KC Tam Follow

New technologies follower and recently a fan of cryptocurrency and distributed ledger technology. Happy to share whatever I learn in this area.

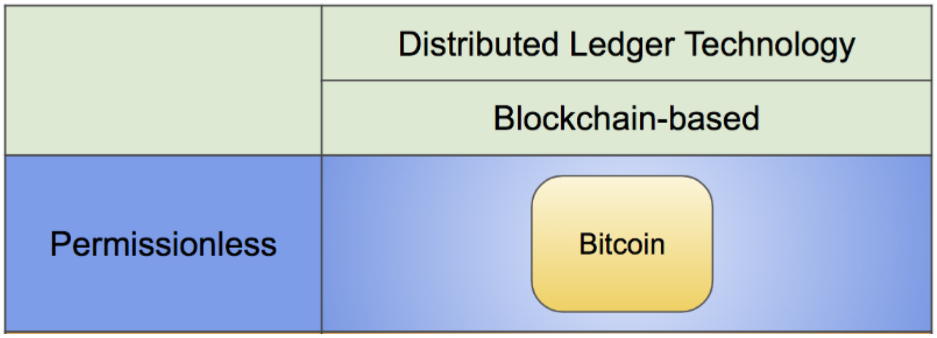
Apr 2 · 8 min read

Blockchain and the Challengers

While blockchain continues gaining attention, be it in cryptocurrency sphere or other innovative use cases in business world, new technologies are coming up to address some of their shortcomings. However the comparison is sometimes made with things mixed together. In this article I try to make it clear what belongs to which area, and then we can have a bigger picture, and make a more proper comparison among them. We don't have to compare apples with oranges.

In the Beginning: Bitcoin and Blockchain

Bitcoin emerged almost a decade ago, and by and large it is still recognized as the first successful implementation of blockchain. Bitcoin is nothing more than a public ledger distributed in a large amount of nodes, and blockchain is the technology enabling this distributed ledger. A more generic term for this type of technology is called Distributed Ledger Technology (DLT).



	Distributed Ledger Technology
	Blockchain-based
Permissionless	Bitcoin

Begin with Bitcoin as Permissionless Blockchain

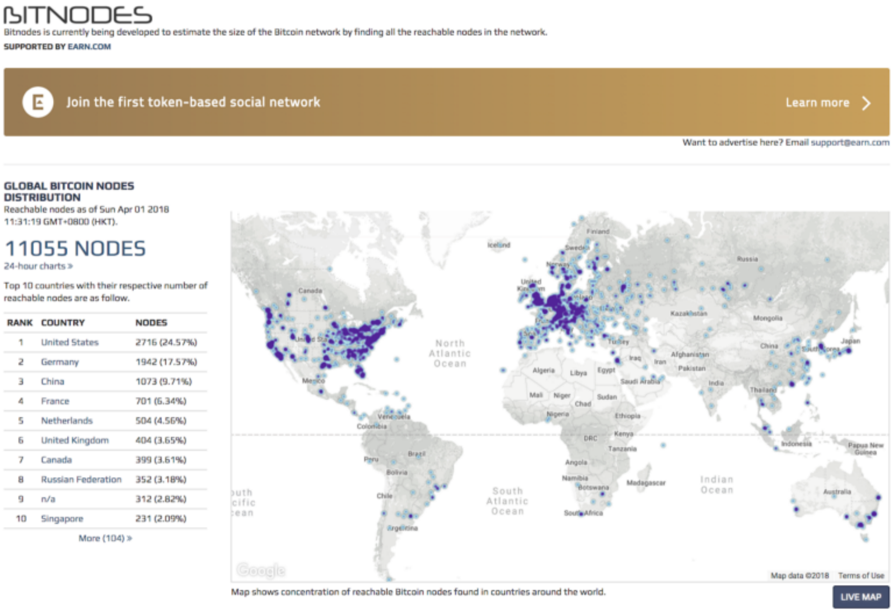
The following is just the highlight about the nature of Bitcoin blockchain. We will refer to them when talking about other blockchain implementations.

It is **distributed**. The Bitcoin network is composed of a big number of computers (nodes). Each node has a copy of the Bitcoin blockchain.

It is **permissionless**, which means node can join and leave the Bitcoin network at any time. Joining the network helps enhancing its robustness, while leaving the network doesn't do much harm at all.

It is **decentralized**, which means that no single organization owns the Bitcoin network, and can shut it down completely. Take a look on the Bitnodes site, the distribution looks quite balanced to certain extent. This also provides some intrinsic capability to withstand Denial of Service (DoS) attacks.

Take a look on how the Bitcoin network is as of today (March 2018), by more than 11,000 nodes running across the world.



BITNODES

Bitnodes is currently being developed to estimate the size of the Bitcoin network by finding all the reachable nodes in the network.

SUPPORTED BY EARN.COM

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Sun Apr 01 2018 11:31:19 GMT+0800 (HKT).

11055 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2716 (24.57%)
2	Germany	1942 (17.57%)
3	China	1073 (9.71%)
4	France	701 (6.34%)
5	Netherlands	504 (4.56%)
6	United Kingdom	404 (3.65%)
7	Canada	399 (3.61%)
8	Russian Federation	352 (3.18%)
9	n/a	312 (2.82%)
10	Singapore	231 (2.09%)

More (104) »

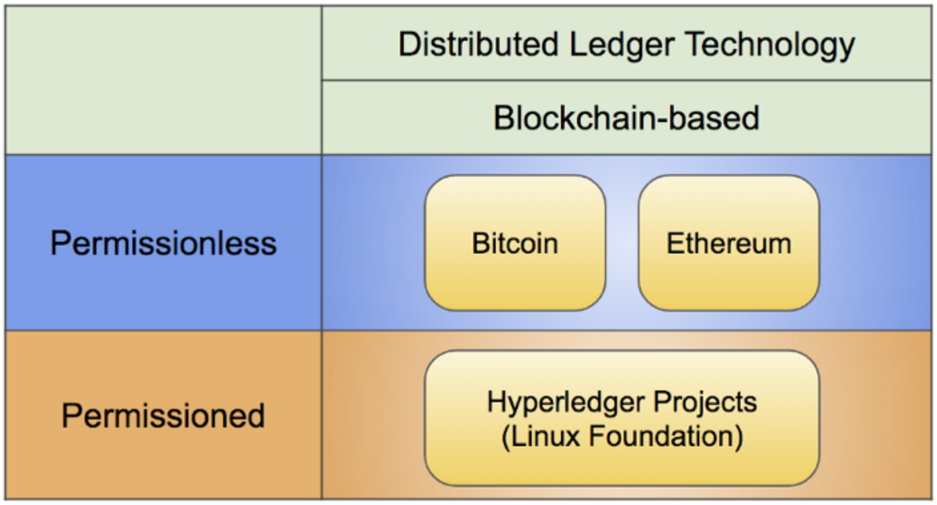
Map shows concentration of reachable Bitcoin nodes found in countries around the world.

Source: bitnodes.earn.com captured in 31st March, 2018.

Then, New Comers in Blockchain Family

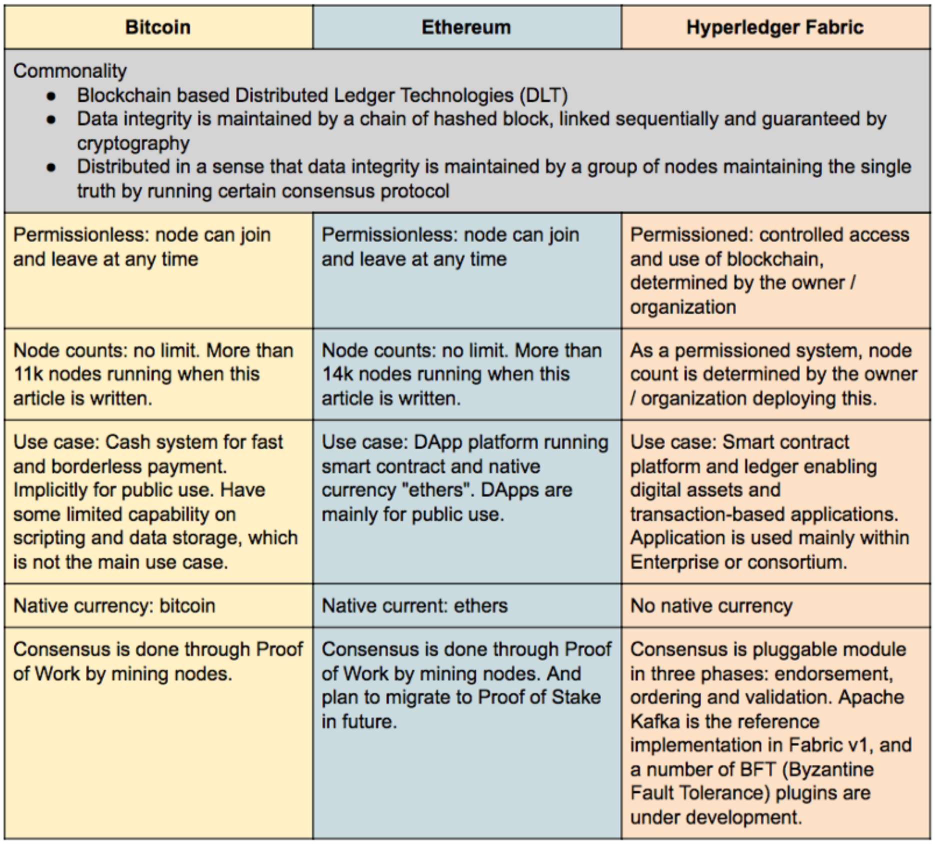
Since then, we see several new blockchain initiatives. The largest two so far are **Ethereum** and **Hyperledger**. They are different in both use cases and deployment model.

A note: Hyperledger is an umbrella of projects hosted by Linux Foundation. It includes several blockchain projects. Different blockchain projects take some different approaches. Here I pick Hyperledger Fabric, contributed mainly by IBM, due to its larger media coverage and business activities.



Now we have both permissionless and permissioned blockchains

It is not easy to put down every detail. Here I just highlight those items that we will see later how other technologies are challenging blockchain.



Bitcoin	Ethereum	Hyperledger Fabric
Commonality • Blockchain based Distributed Ledger Technologies (DLT) • Data integrity is maintained by a chain of hashed block, linked sequentially and guaranteed by cryptography • Distributed in a sense that data integrity is maintained by a group of nodes maintaining the single truth by running certain consensus protocol		
Permissionless: node can join and leave at any time	Permissionless: node can join and leave at any time	Permissioned: controlled access and use of blockchain, determined by the owner / organization
Node counts: no limit. More than 11k nodes running when this article is written.	Node counts: no limit. More than 14k nodes running when this article is written.	As a permissioned system, node count is determined by the owner / organization deploying this.
Use case: Cash system for fast and borderless payment. Implicitly for public use. Have some limited capability on scripting and data storage, which is not the main use case.	Use case: DApp platform running smart contract and native currency "ethers". DApps are mainly for public use.	Use case: Smart contract platform and ledger enabling digital assets and transaction-based applications. Application is used mainly within Enterprise or consortium.
Native currency: bitcoin	Native current: ethers	No native currency
Consensus is done through Proof of Work by mining nodes.	Consensus is done through Proof of Work by mining nodes. And plan to migrate to Proof of Stake in future.	Consensus is pluggable module in three phases: endorsement, ordering and validation. Apache Kafka is the reference implementation in Fabric v1, and a number of BFT (Byzantine Fault Tolerance) plugins are under development.

Some quick comparison among them.

Both Ethereum and Hyperledger Fabric provide smart contract capability. However it makes little sense to tell which one is better than another. It is not very difficult for anyone to decide whether permissionless or permissioned blockchain is more appropriate in one's use case.

Hyperledger does not come with native currency. But just this point does not make it less useful. In enterprise or consortium deployment, currency is usually not needed to fund the transaction, as the owner can take care of this. If needed, interfacing with external fiat currency is something doable to fulfil this requirement.

Consensus in Hyperledger in general can be reached much faster than in Bitcoin and Ethereum. It is due to the nature of decentralization on permissionless blockchains. In a permissioned environment, nodes are all under control by one or several known parties, and consensus can be much simpler.

While Ethereum can be deployed as private blockchain, the requirement of mining and lack of access control make Ethereum far from a permissioned implementation. Some efforts have done on Ethereum such as Quorum to make it more enterprise use ready as permissioned blockchain.

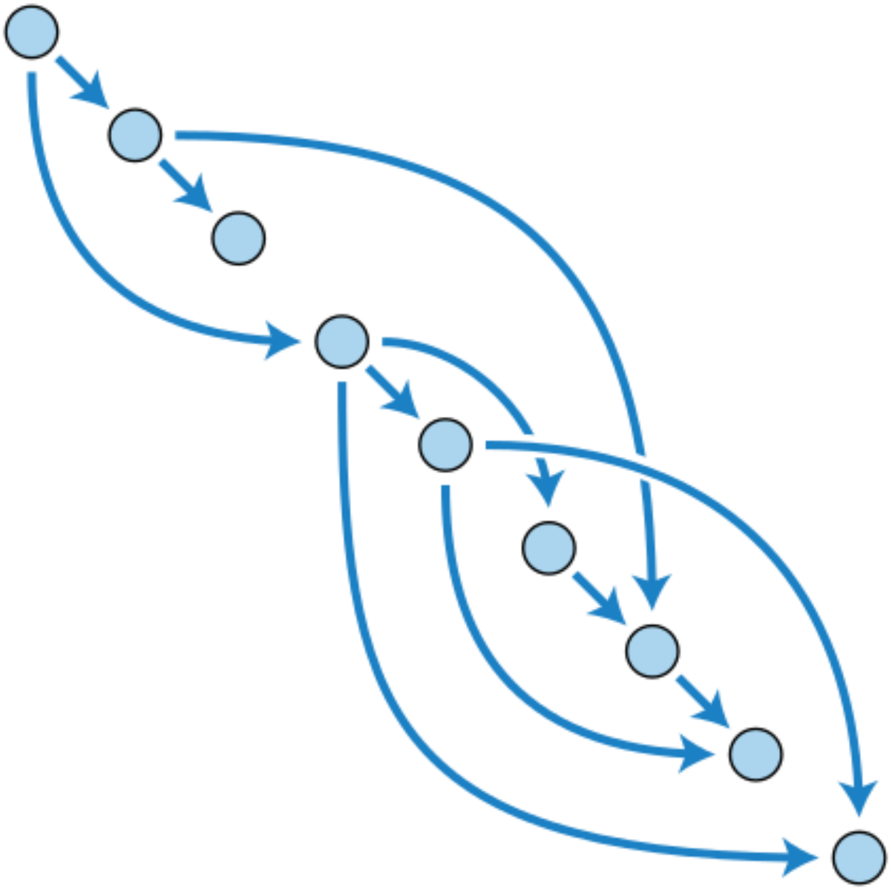
Here Comes the Challengers of Blockchain

Since their launch, many have pointed out various problems or challenges the current blockchain implementations are facing and therefore improvement is much needed. The improvement can come from an evolvement, without largely altering what we have today. Examples include the use of side chain or new consensus protocols. Or totally new approaches are proposed to solve the problems. Among the technologies, Directed Acyclic Graph (DAG) recently gets high spotlight. And there happens two implementations adopting DAG, one on permissionless and one on permissioned.

This article only provides a minimum introduction of these technologies. There are more comprehensive material on each of them.

Directed Acyclic Graph (DAG)

DAG is considered another way to represent the data structure with advantages over the blockchain approach.



A DAG. Source: wikipedia

In DAG there are nodes and connections. Nodes here are not computers. We can just see node as a piece of data. Nodes are linked cryptographically. The graph is called "directed" as we see there are directions for nodes (represented by arrows). It is called "acyclic" as there is no loop. This is the very basic about DAG.

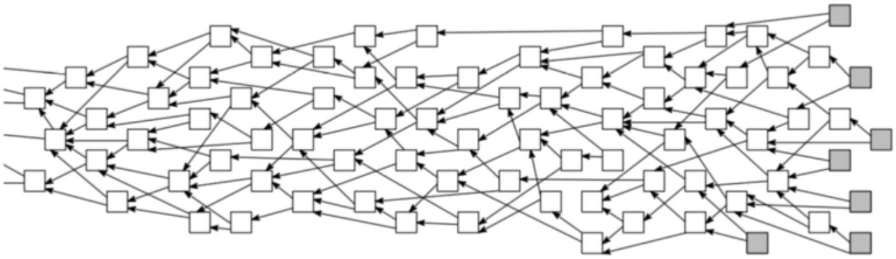
There is no a single model how a DAG should be implemented. Here the two proposed approaches using DAG are implemented very differently. Meanwhile, blockchain is considered as one type of DAG of chain shape, and Ethereum is also an implementation of DAG although it's more perceived as a blockchain.

IOTA Tangle: the Permissionless Ledger

IOTA addresses the challenges of existing permissionless blockchain implementation, in particular on the use cases of machine economy and micropayment. The challenges are,

- scalability in handling large amount of transactions
- high transaction fee
- dichotomy on users (transaction issuers) and miners (transaction approvers)

In short, IOTA introduces **Tangle**, the DAG where user transactions are held. It is called “bundle of transactions” but for sake of simplicity we just term it “transaction”, represented by a square in the diagram. New transaction has to approve two unapproved transactions, called tips (grey square in the diagram), before being placed on the Tangle. This transaction then becomes a new tip, and is to be approved by transactions coming later. This forms the Tangle.



IOTA Tangle. Source: IOTA Tangle Whitepaper

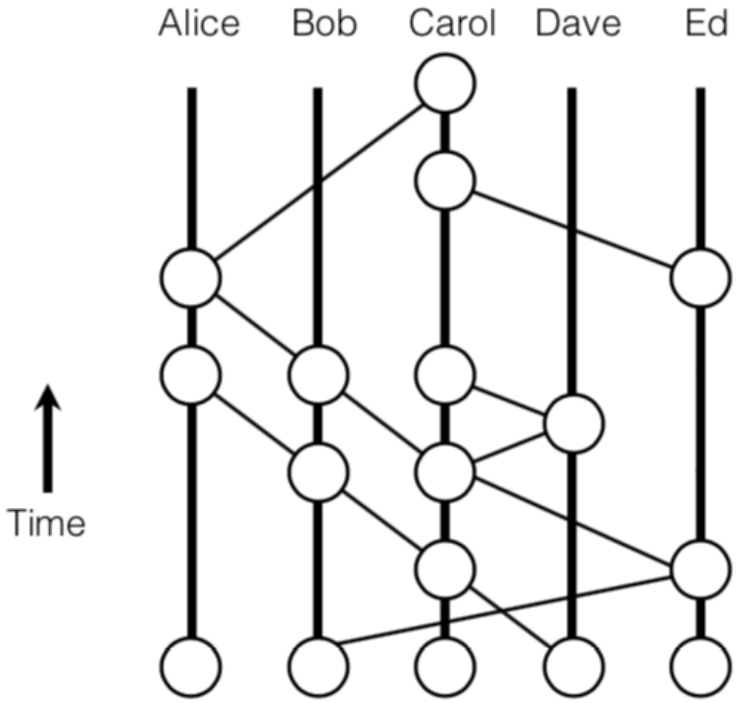
With Tangle, there is no node specifically for mining, as each transaction itself acts as the “miner” to approve two other transactions. As no incentive is needed for miners, no transaction fee is needed. This fee-free fund transfer is foundation of machine economy and micropayment. The DAG is maintained through the tip selection by Random Walk Monte Carlo algorithm by every transaction. IOTA comes with native currency called iota, and the ledger is held inside the Tangle.

Swirlds Hashgraph: the Consensus protocol for Permissioned Ledger

Swirlds **Hashgraph** is positioned as a consensus protocol that promises “fast, secure and fair” when handling large volume of transactions.

Hashgraph today is a permissioned implementation, which is for enterprise or consortium deployment. In a nutshell, a group of participants share the transactions they know to others. The unit is called "event", which contains the transaction items they know and they believe unknown to others (a circle shown in the diagram below). By proper linking the events cryptographically, everyone has the full graphic presentation of events and can therefore come up with a consensus on transactions with timestamp without third party involvement, which is called "virtual voting" among them.

Here is how Hashgraph looks like. The five participants forms the consensus after sharing events to one another. The Hashgraph algorithm guarantees the consensus achieved.

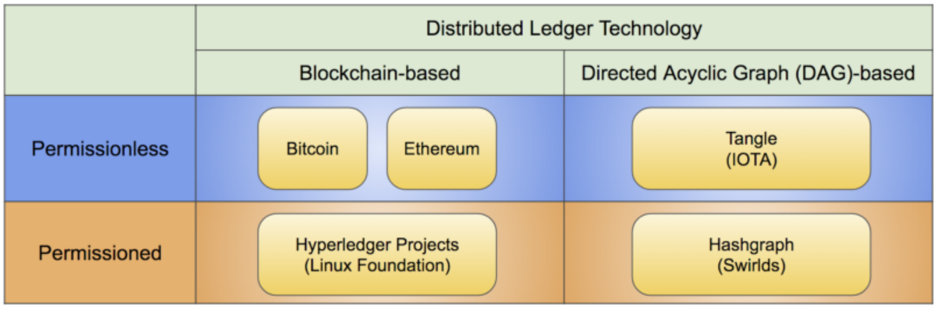


Hashgraph. Source: Hashgraph Whitepaper

While they are considering public ledger, the actual plan is still not announced. The consensus protocol itself does not have any native currency, but currency can be created as an upper layer using the Hashgraph consensus protocol.

Comparison with New Technologies

IOTA and Hashgraph are widely perceived as challengers to existing blockchain technology. Here we put them into the table, and try to make some reasonable comparisons.



	Distributed Ledger Technology	
	Blockchain-based	Directed Acyclic Graph (DAG)-based
Permissionless	Bitcoin Ethereum	Tangle (IOTA)
Permissioned	Hyperledger Projects (Linux Foundation)	Hashgraph (Swirlds)

A bigger picture of DLT, including implementations of blockchain and DAG.

IOTA Tangle is a valid challenger to Bitcoin and Ethereum as they all are permissionless, and coming with native cryptocurrency. In particular, IOTA addresses the shortcoming of scalability and high transaction fee which is not suitable for machine economy. There are quite many issues on IOTA during their first implementation. Nevertheless, just from technology perspective, we can keep our eyes how blockchain-based and DAG-based competes in the permissionless arena. One drawback currently on IOTA is the lack of smart contract capability, though some third parties are working on something like token standard on IOTA.

In some Hashgraph introduction, when they talk about how fast Hashgraph is (at hundreds of thousands per second), they always bring out Bitcoin (3–7 per second) and Ethereum (10–20 per second) for comparison. My view is that Bitcoin and Ethereum require additional effort to maintain its permissionlessness, which is the key difference compared to Hashgraph permissioned implementation. For better comparison, it should be either Hashgraph versus existing permissioned blockchain-based implementations like those in Hyperledger, or when Hashgraph comes out a permissionless network as what Bitcoin and Ethereum are doing today. Note: it is not simply a public ledger, but a real permissionless implementation as what Bitcoin and Ethereum work today.

Besides, Hashgraph is clearly positioned as a consensus layer, and a more complete framework is being built on top of it. As Hyperledgers projects support pluggable consensus services, instead of competing each other, there may be a way of collaboration. Nevertheless, the business model Swirlds currently taking is more an enterprise software approach and therefore they may prefer building their whole platform.

No serious comparison between Tangle and Hashgraph is observed so far. It makes sense as both are addressing different use cases, and the use of DAG has not much overlap. As both are still developing their technology and ecosystem we will see whether there will be any overlapping, such as Tangle in Enterprise use, or Hashgraph becomes a more permissionless deployment.

Summary

As mentioned in the beginning, new DAG-based technologies are challenging the existing blockchain players, in both permissionless and permissioned implementations. Understanding which part they belong to helps us to draft a bigger picture in this industry.

We will continue seeing heated debates among them. Put aside the investment values, reading their effort in bring new approaches is very inspiring, and let’s see how they are evolving and how the acceptance will be in the market, either in community or in business world.

· · ·

Hope you enjoy reading. Give me some claps, and reach me on my LinkedIn.