure (i.e., if a particular part of a system fails, the entire system will stop working).

Private Blockchains

A private blockchain is run by a centralized entity and its use is restricted to those who have been granted access. In order words, a private blockchain is a closed ecosystem that is not open for public participation. Participants must first obtain authorization from the centralized authority before they can use the private blockchain. Key features of a private blockchain include the following:

- **Access**: Private blockchains are centralized, which means users need permission to access the blockchain (although members of the chain can negotiate the level of decentralization that the network can have). In addition, private blockchains can provide varying levels of access to users and can enact customized restrictions based on the user, the information being stored, or any other characteristic deemed appropriate. Private blockchains are attractive to entities that want to be selective in determining who can access the information stored on the blockchain, and the degree of access provided.
- **Identity**: Users of private blockchains cannot obtain entry to the blockchain until they are granted access by the central entity controlling the blockchain. This means that each participant on the blockchain can be easily identified.
- **Speed**: Transactions on private blockchains are much faster than on public blockchains because of its centralized nature.
- **Governance**: The central authority for the private blockchain sets the rules to be followed by the users of the blockchain.
- **Security**: A private blockchain is more vulnerable to hacks because it is centralized and can be targeted more easily. A private blockchain with a centralized single authority also creates a

Copyright © 2025 Fisher Phillips LLP. All Rights Reserved.

single point of failure.

3 Considerations for Businesses and Employers

Whether to use a public or private blockchain is not a one-size-fits-all approach and will depend on your needs. Three things you should consider before making your selection:

1. **Confidentiality**: Do you want to utilize blockchain technology for transactions containing proprietary, sensitive, or confidential information? For example, would you be comfortable using a public blockchain for the transfer and storage of employee medical information, personnel records, personal identifying information, business records, trade secrets, or intellectual property?

   Depending on the nature of the information, businesses may have concerns with using a public blockchain. As a reminder, anyone using a public blockchain can view your transactions. While there are options to keep such information secure, such as encryption and even using NFTs, you may not feel comfortable transferring or storing this information on a public blockchain – especially if inadvertent disclosure could run afoul of privacy laws, healthcare laws, or the terms of confidentiality agreements. Private blockchains may provide advantages to companies that want to have more control over data and privacy with specific permission controls.

   However, private blockchains pose their own risks for businesses, especially those operating in highly competitive markets. For example, given that the business that owns the private blockchain controls access and sets the rules, users of a private blockchain risk locking themselves into a poor solution (as most private blockchains have fees or are subscription based), relinquishing control of potentially competitive data, and being at the mercy of the entity that sets the rules. In addition, once participants are locked in, the platform owner could potentially refuse to do business going forward unless the user accepts new terms and conditions.

2. **Speed and Congestion:** All businesses need to pay their employees and payroll is often the largest expense for many companies. Blockchain technology has the potential to dynamically impact the payroll process. Currently, the payroll process requires many manual, tedious, repetitive and time-consuming tasks. Blockchain technology, however, can eliminate time delays and increase the speed of the entire process through smart contracts. When considering the resources and time that is expended handling payroll, the ability to efficiently and securely enhance the speed of this process is significant. The question then becomes, which blockchain should you use?

   A private blockchain can generally handle hundreds or thousands of transactions per second. In comparison, certain public blockchains can handle fewer than 20 transactions per second. As the number of users vying for block space on public blockchains continues to increase, there has been increased congestion – which can hinder transaction speed and functionality.

Copyright © 2025 Fisher Phillips LLP. All Rights Reserved.

Given that private blockchains can limit the number of total users and also impose transaction restrictions, the functionality of private blockchains should not suffer from the same congestion issues. However, in exchange for speed, private blockchains sacrifice decentralization, and the resulting level of security that is provided by decentralized blockchains. This results in greater exposure to hacks, malicious attacks, and network failures.

3. **Auditing:** Let's face it, audits of any kind can be intimidating and stressful. A government agency shows up unannounced and requests that a business provide records for several years back and often covering a variety of categories, including financial records, payroll documents, and records related to employee tax withholdings. Trying to collect and compile this information can be a heavy load and a company's failure to provide the requested information in a timely manner can result in a significant penalty for businesses. Blockchain technology can be extremely useful as it can quickly and securely share records with auditors while drastically reducing the cost of document collection. Moreover, because the information is secured on the blockchain, the chances that the documents have been fraudulently altered or manipulated is significantly reduced. Public blockchains can provide the benefit of better security and reliability because of its decentralized nature. However, will auditors be familiar with how to utilize a public blockchain and access the records? Would you want to keep these records on a public blockchain? Can you lawfully keep the records that would be subject to a government audit on a blockchain? These are all issues you would need to evaluate.

   On the other side, government agencies may have an easier time accessing a private chain as someone within the organization could provide specific instructions on where and how to locate the information. Similarly, if an auditor needs to review information related to transactions performed by a specific individual, it would be easier to identify individuals on a private blockchain than a public blockchain because each user of a private blockchain will be known by the controlling authority. However, would an auditor trust the authenticity of the records given its centralized nature? Would you want to keep your data on a centralized blockchain given that cyberattacks are heavily on the rise and there is a single point of failure? All it takes is one careless employee and your entire system could be brought down. While some of these issues exist with current technology, would you choose to continue assuming those risks when other options exist? Again, these are issues you will need to consider.

What's Next?

We believe the use of blockchain technology by businesses will continue to increase with time. Employers considering whether to use a public or private blockchain should analyze their company's needs in comparison to the benefits provided by each blockchain. Substantive evaluation with a combination of your core business personnel, legal counsel familiar with these issues, and individuals or entities that comprehensively understand the technical aspects of implementing blockchain for business use cases is recommended to help evaluate which path may be right for you.

Copyright © 2025 Fisher Phillips LLP. All Rights Reserved.

We'll continue to monitor developments in this area, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information. If you have any questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our Cryptocurrency and Blockchain Taskforce.

Related People

Phillip C. Bauknight
Partner
908.516.1059
Email

Copyright © 2025 Fisher Phillips LLP. All Rights Reserved.