Basics of Blockchain

What is a “blockchain technology”?

One simple analogy is that the blockchain is to money as the internet is to information. It removes the friction and cost of access to the masses. But don’t confuse blockchain technology with the bitcoin-ethereum-blockchain cryptocurrency. It is quite easy to be distracted by the media onslaught of coverage around virtual currencies, and more recently, Initial Coin Offerings (ICO), however, this is mostly smoke and mirrors when compared to the potential held within blockchain itself. Token technology may anchor the next web revolution, spawning crowdfunding behemoths that expedite the value delivery path to their users while cutting out the advertisers and fee-based middlemen.

The current thought model posits the question, “What can’t be tokenized?” Future research notes will explore and detail the many use cases of blockchain and how they are being put to the test with early adopters in this bleeding edge space. Big banks are embarking on programs to provide syndicated loans and the grocery supply chain has signed up with IBM to launch a blockchain-based solution to track food shipments and monitor food safety.

It all sounds mysterious, intriguing and, to be frank, easy to dismiss as so few of us really understand what blockchain technology really is and how it works. Let’s take the first steps towards closing this knowledge gap.

There are five foundational principles that underlie blockchain technology:

- **Distributed Database:** All access all the time! Everyone partaking in the database can see everything in the database. This architecture provides true decentralization where there is no single point of control or failure. This transparency allows independent verification of transactions to occur without a middleman verification step.

- **Peer-to-Peer Transaction:** Blockchain takes the idea of “serverless computing” to a whole new level as there is no central hub for processing transaction data. All transactions are processed and stored in the nodes plugged into the network and those nodes share that data with all of the other nodes.
- **Transparency with Pseudonymity:** Blockchain users have the choice to remain anonymous or share their identities. However, the record itself is present and visible to all. Transactions are encrypted and assigned a unique address as the means of identification.
- **Irreversibility of Records:** Once a record has been transacted in the distributed ledger, it cannot be modified due to the linkage between all records (blocks) that comprise the blockchain. These records are encrypted, ordered chronologically, and visible to all.
- **Computational Logic:** Due to the programmatic nature of the blockchain, logic and algorithms can be applied to automate transactions between nodes upon pre-defined conditions.

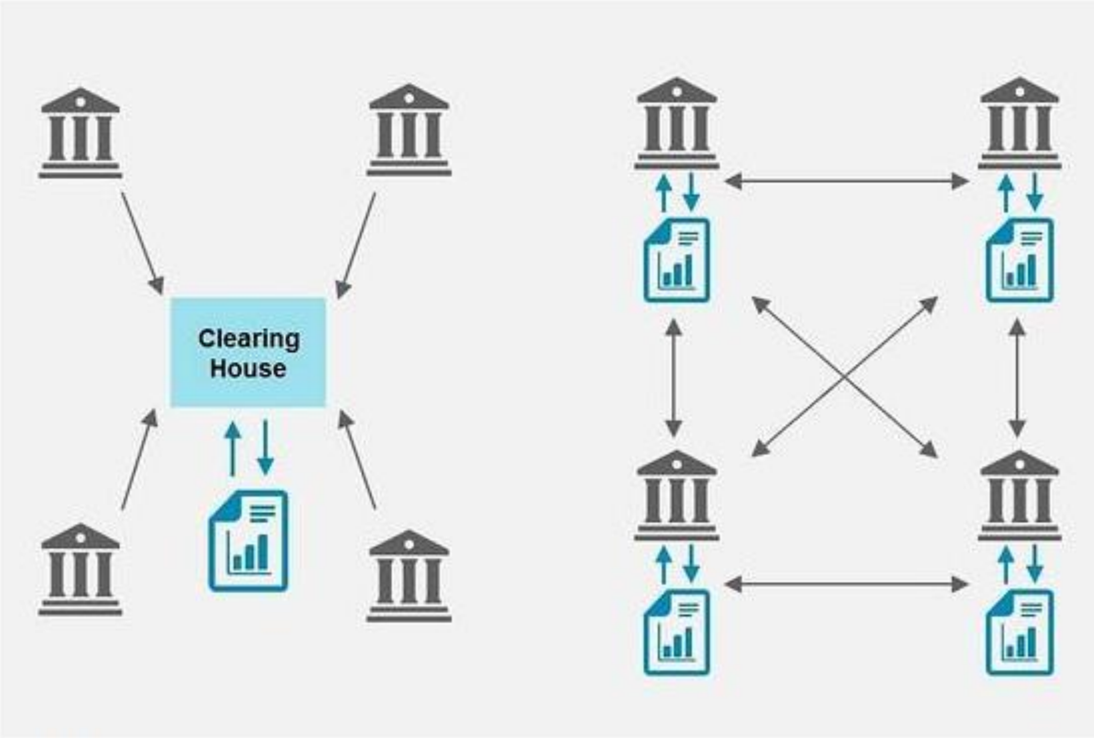
Think of blockchain and the distributed ledger it operates upon as a massive shared database that is collectively shared, replicated, and synchronized across all of the database members, which can number in the millions, based on the allotted size of the blockchain in question. Blockchains eliminate the need for third-party mediation through channels like financial clearinghouses and other intermediate verification process steps. The members of the network govern and agree on all updates to the ledger. Every ledger record is unique and contains a timestamp and its own cryptographic signature enabling full auditability of the ledger, forever, for all records in that network. There will be ledgers created across virtually all industries based on the use cases involved and the problems to be solved. These blockchain ledgers may be on a public or private network. The blockchain sequentially records all transactions in the network in segments called “blocks.” The blocks are “linked” to form a chain…aka blockchain. This blockchain provides a single source of truth.

Why is blockchain considered secure?

- The replicated nature of the ledger database ensures “consensus” is reached for any change to occur to the database, as any attempted manipulation of the data would be required to occur everywhere simultaneously.
- Use of cryptographic hashes ensure that any changes to the ledger forces a new hash value to be created.
- Digital signatures – private key usage verification.
- Decentralization – P2P model disintermediates any centralized control of the underlying network. All actors are created equal, whether or not they are an individual or a Fortune 500 corporation. Once a transaction receives consensus, it is irreversible.

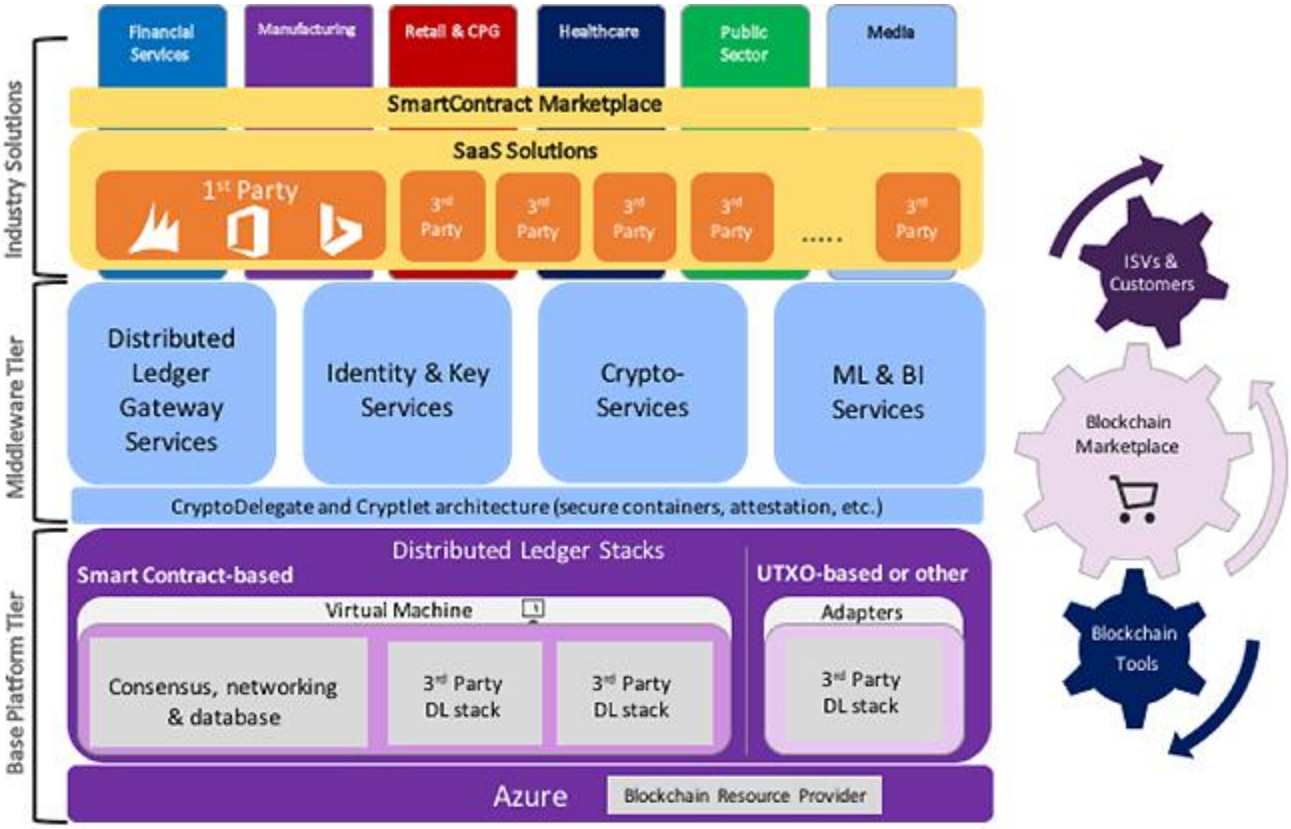
Blockchain Architecture Models

Blockchain Diagram vs. Clearing House Model: This illustrates the automated distribution and verification of information in an asynchronous model vs. the process-heavy synchronous model of a clearing house.



A distributed ledger, right, is a network that records ownership through a shared registry *OLIVER WYMAN*

A more comprehensive blockchain architecture model is shown below and demonstrates the concept of "smart contracts," which will open up the technology to multiple industry solutions.



Source: Nasdaq.com

One of the inhibitors to blockchain adoption centers on security concerns. Most organizations will be addressing this concern in part via the deployment of a permissioned blockchain.

Blockchain Implementation Types

Unpermissioned Blockchain

An open, publicly available, universally accepted ledger where participants do not have to know or trust each other.

- Compute heavy and expensive.
- Time consuming.
- Requires massive numbers of nodes to provide adequate security.
- Risk present, although slight, of hack due to public nature.

Permissioned Blockchain

Private blockchains only available to specific parties

- Usually between known participants.
- Current environment likely to be in legacy financial institutions, but use-case expansion is robust.
- Innovation occurring for permissioned blockchain to improve security.

Core areas that early adopters of blockchain technology are emphasizing, as expressed by Marley Gray, the Principal Program Manager for Microsoft's Azure Blockchain Engineering team, include:

- Platform openness is a requirement.
- Features like identity, key management, privacy, security, operations management, and interoperability need to be integrated.
- Performance, scale, support, and stability are crucial.
- Consortium blockchains, which are members-only, permissioned networks for consortium members to execute contracts, are ideal.

Role of Hyperledger

They hyperledger is the product of a cross-industry collaboration hosted by The Linux Foundation. Members of the consortium are comprised of members from the finance, IoT, banking, supply chain, manufacturing, and technology industries, all working towards the creation of a distributed ledger framework and source code that is open, standardized, and enterprise-grade.

Projects within the hyperledger collaborative include Hyperledger Fabric and Hyperledger Composer, among others. Each hyperledger project aims to create a new framework with a specific set of features and functionality such as modular application development, identity management, and smart contracts as examples.

Another blockchain collaborative blockchain hub, R3 CEV, has launched a blockchain derivative platform called Corda that limits verification capabilities to parties involved in the transaction or that have access granted.

The takeaway here is that blockchain technology is a platform movement that has “legs.” Consortium members are making an investment in the future, with the true return on investment taking the form of advanced early knowledge that will enable these companies to strike immediately once the use cases are refined and core concerns around government and industry regulation, as well as security, are tackled over the next few years.

Am I a Blockchain Candidate?

What are the criteria for a blockchain use case?

IBM provides some solid guidance for general criteria that should be considered when evaluating potential blockchain projects:

- Is a business network involved?
- Is consensus used to validate transactions?
- Is an audit trail, or provenance, required?
- Must the record of transactions be immutable or tamper-proof?
- Should dispute resolution be final?

Recommendations

- **Take a measured approach.** Initial use cases and anticipated paths of new technologies usually change and evolve significantly as they mature over time.
- **Think big.** Start exploring the potential use cases for blockchain technology in your industry. Are you ahead or behind the curve already?
- **Stay up to date.** As blockchain hits the mainstream media hype cycle, new developments from government regulators, industry-driven consortiums, big tech, and the VC community will be overwhelming. Develop a structured plan for filtering down to the critical information.

Bottom Line

Cryptocurrencies are in all the headlines, but the transformative power of the underlying blockchain technology is the pot of gold at the end of the rainbow. Learn about the building blocks of blockchain in this research note to better envision future impact on your organization.