Emerging technologies such as 5G, microservices, the Internet of Things (IoT), cloud computing, containers, blockchain and many others are shaping the meaning of “technology-based trust.” Consequently, technology-based trust deals with the acceptance that a particular technology is reliable, does what it is supposed to do and delivers what it should.

Although blockchain can be analyzed from a very technical perspective, it is also helpful to focus on technology-based trust with blockchain from a management point of view.

The PricewaterhouseCoopers (PwC) 2017 Global FinTech Executive Summary, Redrawing the Lines: FinTech’s Growing Influence on Financial Services stated that “blockchain is moving out of the lab.” However, this particular statement portrays how the application of scientific knowledge can be used for practical purposes outside the research and development laboratory for the benefit of the enterprise.

In fact, it is very interesting to see the effect of blockchain’s debut in the fintech industry with Bitcoin.

However, blockchain is well known for having disruptive effects by transforming financial services and supporting new business models, applications, processes, products or services.

As a result, it is important to understand the idea of technology-based trust with blockchain by grasping the concept of distributed ledger technology (DLT), the meaning of blockchain, blockchain types, intermediation problem and the use of trusted fintech products using blockchain.

**Distributed Ledger Technology**

The terms “distributed ledger technology” and “blockchain” are frequently used interchangeably; however, it is important to highlight that although every blockchain is a DLT, not every DLT is a blockchain.

DLT is an asset database of financial, electronic, legal, physical and many other data attributes spread across a network of multiple sites, geographies or institutions on a peer-to-peer network. Accordingly, all participants within the network can replicate and save an identical copy of a ledger and update it independently in minutes or seconds. Correspondingly, security and accuracy of assets stored in the ledger are managed via cryptography algorithms through the use of signatures and keys. As a result, DLT can deliver a new kind of trusted mechanism to a wide range of services. In addition, with DLT, data storage is not centralized and there is not a central administrator.

Luis Emilio Alvarez-Dionisi, Ph.D.

Is a fintech professor and management consultant. He has provided advisory services to chief executive officers (CEOs), boards of directors (BoDs) and senior management of Fortune 500 companies, and has consulted on project, program and portfolio management with numerous enterprises worldwide, including Intel, IBM, Merck, Chevron, Isuzu, Smiths Detection, the Beijing 2008 Olympic Games, Citibank, Standard Chartered Bank and the Government of Singapore Investment Corporation (GIC). His fintech research focuses on risk management, robo-advisory consulting, governance structures and start-up fundraising. He can be reached at dr.luis.alvarez@outlook.com.
Blockchain

Blockchain is a shared ledger of transactions across a network of multiple nodes without reliance on a trusted single central authority.

In that sense, the ledger is a catalog of all the transactions produced on the blockchain. Each node is a computer on the network that stores the ledger. For example, all copies of one document are distributed among users in the nodes and they are continuously and automatically synchronized so they are equal at all times.\(^5\)

A simplified example of a blockchain architecture is illustrated in Figure 1. From a technical point of view, the blockchain is composed of a chain of blocks.

The first block is called the “genesis block.” In Figure 1, each block contains the hash of the current block; a timestamp; a nonce, which is a random number used to verify the hash; the block data; and the hash value of the previous block (the parent block).

The objective of this technology is to ensure the integrity of the whole blockchain through the first block (the genesis block).\(^7\)

Because hash values are unique, fraud can be easily detected. This is because changes in the blockchain immediately change the respective hash value.\(^8\)

In addition, each user is required to use a digital signature applying a private key and public key, following the signing stage and the verification stage.\(^9\)

Blockchain technology is denoted by the following attributes:\(^10\)

- The ledger is shared between several participants, having a possible disrupting effect, without a single point of control over the ledger.
- The history of all the transactions are captured in the blockchain of the ledger to prevent changing or updating previous records.
- Digital signatures are used to conduct transactions on the data (i.e., transferring digital assets).

Blockchain Types

Not every blockchain is the same. There are many variations found; however, there are two main types of blockchain to highlight: \(^11\)

- **Open Blockchain**—This is an open platform that could be “public permissionless” or “public permissioned.” At the public permissionless level, it is open to anyone to read, write and commit. Examples of this category of blockchain are Bitcoin and Ethereum. At the public permissioned level, it is open to anyone to read, users need to be authorized to write, and all or a subset of users require authorization to commit.

---

**Figure 1—Simplified Blockchain Architecture**
An example of this category of blockchain is a supply chain ledger for a retail brand viewable by the public.

- **Closed Blockchain**—A closed platform that can be a “consortium” or “private permissioned enterprise.” At the consortium level, it is limited to an authorized set of users to read, write and commit. An example of this category of blockchain is when several banks work with a shared ledger. At the private permissioned enterprise level, it is fully private or limited to a reduced number of authorized nodes to read, and only the network operator is authorized to write and commit. An example of this category of blockchain is when an external bank ledger is shared between a parent holding company and branches.

**Intermediation Problem**

In terms of blockchain, the idea of intermediation is related to the verification of a transaction between two parties.

One of the challenges that financial services face is the verification of ownership of assets and transaction processing. This situation becomes even more cumbersome when all the network participants and intermediaries involved in the chain of validations need to be checked.\(^\text{12}\)

As a result, this verification process becomes time-consuming and costly in a long chain of validations in terms of the origin and transactions processed by people. This scenario is the “intermediation problem.”

Blockchain represents a technological solution to tackle the intermediation problem by shifting from “trusting people to trusting math”\(^\text{13}\) via blockchain consensus algorithms such as proof of work (PoW), proof of stake (PoS), practical byzantine fault tolerance (PBFT), delegated proof of stake (DPOS), Ripple and Tendermint.\(^\text{14}\)

**Trusted Fintech Products Using Blockchain**

Because technology-based trust is based on a “tangible proof” that a technology has been tested and is reliable, examples of trusted fintech products using blockchain technology include Bitcoin, Monero, Litecoin, Ripple, Everledger, Coinsetter, Medici, Blockstream and Chain.com.\(^\text{15}\)

**Conclusion**

Several ideas can be used to enhance the technology of blockchain including distributed ledger technology (DLT), the meaning of blockchain, blockchain types, intermediation problems and trusted fintech products using blockchain. Consequently, in order for an emergent technology to be labeled as “trusted technology,” such technology needs to be widely tested and implemented in real-life environments. In fact, this is the case for technology-based trust with blockchain.

**Endnotes**

4. Ibid.
5. United Kingdom Government Office for Science,


8 Ibid.


12 Op cit Nofer, Gomber, Hinz, Schiereck


14 Op cit Zheng, Xie, Dai, Chen, Wang

15 Op cit Nofer, Gomber, Hinz, Schiereck