BLOCKCHAIN TECHNOLOGY

Internet 2.0

In its simplest terms, a Blockchain is a digitally distributed ledger spreadsheet.

Although that is not simple and doesn't explain why this new technology is the hottest buzzword in the finance and accounting communities. Yet despite it being such a hot topic, no one seems to clearly explain what Blockchain is, or why we should care. Further confusing the issue is that as the underlying technology behind Bitcoin, Blockchain is often conflated with the dubious cryptocurrency, and as a result many view it with a certain skepticism. It can be tough enough to understand new technology without also needing to tackle the subject of cryptocurrencies. However, Blockchain is already starting to be used in many areas in the world of finance and accounting – For instance, the Australian Stock Exchange is currently converting its systems to utilize Blockchain technology for recording all trading activity.

Financial professionals need to embrace this coming new tech wave, as it will be a major paradigm shift towards triple entry accounting.

The Coming Revolution – Implications and Opportunities

The possibilities and applications for this new technology platform are almost endless. Blockchain networks will in some ways be a whole new type of internet. Still in its nascence, the coming innovations are all still up for conjecture. But although we cannot predict all the ways it is ultimately to be used, be assured plenty of technological changes are coming soon, with many of which using Blockchain as their underlying structure.

Some potential societal mechanisms and business processes for Blockchain-based innovation;

- Settlements & Closings
- Transfers / Trading
- Vendor/Client Activity for Improved Inventory Management
- Supply Chain Verification

- Title Registrations
- Medical & Legal Records
- The Next Evolution of Social Media
- Digitized ‘Smart’ Contracts
- Voting & Governance
- Financial Reporting / Audits
- Regulatory Reporting
- Real-Time Management of all areas throughout a Value Chain

As an example, think of a restaurant or food distributor managing purchases with their vendors for supplies and food. Management must employ just-in-time inventory techniques to prevent spoilage and ensure freshness, and therefore will place purchase orders every few days. Additionally, with limited working capital and storage capacity, this can be a tenuous relationship for all parties involved. A shared database could bring increased efficiency and transparency regarding both real time inventory management and reconciliation of payments. Blockchain is already currently innovating supply chain tracking and verification when combined with GPS and new sensor technologies. Consumers can now be ensured of where their products truly are coming from, and buyers can better track a product’s location when in transit.

And the idea of digital banking is not limited to cryptocurrencies but could also pertain to safeguarding the management of important documents (e.g. Birth Certificates, Wedding Certificates, Passports, Insurance Documents, Wills, etc.). While people may still use traditional safe deposit boxes for their tangible valuables, digital safes can now allow important documents to no longer need to be physically kept at all. Think of the benefits such a system would enable for victims of a home fire or flood or natural disaster – One could quickly access their critical information (such as insurance documents) in the immediate aftermath of a tragedy.

So, what is Blockchain, and how does it work?

Tamper-Proof Data Legos

At its most basic level, Blockchain is simply a growing list of connected records, in which only new records can be added, but the existing records can never be altered.

In more technical terms, Blockchain is an open-source, encrypted database network technology, which uses cryptographic protection to ensure overall information integrity. Blockchain's architecture is replicated across a peer-to-peer network of multiple 'nodes', which validate transactions by consensus using specific mathematical algorithms. Once validated, transactions are complete and become a permanent, unalterable 'block' of data added onto the existing 'blocks', otherwise known as the Blockchain. Its innovative structure offers genuine technological transparency whereby the information is maintained on a decentralized, single communications system such that data is delivered in the exact same bit sequence as what was originally input, making the technology essentially incorruptible and instantaneous. This shared data platform can be used to automate transactions within any given system or organization, allowing numerous parties to access constantly reconciled and updated records.

Most of us played with Legos at one time or another. One of the great things about Legos is that you can build anything with them – Just like a Blockchain. Open-source means free and collaborative. With Blockchain, we all have access to a digital library full of 'Legos'. We don't have to buy software, nor will we ever need to buy updates or software licenses. In this brave new world, all the Legos are virtually free. We can all have as many Legos as we want or need.

Now, what if our Legos could hold whatever kind of information that we wanted? If each specific Lego block could be whatever we needed it to be – A purchase order for product, a payment, a posting of critical information, a signature, a vote, a title registration, etc. And what if that information on each little block was verified, encrypted and time-stamped? Finally, what if once we connected these Legos together they became permanently fused and bonded, so that they were inseparable and unchangeable?

The use of cryptographic encryption converts data into a unique cryptographic hash, which serves as the data point for the next block. The algorithms in this method are such that just slightly different data will produce an extremely different data hash. A hash is like the bumps on top of our Legos. This is where the data becomes tamper-proof, because if existing data were changed, it would drastically change the cryptographic hash such that the next block would not fit.

Blockchain technology - A growing list of connected records, in which only new records can be added, but the existing records can never be altered.

A Coffee Table in the Cloud

At the beginning of this 21st century, most of us would have defined a *platform* as a raised structure or stage on which someone might stand, and maybe some astute intellectuals would infer the word's meaning to be about the stated positions of a political party. In digital terms however, we are now surrounded by 'platforms' all the time – Our smartphones, computer networks, social media, public & governmental databases, the internet itself, and the list goes on and on and on. Perhaps, instead of 'the information age', humanity's current time should have been coined, 'the age of the digital stage', or some derivative thereof.

Nonetheless, viewing Blockchain in the context of a digital platform is helpful to understanding and appreciating it. Like any other platform, a specific blockchain can be set-up for a select group of users. When playing with our Legos, we need a place to scatter them around to build something. We can use a coffee table in our Blockchain library to gather around to collaborate with friends. So, we now have a platform with our data and other parties with whom to connect the Legos in a meaningful way – We have facilitated our metaphoric Blockchain network. The virtual table serves as a foundational platform where we can work together with clients, vendors and other stakeholders to build our Lego Blockchain while conducting our businesses. But where is this digital coffee table really? Is it in a cloud?

First, let's distinguish between the cloud and Blockchain. Cloud-based applications, despite the term's heavenly implication, keep their databases here on earth on a server(s) in some datacenter(s). This leaves cloud-based systems vulnerable to hacking or data-tampering because all their data still resides in just one place. As a result, users are forced to trust that the third party who maintains the server(s) will properly and successfully safeguard against such threats.

No Longer Relying on Trust

No, Blockchain is not up in the proverbial cloud. Since its architecture is replicated across a peer-to-peer network of multiple 'nodes', Blockchain does not rely on a trusted third-party to authenticate data nor for the protection of it's information. Without a third party, unlike other digital platforms, there is no single point of failure, thus preventing any threat of hacking or data-tampering. With no such central authority, Blockchain technology revolutionizes cybersecurity using its combination of cryptographically encrypted 'keys' for each user, along with the algorithmic computations employed by the various nodes throughout the network to authenticate data. But that's a mouthful – especially words like 'encrypted', 'algorithmic', and 'nodes'. We'll skip over those first two, but what are nodes?

The nodes, or peers, are simply anyone and/or any device on a network - employees, vendors, clients, and/or any other stakeholders in our specific communications system. What makes Blockchain so innovative is its adaptability to incorporating all the various other parties into our database network to share real-time information and better improve our processes. A traditional business network would never allow clients and vendors access to its internal database activity, and many large organizations will segregate their various departments. Blockchain can bring the entire value chain into one database community to maximize transparency and efficiency.

Venture Communism

Decentralization and synchronization differentiate this type of digital architecture. Peer-to-peer (P2P) networks are essentially digital communism – Virtual collectivism versus the individualistic client-server relationship in a traditional computer network. Political views aside however, there is safety and strength in numbers, and a P2P environment can merge resources for more processing power, higher band-with and increased storage without ever needing a central server. Moreover, replication of data means that every node in the P2P network holds all our information, because everyone on the network shares data equally. So, even if one node were corrupted or otherwise impaired, our data is still intact. Furthermore, since the shared nature of a Blockchain platform harnesses such an enormous amount of computing power, no other system would have the resources needed to override a majority of a specific Blockchain network. And ultimately, it only takes one node to preserve a Blockchain's transaction history.

Although a Blockchain ledger is replicated across a network, information separation can still be enforced as needed using the encrypted keys, which are required for users to access the network. Blockchain will typically assign each user both a public key and a private key. The public keys allow the viewing of information, while a user needs their private key to enter any data. Despite all the various nodes storing the data, users still must have the needed encryption credentials to view certain sets of information within the database. As a result, Blockchain's encryption enables the same benefits of control and privilege found on the traditional client-server model.

Signing Off Securely

The benefits of Blockchain's decentralization are not limited to the integrity and safety of our data. The provision and authentication of digital signatures is vastly improved and more secure with the combination of cryptography and use of mathematical algorithms inherent in a Blockchain network. Additionally, Blockchain technology allows for an enhanced method of time-stamping digital signatures due to the immutable aspect of each block of data. This is a key feature when considering the real-time implications of a transaction – Imagine being able to complete all the settlement and closing proceedings of a home purchase online.

Blockchain technology offers a unique solution to revolutionize the protection of our identities. With identity theft increasingly becoming industry's foremost issue in today's environment, many companies are currently spending up to 25% of their resources to protect the personal data of their customers. The very nature of Blockchain's authentication using key cryptography and digital signatures offers a far more secure method than passwords and secret questions stored on the servers of proprietary third-parties. One could envision a technologically advanced society in the not-too-distant future, which utilizes a digital identification system to carry out most of our economic and social activities. One would no longer need to keep countless passwords to various applications, but rather there would be just one single cryptographically encrypted private key, which when used is inferred to have been done so by the key's owner.

Such a system of identification could easily pave the way for a digital form of government – Blockchain could very well prove to be the medium to bring the electoral process online. No longer would voter fraud be a question or concern. No longer would there be a need for volunteers to serve as poll workers. Such a system could radically increase voter participation and bring greater accountability to elected officials. Granted, the idea of making politicians better may indeed be unrealistic, but we can always dare to dream.

Implementation and Limitations

The last area needed to fully understand Blockchain is how to facilitate and implement it.

Since Blockchain stands to be such a disruptive technology, many large companies and financial institutions whose legacy systems are at risk of being displaced by new technological innovations are racing to adapt and protect their business models. IBM is heavily investing in a 'permissioned but public' blockchain network typology. And the top accounting firms are now hiring as many IT professionals as they are accountants, recognizing that Blockchain and artificial intelligence will rapidly change many of the methods and processes currently used in finance and accounting.

To envision how a Blockchain network could be implemented for an organization, we must revisit Blockchain's architectural structure for a more in-depth understanding. In short, all peer-to-peer networks are not alike – There are three distinct types of Blockchain networks, each of which can have significantly different implications and applications. Blockchain networks can either be public (open), private (closed) or consortium, the last of which is a hybrid of a private network.

Like any digital connection, Blockchain relies on certain protocols to access a network. An open, public Blockchain network is a true peer-to-peer decentralized system. As such, anyone with a computer and an internet connection can become part of a public network. However, more computing power is exponentially necessary to run transactions on a Blockchain database for every additional node in the network. Therefore, a public Blockchain can be more expensive and will run slower compared to a private network.

Conversely, with a private Blockchain companies can control who has access. In this respect, a private Blockchain is much like traditional client-server architecture. But this also means that the network is not truly decentralized because there remains a central authority controlling who has access, as well as determining the rules of consensus. So, private Blockchains may not eliminate the need to trust a proprietary third-party. Also, in small peer-to-peer networks, there remains risk of the network being overtaken by more than half its nodes – A kind of digital coup d'état.

Consortium Blockchains are essentially a hybrid of private networks, which allow for decentralization by including pre-selected other parties. These other parties would generally be known entities – Some theorize the idea of digital *professional associations* whereby similar organizations within specific industries could mutually maintain consortium Blockchain platforms. Instead of being controlled by a single entity, consortium Blockchains are managed under a group and not under the company's control. Such a system is relatively cost and resource efficient while ensuring data privacy, yet there is no need for users to trust a third-party company.

But while this may seem the solution, this is where the technology currently finds itself struggling to take the next step. There are many start-up and established companies actively trying to be pioneers in creating commercial platforms on which companies can set up a Blockchain network that allows them to offer their customers or stakeholders freedom from relying on them as a trusted third party.

Finally, there is one last and obvious limiting issue regarding the security of Blockchain. Many critics are concerned with the lack of additional measures required for users to access Blockchain. While cryptographically encrypted keys are arguably the best and strongest security method that currently exists in a digital environment, this measure is only as good as the security of the encrypted key itself. Just like a unique physical key to a car or a house or a PIN number or password for an account, a Blockchain key could also be lost or somehow shared with another party, thus putting the user's account in the database at risk. Blockchain inherently assumes that the user of a key is the correct individual, and the technology currently has no safety net to safeguard against this type of breach. For now, multi-factor authentication can help mitigate this risk, but the technology will likely need to address such issues to maximize its scalability for future platforms and applications.