SpiderOak Mission Systems

Tech Brief: Distributed Ledger Technology

DLT and Blockchain are popular buzzwords in today's security market because DLT and Blockchain create security opportunities that haven't existed before.

A key component of the SpiderOak Platform is the way it securely manages authority across the system. It does this with distributed ledger technology (DLT), also known as blockchain. SpiderOak's family of products and platform simplify the implementation of these technologies into an easy-to-use tool.

How the Technology Works

In a distributed ledger system, all devices with access to the ledger have the complete source of truth, which is maintained by agreement between the devices. Transactions from the devices, such as changes to the user list, are bundled into blocks and then distributed to all the devices. Each block references the cryptographic hash of the prior block, which means no individual block is valid unless the hash of the prior block is valid, which implies that the hash of the block prior to that is valid, and so on to the beginning of the ledger's history. Blocks with the wrong hash, incomplete data, or other errors are rejected. This chain of blocks ("blockchain") is therefore an irrefutable ledger of changes within a system. The central database is just another place where a copy of the ledger is stored – it is no longer a single source of truth. Instead, all devices with a copy of the ledger (known as clients or endpoints) calculate an inductive proof of the current state of affairs by beginning at the initial block and working through the history of changes to the present.

The most common type of distributed ledger is a cryptocurrency blockchain, also typically referred to as a type of 'public' ledger. These systems de-trust the infrastructure, requiring expensive "mining", where infrastructure performs increasingly expensive computations as a proof-of-work to ensure fairness. Systems like this cause delays and increased resource consumption: a single block in the Bitcoin distributed ledger takes 10 minutes and 650.55 kWh of electricity to transact[1]. **SpiderOak avoids these problems.**

[1] https://digiconomist.net/bitcoin-energy-consumption , accessed February 24th, 2020.

Our system assumes enterprise system administrators can be trusted for providing the *availability* of information systems. Unlike a public ledger, being able to control and restrict access to a ledger is a positive feature. SpiderOak uses a proprietary private distributed ledger as the underlying platform for our products (Figure 1). Private ledgers can restrict who can be a part of the system or not.

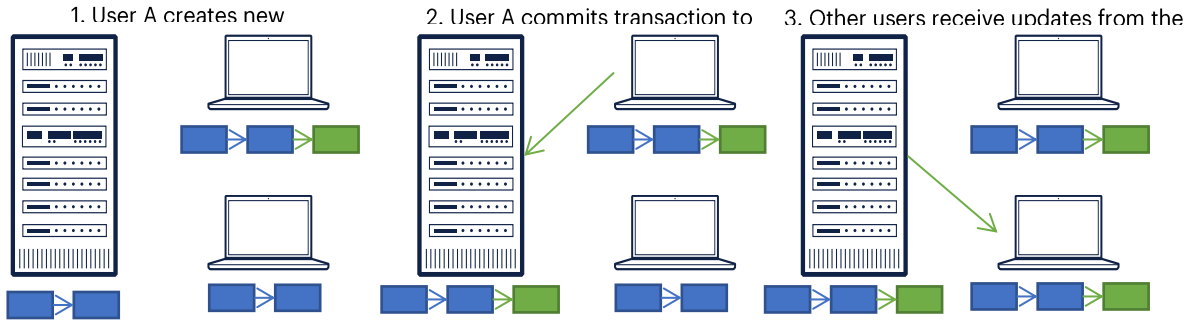

Figure 1: Private distributed ledger. Note that the policy engine validates transactions before accepting them in steps 2 and 3.

Instead of a monolithic ledger defining authority through all parts of the system, the SpiderOak Platform provides a separate ledger to define membership for each group. This provides two advantages. First, it reduces the scope of network, storage, and computational resources that each client consumes to manage and track changes to authority. Secondly, it provides a level of compartmentalization- each client has *only* the data necessary to do work, and not any more than that.

Because in the SpiderOak Platform key management is tied to group membership, there are high assurances of agreement in the "truth" represented by the distributed ledger. Differences in what clients within the same group consider truth result in highly visible encryption errors, requiring intervention and investigation. Our protocol is designed to never split ledgers in this manner, so the fact of a split happening is a tell-tale sign of something wrong.

Supporting Your Mission

SpiderOak has been providing cryptographically secure blockchain solutions since 2006. Since 2019 we've been building partnerships that allow us to create the most strategic secure communication solutions that modern technology can provide. We know that no one knows your mission set like you do, so please reach out to us and let us know how we can build the solution that addresses your particular challenges.

learnmore@spideroak-ms.com
+1 866.432.9888 x2