Hedera Hashgraph

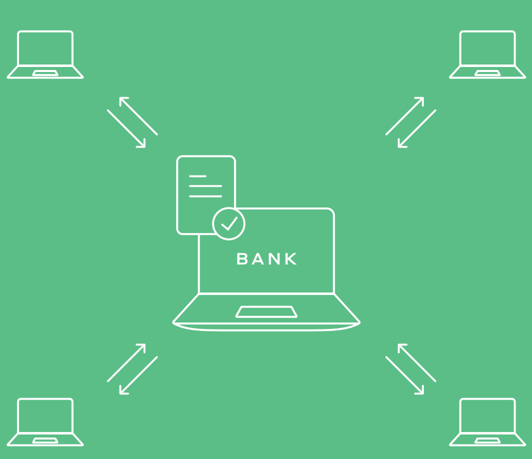
An introduction to distributed ledger technologies (DLTs)

HEDERA 2019

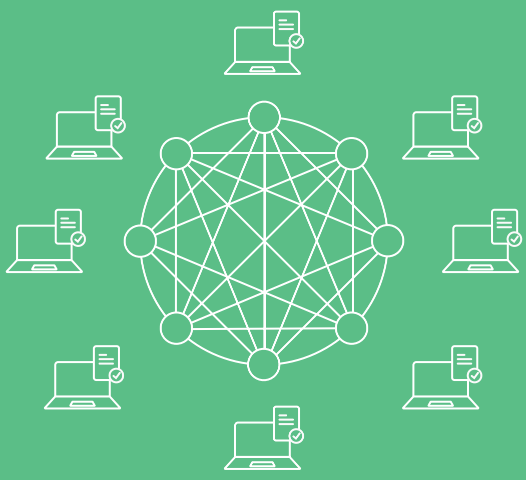
In a traditional marketplace, middlemen oversee the exchange of assets. When you receive your paycheck, for example, a bank controls the transaction. The bank validates the check, verifies that the employer holds the required funds in their account, and records the exchange. **This record, or ledger, documents the transaction and the resulting change in wealth**; you can look at your bank statement and see that you're a little bit richer. For most transactions, a central entity like a bank has sole power over this ledger.

While giving control of our transactions to a central power requires a great deal of trust, it has historically been the best method for ensuring the security of the ledger. Imagine, for instance, that your employer owned the ledger instead of the bank. Your employer could falsely claim that they paid you and manipulate the records to back up their lie. Because of this security risk, neither participant in the exchange should be given sole control of the ledger. For most of history, the best way to avoid this kind of fraud was to entrust an unbiased intermediary with the ledger and hope that this middleman would faithfully maintain the ledger. In other words, traditionally, two parties who agreed upon a transaction relied on a third-party institution to carry out and record the exchange.

However, central ledgers are no longer the only viable option for exchanging our assets. Now, due to the advent of distributed ledger technologies, we can safely get our paychecks without needing to trust a bank.



TRANSACTIONS ON A CENTRALIZED LEDGER ARE VERIFIED, RECORDED, AND EXECUTED BY A SINGLE AUTHORITY.



ON A DISTRIBUTED LEDGER, THE ENTIRE NETWORK RECORDS AND VALIDATES EACH TRANSACTION.

What are distributed ledger technologies?

Distributed ledger technologies, like blockchain, are peer-to-peer networks that enable multiple members to maintain their own identical copy of a shared ledger. Rather than requiring a central authority to update and communicate records to all participants, DLTs allow their members to securely verify, execute, and record their own transactions without relying on a middleman.

While there are a wide variety of DLTs on the market, they are all comprised of the same building blocks: a public or private distributed ledger, a consensus algorithm (to ensure all copies of the ledger are identical), and a framework for incentivizing and rewarding network participation.

Distributed Ledger: a database shared by multiple participants in which each participant maintains and updates a synchronized copy of the data.

Public vs. Private Distributed Ledgers

DLTs require a large number of participants (nodes) to ensure that no one member has too much control over the ledger. After all, a distributed ledger with only one participant would be identical to a central ledger!

Therefore, some DLTs have open access. **These public distributed ledgers allow anyone with a decent computer and internet access to maintain their own copy of the ledger**. With no restrictions to entry, these DLTs can be highly populated and widely transparent, two qualities of a secure network; the greater the distribution of control, and the easier it is to see when the ledger has been tampered with, the harder it is for malicious actors to compromise the database. Because of the accessibility, security, and transparency of public distributed ledgers, many DLT implementations choose to be public.

The alternative to a public distributed ledger is a private distributed ledger. **Private distributed ledgers place restrictions on membership, often for the sake of speed and stability**. While having a greater number of nodes allows for higher security and transparency, each additional node that must maintain the ledger slows down the network. To avoid slow and unstable transaction speeds, private ledgers restrict membership. Though these restrictions sacrifice transparency and network size, private DLTs compensate for the loss in security by only admitting trustworthy participants. In cases where trustworthy participants can be found and privacy is preferred or required, private distributed networks provide a fast and stable alternative to public distributed networks.

Reaching Consensus

Although every member of a public or private distributed ledger maintains and updates their own copy of the ledger, it is imperative that each of these ledgers remains identical. Imagine, for instance, that your copy of the ledger reveals that you have $100 in your account, while the cashier's ledger holds that you have $1. This discrepancy would make it very difficult, if not impossible, to buy a candy bar. Without identical ledgers, participants in the network could not make transactions.

In order to keep the distributed ledger consistent, DLTs must have a consensus algorithm, or a method of ensuring that all copies of the ledger agree.

> **Consensus Algorithm: a method of synchronizing the data across a distributed system. In the case of a DLT, the consensus algorithm ensures that all copies of the ledger are identical.**

There are many different consensus algorithms on the market, each with different advantages. Perhaps the most intuitive algorithm is a simple vote. According to this algorithm, each node independently calculates how they think they should update their ledger based on the information available to them. Then, each node sends this information to every other node. At this point, every node in the network has access to their decision and every other node's decision. The nodes then calculate the majority or plurality vote, and they all update their ledgers according to this democratic consensus.

Although the simple vote is effective and intuitive, it is not efficient at scale. Because every node must send their vote to every other node, the bandwidth and processing power required to come to consensus grows exponentially with the size of the network. In other words, every additional node dramatically decreases the efficiency of the network. Because DLTs become more secure and transparent when more nodes are added to the network, many other consensus algorithms have been developed to better suit the need for large, efficient, and reliable peer-to-peer networks.

If you are curious about other consensus algorithms, you can hear from our Co-Founder and CEO, Mance Harmon, comparing Leader-based, proof-of-work blockchain, simulated economy, voting- based systems, and Hashgraph with virtual voting, by visiting: Hedera.com/consensus-algorithms

Cryptocurrency and Compensating Participants

To carry out their consensus algorithms, DLTs require a significant amount of processing power per transaction. Just as DLTs distribute the responsibility of maintaining the ledger to each participant, so do they divide this computational burden. Every node must donate computing power to run the consensus algorithm and process transactions.

Of course, computing power is not free. To compensate participants for their work, and incentivize further participation, DLTs typically reward active membership with cryptocurrency.

Cryptocurrency: a virtual, encrypted token which can be exchanged using across a decentralized network. These coins can be exchanged, purchased, or earned by participating in the network.

While cryptocurrencies have no inherent value (much like fiat currency), they may be valuable to participants in a network because they are necessary for performing actions quickly, securely, and cost effectively across the decentralized network. Their usefulness as currency generates a demand for these coins. Therefore, participants have an incentive to contribute computational resources to the network. Not only is their work rewarded in cryptocurrency, the value of that currency may rise as the network grows and more build useful applications on the distributed ledger platform.

To learn more about Hedera's cryptocurrency and join our community testing program to earn hbars, visit **portal.hedera.com** to register.

Why are distributed ledger technologies useful?

Distributed ledger technologies allow businesses and individuals alike to quickly carry out secure transactions without needing to rely on a middleman. By avoiding intermediaries, distributing control of the ledger, and providing a tamper-apparent network, DLTs present a more cost-efficient, accessible, and reliable transaction platform than centralized ledger systems.

REMOVE THE MIDDLEMAN AND ENGAGE IN DIRECT, TRUSTED TRANSACTIONS.

INCREASE ACCESSIBILITY AND BUILD TRANSPARENT APPLICATIONS.

PROTECT THE LEDGER WITH CONTROLLED MUTABILITY AND TAMPER-APPARENCE.

Remove the Middleman

Because central ledgers rely on intermediaries, they are burdened by the costs and inefficiencies of the middleman. DLTs do away with these limitations by avoiding middlemen and intermediaries altogether. **Without a central agent, there is no need to pay a central agent. And, without the need for clunky bureaucracy, you can exchange assets directly and immediately**. You no longer have to limit the speed of your transaction to the efficiency of expensive bankers, lawyers, or politicians.

Moreover, you no longer have to trust bankers, lawyers, or politicians with the ledger and your assets. DLTs are trustless systems, meaning that no participant needs to trust any other participant to guarantee a valid ledger.

Accessibility

While centralized systems monopolize control and limit access to their ledger, DLTs provide a much more accessible service. DLTs allow businesses and individuals to carry out transactions freely, without relying or trusting any other individual. Public DLTs take this further by issuing no restrictions on transactions or participation; no one can be denied from the platform, and no transaction will be treated with priority over another.

Tamper-apparent

Traditional ledgers may provide fast and simple record-keeping, but they are vulnerable to corruption and hacking. Because only one central entity controls the ledger, a corrupt central agent can tamper with the records without the consent or knowledge of the affected members. Moreover, because there is only one copy of the ledger, hackers have a clear, single target for their attacks. Without visibility into whether tampering has occured, we must simply trust that the central third-party is neither corrupt nor compromised when we use a centralized ledger.

Distributed ledgers, however, are inherently resistant to tampering. While a malicious agent could compromise a central system by altering the single ledger, they would need to alter at least a plurality of ledgers to have an impact on a distributed system.

Though DLTs are not tamper-proof, they are tamper-apparent. That is, if tampering does occur, the network's transparency ensures that all members of the network will be aware of the change. Though a participant of a DLT cannot be completely certain that the ledger will remain unaltered, they can rest assured that they will know if tampering does occur.

Hedera Hashgraph has achieved the gold standard of security in distributed ledger consensus mechanisms, which is asynchronous Byzantine fault tolerance (aBFT) and is the only distirbuted ledger to-date which has formally proven this quality. Hedera guarantees consensus, in real time, and is resistant to Distributed Denial of Service (DDoS) attacks, an area of vulnerability for some public ledger platforms.

Immutability and Controlled Mutability

Some distributed ledgers take security beyond tamper-apparence by establishing immutability, preventing any and all participants from changing established records for any reason. Members of these immutable DLTs can only view the ledger and carry out new transactions. Even if all participants in the network wished to change the ledger, there would be no pathway within the system's architecture for that change to occur. Therefore, participants of an immutable distributed ledger can be certain that their ledger is not only tamper-apparent, but tamper-proof.

Immutable: a distributed ledger technology is immutable if it does not provide any participant or group of participants the ability to alter or delete established records.

Of course, immutability does come with downsides. In some cases, changing past records could be beneficial. For instance, if a bug in the DLT's code causes a transaction to be misrepresented in the ledger, immutability would prevent anyone from fixing that problem. The invalid transaction would forever be part of the official ledger. Additionally, as laws change to catch up with technology, new government regulations may necessitate a change in record-keeping practices. Immutable systems would not be able to adapt to these changing legal conditions, and would therefore risk violating government standards.

Recognizing the downsides of both mutability and immutability, some DLTs opt for controlled mutability.

Controlled Mutability: DLTs with controlled mutability allow records to be changed, but place heavy restrictions upon that pathway.

Controlled mutability is the best of both worlds: no malicious participant or group of participants can alter the records without everyone knowing (tamper-apparent), but the DLT can adapt to bugs and changing regulations. Hedera Hashgraph is one example of a DLT with controlled mutability. Hedera Hashgraph will establish the Hedera Council, a diverse group of businesses across nearly every industry. The council will have the ability, through unanimous vote, to remove illegal or malicious content to abide by local and global regulations. Because the council will be completely transparent and bound by term limits, participants will observe and hold the council accountable for any changes that they may make to the ledger. By having the Hedera Council, Hedera Hashgraph provides a controlled mutability that retains security while allowing the DLT to adapt to changing government standards. To learn more about the Hedera Governing Council, visit: Hedera.com/council

Build on Hedera.

If you're a developer looking to learn more about the Hedera Hashgraph platform services and how to build a decentralized application, please visit: **hedera.com/platform**

Test the mainnet. Earn hbars.

If you're interested in joining Hedera Hashgraph's community testing program and earning hbar cryptocurrency for your efforts, please visit: **Hedera.com/community-testing**

Hedera™
Hashgraph

What future will you build?