CompTIA Blockchain Advisory Council

WHEN IS BLOCKCHAIN OR ANOTHER DATABASE THE RIGHT CHOICE?

TABLE OF CONTENTS

1. IS THERE A NEED FOR A TRUSTED CENTRAL AUTHORITY?

The lack or elimination of a trusted central authority is a fundamental principle of blockchain. Blockchain was designed to be a trustless system which means that trust is not necessary to transactions or entries to the blockchain. Every transaction is independently verified via a mathematical consensus algorithm which eliminates the need for involved parties, or third parties, to trust each other. Its decentralized, peer-to-peer architecture can lead to a solution that is low-cost and offers quicker settlement.

If a use case can dispense with the trusted central authority, blockchain might be a good choice as it will optimize the business process by increasing the settlement speed, reducing errors and lowering operational costs, which may require redesigning the process workflow to best utilize blockchain properties to fulfill these goals.

2. IS THERE A NEED FOR HIGH PERFORMANCE (OVER TPS 1,000)?

The algorithms at the core of blockchain transaction are slow. Bitcoin's average transaction rate is 7 transactions per second (TPS), and the time to confirm a transaction can take from 10 minutes up to 6 hours. For comparison, high performance database clusters are capable of up to 1M queries/second. There are emerging blockchains that are claiming transaction rates up to 300,000 TPS, but these high transaction rates come at significant costs that are not practical for most applications. If an application requires less than 1,000 TPS blockchain may be a suitable solution for the application.

3. IS THERE A NEED TO CAPTURE MASSIVE AMOUNTS OF DATA?

Blockchain does not support large datasets (on chain). When considering data storage on blockchain there are three major factors to consider size, transaction cost, and performance.

3A. SIZE

As a point of reference, Bitcoin's block size is limited to 1MB and a typical MP3 song is closer to 3.5MB in size. The reason is because blockchain ledgers are duplicated on thousands of computers around the world, most of which are not industrial grade, so blockchain files would grow to unsupportable sizes if the data per transaction was not limited.

3B. TRANSACTION COST

It is possible to divide files into smaller pieces on-chain. However, that will not only not solve the problem because the total file would still be the same size, it would also increase transaction cost. Every transaction written to a public chain requires a "gas" fee to pay the minors (or validators). Large databases typically imply high transaction rates to begin with, and the cost of posting data on blockchain is significantly higher than writing traditional databases.

3C. PERFORMANCE

Performance is significantly impacted when writing to blockchain. For example, Bitcoin on average handles 7 TPS and Ethereum about 15, while VISA operates around 15,000 to 25,000 TPS.

There are strategies using permissioned blockchains, since they are run on fewer servers and there are no gas fees, that can improve cost, performance and speed for data storage. One such strategy is to only store write transaction hashes on blockchain while leaving the raw data in a traditional database. However, such an architecture adds complexity to the system and transaction speed is still significantly slower than the best standard database.

If data storage needs are small or large datasets can be stored off-chain, blockchain may be a suitable solution for the application.

4. DO ONE OR MORE PARTIES NEED TO BE ABLE TO MODIFY ENTRIES?

Blockchain is a multi-node database maintained by a network of independent participants and so it is decentralized with no single user having the ultimate authority. Once a transaction is written on the blockchain framework, it is immutable and available for viewing to all authorized users. Conceptually, blockchain consists of blocks of data that form a chain from the past to the present. Fundamentally, blockchain entries (transactions) cannot be modified. The only way to "modify" a previous entry is to add an adjusting entry, much like any double entry accounting system, which is why blockchain is part of a class of solutions called distributed ledger technology (DLT).

If the use case requires deletion or modification of entries, blockchain is not a good solution.

5. IS THERE A NEED FOR A PERSISTENT HISTORICAL TRANSACTION RECORD?

Blockchain offers inherent historical records as every transaction is immutably written to the ledger. An alternative is a data warehouse, but the difference is that the ETL transfer process from the original database to the warehouse often transforms the data from its original form, so it is representation of the original data, but not a true record. As each transaction is written immutably, tracking chain of custody (ownership from raw materials to customers) and provenance (information about how the product was produced), which are critical to many products that are produced today, are strong use cases for blockchain. ~~Many are required by law for products such as~~ firearms, cannabis, aircraft maintenance records, pharmaceuticals, military products and others.

There are other industries where knowledge about a product during its lifecycle ~~was manufactured that~~ could benefit greatly from this type of information. A classic example is tracking food from farm to customer so that sources of contamination can be quickly identified, reducing the risk to the consuming public. In the case of flight safety parts (landing gear for example), their value increases significantly if the entire chain of custody and provenance is known for that part. Another example is equipment in the oil drilling industry where approximately 15% of piping is counterfeit.

If the use case requires a persistent historical record of the original transactions or entries, blockchain may be a good solution.

6. DO MULTIPLE PARTIES NEED TO BE ABLE TO ACCESS OR AUDIT DATA?

Sharing data with other parties is not always easy to execute in a secure and trusted manner, blockchain technology can provide the means to this. Providing access to data ~~maybe~~ valuable in creating efficiencies with partners and could also open doors to new revenue streams. Additionally, in situations in which a party may need to conduct an audit, blockchain allows them to trust the data is unaltered. Audits around regulation, legislation or process are data points which blockchain can assist in creating an immutable audit trail. This can reduce audit and compliance cost while increasing trust.

7. ARE CONTRACTUAL RELATIONSHIPS OR VALUE EXCHANGES BEING MANAGED?

A smart contract is simply computer code that, upon the occurrence of some specified condition, is capable of running automatically according to pre-specified functions. Whether a smart contract is legally binding depends on whether it fulfills the legal elements of a contract. In the US, that means there must be (1) an offer; (2) acceptance of that offer; and (3) the exchange of consideration between the parties to the contract. Generally speaking, smart contracts fall into one of two buckets: internal and external. Internal smart contracts

encompass the entire agreement between parties, or the entirety of a discrete part (clause) of that agreement. External smart contracts, by contrast, merely automate the performance of certain terms of a contract which exists in some other (conventional) form.

Whether blockchain technology is suitable for a given contractual relationship will vary on the nature of that relationship. For instance, contracts for the automatic or irrevocable performance of certain services (say, mortgages or other installment payments), especially those involving hundreds or thousands of parties, may be very well-served by either internal or external smart contracts. Each component transaction to the contract will be immutably and securely recorded on the distributed ledger. On the other hand, if it is important that the contract be easily amended or modified, or if the meaning of certain material terms is expected to change over the life of the contract, smart contracts (and especially internal smart contracts) may be less suitable. There are potential workarounds, such as coding a smart contract to check for superseding smart contracts, but the utility of an internal smart contract for such purposes will be limited absent the development of mechanisms allowing parties to address changed circumstances. Moreover, many commercial contracts incorporate equitable concepts such as "good faith" or "best efforts," which seem particularly ill-suited to pre-defined automatic performance. Indeed, with limited exceptions, every contract executed under U.S. law is deemed to include an implied covenant of good faith and fair dealing. There is a natural tension between the flexibility of such a concept and the deterministic nature of the distributed ledger.

If the business case can be stated in clear, simple terms that do not require human judgement and does not need to be modified during its lifecycle, blockchain may be a good solution.

8. CAN BUSINESS PROCESS BE REPRESENTED BY CONDITIONAL LOGIC?

Programming languages for smart contracts on blockchain, such as Solidity for Ethereum, are essentially a series of if/then statements (i.e., conditional logic) which are executed based on an event. Programs written in those languages can be very simple or very complex, but, in the end, conform to standard programming structures.

If the business process has a number of stop points, e.g., for approvals, or requires any kind of judgement or fuzzy logic, smart contracts are not likely to be sufficient.

The more complex and the more the code relies on external sources for inputs or variables, the more vulnerable they are to external attacks. There are companies that audit smart contracts for vulnerabilities and any enterprise application should have its smart contracts audited.

If the business process can be translated into conditional logic, blockchain may be a good solution.

9. IS THERE A NEED TO CENTRALLY OWN APPLICATION FUNCTIONALITY?

Anyone with permission to access a blockchain (see below for more on permissioned vs. permissionless blockchains) can create an application to read or write to the blockchain. Therefore, if application functionality needs to be centrally controlled, not allowing for user created functions or unauthorized application development, then blockchain is unlikely to be a good fit.

However, if permissioned users can be free to develop their own applications, blockchain may be a suitable solution for the application.

10. CAN TRANSACTIONS BE PUBLIC BUT HASHED?

There is a strong debate in the blockchain community as to whether permissioned blockchains are actually blockchains in the purest sense as opposed to an alternate implementation of distributed ledger technology. Of course, the technology is the same, but one of the prime blockchain values is that they are transparent. Anyone should be able to read and write to the blockchain. Obviously, permissioned blockchains to do not allow for this. There are several good reasons for using permissioned blockchains, but one misconception is that just because the transactions are publicly readable, that they are not secure. All information on the blockchain can be hashed and identity independent. Cryptowallets provide any owner with a private key for encryption so any information within a transaction hashed with a public key derived from that private key is only available to whoever holds the private key. While a third party could identify a wallet (via its publicly available address) and all transactions using that wallet, the wallet cannot be associated with an individual because no unencrypted private information (e.g., SSN, email address, phone number, etc.) is part of the transactions.

Therefore, if an application's encrypted transactional information can be publicly available, a public blockchain may be a suitable solution as it would reduce cost (e.g., hardware, maintenance, labor) and allow for independent innovation.

11. UNDER 30 TPS OK?

If an application requires less than 15 TPS, blockchain may be a suitable solution for the application. If an application requires less than 1,000 TPS blockchain, permissioned blockchain or public/permissioned hybrid may be a suitable solution for the application.

12. IS THERE A SPECIALIZED WORKLOAD?

Applications with unique computational or data models sometimes require databases that do not fit with existing solutions. In these cases, customized solutions could incorporate multiple different database types, potentially including blockchain. These types of applications will need to be evaluated on a case-by-case basis.

13. IS THE DATA STRUCTURED?

Each non-blockchain database is designed to handle different types of data storage and retrieval. One significant differentiation is whether the data being stored has a rigid, defined structure (data models with unique keys connecting tables) or unstructured (storing various file types – pdfs, images, etc. – data lakes, etc.). NoSQL databases are designed to handle unstructured data while RDBMS (relational database management systems) are best for structured data.

14. IS THERE A NEED TO SCALE FOR SIZE OR PERFORMANCE?

Once it's been determined that an RDBMS is the best database, the question becomes what is most important to optimize – size or performance. If the application needs to be optimized for performance, a traditional, locally hosted RDBMS is likely the best choice, while if the application needs to be optimized for database size, where local storage could become an issue, a cloud or distributed RDBMS would likely be the best choice.

15. PUBLIC (PERMISSIONLESS) VS. PRIVATE (PERMISSIONED) VS. HYBRID BLOCKCHAINS

15A. WHY USE A PUBLIC (PERMISSIONLESS) BLOCKCHAIN?

Bitcoin and Ethereum are examples of projects that use public permissionless blockchains. When using a public permissionless blockchain, anyone, or any organization, can join the project, use its cryptographic keys, become a node, review all transactions, write new blocks to the chain, participate in the consensus process and be rewarded for their efforts. Public blockchains are considered to be decentralized and largely censor-proof as no single entity has control over them.

Public permissionless blockchains represent an excellent choice when community members can offer up underutilized assets to grow and scale a network, when looking to prevent an entity, or even small group of entities, from taking control over the network, and when looking to incentivize others to join the community to participate in the network. Essentially, entities offer assets like underutilized computational power, storage capacity, and/or network bandwidth and in return they are offered coins, tokens, or other equivalents.

Public blockchains would not be optimal in cases where control is necessary, network consistency is required, or high transaction volumes are critical. Just as easily as an individual, or organization, can join the network, they can also leave which can impact network consistency. Today's public blockchain technologies are largely limited to ~~less~~ than 10,000 transactions per second (TPS), however, this limitation is being addressed by the community and will likely become less of an issue as the technology matures.

15B. WHY USE A PRIVATE (PERMISSIONED) BLOCKCHAIN?

Hyperledger is an example of an umbrella project consisting of permissioned blockchains and tools that can be leveraged privately by organizations that would like the benefits of using blockchain technology without relinquishing control. When using a private permissioned blockchain, an enterprise can use its own cryptographic keys, determine which infrastructure, partners, or other third parties are allowed to participate in the network, determine what type of infrastructure can be used and for which node roles, determine which entities or nodes can read, write or have full access to the blockchain, and determine the incentive program for participating. Private permissioned blockchains are centralized and controlled by the entity that commissions the blockchain.

Private permissioned blockchains represent an excellent choice when an entity would like to control which individuals or organizations can participate in the network and in what capacity. For example, an enterprise may allow all transacting entities in its ecosystem to take part in consensus and add blocks to the chain, yet only allow members of audit ecosystem to read, but not write, to the digital ledger. This approach allows enterprises to leverage blockchain technology while simultaneously maintaining required controls, reducing business risk and complying with relevant regulations.

Private permissioned blockchains would not be optimal when looking to reduce reliance on internal or partner infrastructure or when looking to be perceived as being fully transparent. For example, the costs associated with space, power, cooling, network infrastructure and compute infrastructure could be further reduced by leveraging any underutilized assets of third parties willing to participate in the network. Also, considering factors including an entity's corporate structure or acceptance of public funds, stakeholders may demand full access to the digital ledger for individual audit purposes.

15C. WHY USE A HYBRID (PERMISSIONLESS + PERMISSIONED) BLOCKCHAIN?

An entity may want to use a hybrid blockchain to only allow specific nodes to validate transactions and add blocks to the chain (permissioned) but allow any individual or organization to offer their network or compute infrastructure resources (permissionless) to the network. In this instance control can be maintained, costs can be reduced, and an entity can leverage blockchain technologies where they deem fit.

Complexities can, and likely will, arise if using different blockchains for different purposes while needing them to be fully interoperable.