

8 critical questions to ask before investing in blockchain solutions

As part of his longstanding and extensive experience with Bitcoin and blockchain, *Simon Ousager* has witnessed first hand the successes, but also the profiteering, unfulfilled promises and failed projects that have shaped the landscape of this emerging technology to date. He has developed a list of eight critical questions that he believes all organisations with respect for their professional integrity and economic sensibility should be able to answer before they write, or pay for, one-line of blockchain code.

1. What is the problem you are trying to solve?

Regardless of the technology, the first place to begin is to truly understand the problems and challenges that require solutions. From there, framing a specific problem to be addressed, understanding its complexities, pain points, needs and requirements will provide a use case.

Those creating the technology are not the experts in your field or your industry and they are only as good as the information they receive. Creating a thorough analysis of the problem to be solved will serve to assess the feasibility of a concrete technical solution as well as the road map, and will avoid wasting time and money on deploying technology simply for technology's sake.

2. What is a blockchain?

Beginning with the definition of a blockchain being a shared database with protocols that govern what actors can and cannot do within the database, it is important that you start by building from there and asking what a blockchain is to you and what type of blockchain has the characteristics that are relevant to your use case. As mentioned, there are several types of blockchains and protocols and although it might not make sense at first, it is the responsibility of the project owner to ensure these questions are investigated until it does.

3. What features do you need from a database?

Defining the critical features that are needed will determine what Blockchain or Bitcoin solution is needed, if any at all. Databases are not new and they come in all forms. In fact, secure and relational databases have been around for decades and are a proven technology. These databases can also be distributed and shared, read/write permissions may be granted and applications can be built on top of them. It is how most of our enterprise IT infrastructure has been built thus far.

So you need to know why exactly you are using a database, and what properties are currently missing from the traditional databases that blockchain may provide. These properties include requiring multiple writers, sharing access with public and private keys and creating trust in a trustless system, to name a few. Likewise, if what you are looking for is a technology that can facilitate value transfer and the issuance of digital tokens that represent that value, then you may not have to look any further than Bitcoin.

4. Who should validate your blockchain?

Blockchains require a so-called consensus protocol. The consensus mechanism that underpins this protocol varies from one blockchain system to the next and could be confirmed by a percentage of the validators, a group, or all members of the network (usually referred to as nodes). In short, we want to



8 critical questions to ask before investing in blockchain solutions

agree who can carry out transactions, as well as who has transferred what to whom and when they have done it. But who should ultimately validate this blockchain and list of transactions? One of the defining features of blockchains is precisely that they are distributed, so until this question is answered properly, you are probably buying a database and not a blockchain.

5. Would your blockchain be transparent?

If we are to be able to achieve consensus, with validators able to see and validate all other transactions, they will need access to all information, all the time in order to do so. Additionally, the implementation of public and private keys and digital signatures is what controls who can do what and what is shared with whom. Asking yourself whether you are actually interested in this high level of transparency that gives your financial counterparties full insight into your activities, is critical. In addition, defining the level of transparency, roles and who can see what is key to interoperability and integrity.

6. How do you define 'blocks' and 'chains'?

A block itself is a data container that can store millions of transaction entries and a few data points such as a timestamp and a 'hash' (or chainlink) that securely chains it to the previous block of transactions. As the chain serves to reference directly to transactions in previous blocks, a streamlined set of transactional data is created. If one were to update the transaction data, one would need to add another transaction in a block and append it to the previous chain of blocks.

Because this is cryptographically secured, you cannot update or change the data stored without breaking the cryptographic link. Therefore, ask yourself whether or not immutability and chain of custody of your data is a requirement, otherwise appending corrections to your chain may become a resource intensive task with little pay off.

7. How would censorship rights be handled on your blockchain?

Blockchain requires special rights to execute censorship on a shared platform and a clear definition of these rights is therefore a prerequisite for all private systems to handle value transfers and administration of these rights.

As a company or consortium, you will still need to decide when transactions can be corrected or cancelled, under what conditions this can be done and how to achieve consensus among all validators in the common blockchain when transactions are changed. This requires decision making between all stakeholders to agree upon the terms prior to implementation.

8. Who will control the keys to your blockchain?

The most important and often overlooked question you should be able to answer is about something as basic as passwords, identities and rights. Ultimately what is at stake is the security of your system; what public and private keys control user rights, account holdings, system updates, censorship etc.

The moment we begin to place our trust in decentralized blockchain platforms instead of third parties, the administration and management of these digital keys and signatures are also important as they relate to the question of who has the authority to suggest, dictate or implement a solution to the problem.