# A Primer on Blockchain and its Uses

**Sandra J. Wunderlich**
**Tucker Ellis LLP**
**100 South Fourth Street, Suite 600**
**St. Louis, MO 63102**

# A Primer on Blockchain and its Uses

Blockchain is one of the most revolutionary innovations in recent years. It allows the transfer of digital property (such as money, music, movies, etc.) faster, safer, and cheaper. It is also a tamper-resistant electronic record keeper. Blockchain prevents the unauthorized transfer of electronic files, and eliminates the need for a third party to manage the transactions.

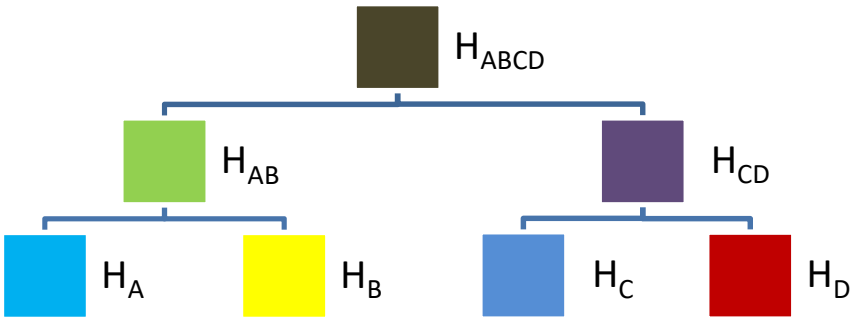
Using money as an example, banks manage transactions by recording the money owned by each of its account holders, and the additions and subtractions from that money. Blockchain manages the transactions by verifying and recording each transaction in a block of data. This eliminates the third party bank from the transaction, thereby reducing the cost of the transaction, eliminating the significant wait time for verification and execution of the transaction, and the chain of title for each transaction on the block chain is nearly impossible to alter without authorization.

This technology is likely to disrupt many industries in the next few years, including the tracking and transfer of intellectual property such as songs and movies. It should help prevent counterfeiting, and ensure that the owners of copyrights receive the revenues they are owed.

**What is it?**

In its simplest form, blockchain is an electronic general ledger of digital property maintained in more than one location. It is a record-keeping technology, and a secure method of transferring digital assets with clear title.

The name refers to the fact that it consists of a digital chain of blocks of information. The "blocks" in the chain consist of data such as the date, time, owner, and dollar amount of a transaction, the participants in a transaction, along with a "hash." The system assigns each block a unique code called a "hash" so that one block is distinguishable from another block. If, for example, you purchased two identical items from the same seller on the same date in separate transactions, the blocks of information would be identical but for the unique hash code embedded in the block. The blockchain has a tree-like structure so that each block has a chain of title back to its origin, as illustrated by this simple example:



**Is it secure?**

By design, blockchain data cannot be modified. It records transactions in a verifiable and permanent way. Real property records at the Recorder of Deeds office is a close analogy. The original title documents do not change; another document records the change in the chain of title. In this way, these records track the owner, transfers of ownership, dates of transfer, and other information impacting title such as mortgages, easements, etc. Blockchain works similarly. In the illustration above, the $H_A$ block remains unchanged after the $H_{AB}$ transaction. To trace the title of H, you simply trace back through the chains of blocks.

A network of computers verifies the transaction requested. Once verified, the information is added to a block of data. The blocks are always chronological. Each block carries its own unique "hash," but also carries the most recently added block code to indicate where the block fits into the chain. When a new block is added to the chain, each computer in the network receives a copy of the digital ledger reflecting the additional block in the chain in sequence. At that point, the block is available for public viewing on the network (although it uses digital names so there is some level of privacy). Although some portions of the blockchain are publicly available, which allows it to work, there are also private portions that only the authenticated user can access.

The blockchain system imposes "tests" that a computer must meet before it can be added to the network. It requires users to prove their authenticity and authorization before they can participate in a blockchain network. For example, in the example of bitcoins, this proving process is called "proof of work." The computer must solve a complex computational problem to be eligible to join the blockchain. The problems are complex and require a highly sophisticated computer to be solved. The odds of a hacker being able to solve the problem are extremely low because the complexity requires so much computer power.

The blockchain is a distributed ledger, meaning that it is typically managed by a peer-to-peer network of multiple computers that follows a protocol for communication and validation of new blocks. Once recorded, the data on the block cannot be altered, without alteration of every block in the chain, which requires a consensus of the network. This offers greater security in the validity of the transaction, and prevents unauthorized transactions. If there are different versions of the blockchain on the network, the blockchain defaults to the longer chain, meaning the most up to date data based upon the links of blocks in the chain because information can only be changed through the addition of a block rather than altering a prior block in the chain. Even if a cybercriminal was able to change a copy of the ledger on one computer, or even a few computers in the network, multiple other computers have a copy of the correct ledger, and the blockchain system is designed to choose the most accurate ledger by choosing the one that matches in the majority of the computers.

Theoretically, a hacker could control the majority of computers on the blockchain, and alter the majority of them, but it would be extremely difficult to accomplish and could only be done by an extraordinarily sophisticated system and resources, particularly in systems with millions of copies of the blockchain involved. This theoretical threat actually incentivizes other users to

ensure that a majority of the computers are not controlled by a small number of users. If users lose their faith in the integrity of the blockchain system, it is no longer useful.

**How can it be used?**

The most common use of blockchain technology today is in the financial industry. Cryptocurrencies operate on the blockchain without the need for a central banking authority, thereby eliminating transaction fees, and expediting transfers. Some banks are using the technology to provide access to money 24/7 and eliminate the float time for transactions, and to minimize the risk of fraudulent transfers.

Some health care companies are investing in blockchain technology to store medical records. Each time a medical record is generated, it can be recorded in a blockchain. The system encodes the records to make them readable by certain authorized individuals, thereby minimizing the impact of a potential data breach.

Some states are experimenting with blockchain technology to record transactions concerning real property. Title searches without blockchain are time-consuming, and can be prone to human error. Blockchain allows for secure transfer of property without the need for a title search because the block chain contains the entire verified history of the title.

Another use of blockchain involves "smart contracts." These are computer-generated contracts that operate under a set of terms and conditions. If the terms and conditions are met, the contract is fulfilled automatically. By way of example, if you rent a hotel room using a smart contract, the door code is provided in exchange for payment of the rent. If the funds are not received, the smart contract does not supply the door code; and if the funds are received, but the door code is not provided by the hotel, the rent is refunded automatically. This system eliminates the need for a third party to manage the transaction. Other examples include automatic payment of invoices upon receipt of a shipment, or automatic payment of dividends at a certain level of profits.

Supply chain optimization also benefits from blockchain, particularly in the food industry. This improves food safety and allows companies to verify that a product is organic, locally sourced or fair trade.

Voting systems are also being revolutionized with blockchain. The hope is that it will eliminate fraud by making votes tamper-resistant, and increase efficiency in the voting process by reducing or eliminating the involvement of human beings, and provide instant results.

The music industry hopes that blockchain technology will provide a reliable ledger system that tracks copyrights, and pays the creators of the works. Tracking royalties in the music industry has been a challenge in the wake of the Napster file-sharing revolution. The ability to share digital files of music upended the music industry because songs could be transferred multiple times to multiple owners without paying the copyright owners for the songs. The owners of the copyrights had no way of tracing the transfers, or stopping them from occurring. The hope is that blockchain will lead to a permanent, public ledger system to compile data on the ownership and use of musical works, allowing artists, songwriters, and publishers to track use, and receive payment for the use of their work. This gives artists more control over their work and ensures that they receive the payments they are entitled to receive. Essentially, blockchain would track

ownership of a copy of a song to prevent unauthorized transfer, copying, or use of that digital file without compensation to the copyright holder. If you wanted to share the song with another person, the ledger would track that transfer so that the original owner would no long own the song and be able to use it, or the transferee would have to pay for the use of the song.

This technology will likely be a significant weapon to combat counterfeiting in a myriad of industries including retail, software, and visual arts such as photographs and film for the same reasons. The chain of title authenticated through a blockchain can be used to confirm the product is authentic, that the transfer or sale is authorized, and to track the origin of counterfeit goods.

The future is likely to reveal a myriad of other uses of blockchain technology. It offers multiple benefits to traditional processes. It can eliminate the delay resulting from multiple rounds of verification for every contract, transaction, and relationship. It can reduce fees by eliminating the humans involved, and the need for a central monitoring institution. Most importantly, however, may be its ability to protect against cybercrimes and counterfeiting of intellectual property.