Blockchain – Business' Next New "It" Technology?

By Peter J. McAliney, Ph.D. and Ban Ang

This article is a collaborative effort of Peter J. McAliney and Ban Ang. The authors have each worked with information technology for over 35 years and bring a historical perspective to the emergence of Blockchain technology. Both started their professional careers as APL programmers, back when APL was the "it" programming language in that sector of Financial Services that would later become known as FinTech. Ang is currently looking at the technical implications of Blockchain, while McAliney is designing educational programs to meet the potential human capital shortage associated with the emergence of Blockchain as part of the global economic ecosystem.

Overview

Riding the coattails of – or in the more nuanced business vernacular of leveraging, exploiting, or capitalizing on – the latest "it" trend is nothing new.

- With the advent of the transcontinental railroad and the opening of the western United States, a small grocery store called "Gilman and Company" morphed into the supermarket chain A&P – The Great Atlantic and Pacific Tea Company. However, it was in business for over 70 years before it opened up a store on the shores of the Pacific Ocean in the western United States.
- In the early 1990's, thin clients became "Application Service Providers" and a new industry was born – and collapsed ingloriously until the next resurgence as "the cloud."
- During the early days of the internet, Halfway, Oregon, agreed to change its name to Half.com as a publicity stunt.

These examples are just a few of the ways entrepreneurs co-opted the latest trend to garner attention and grab headlines.

So, too, with Blockchain. Late in 2017, the Long Island Iced Tea Company changed its name to Long Island Blockchain Corporation and saw its stock price surge nearly 300%, albeit only temporarily. A little more in line with some reality to reflect a genuine business model, Kodak announced KodakOne, a new digital rights platform that would be built on a Blockchain with its own underlying cryptocurrency to support it. Kodak, too, saw a renewed interest in its stock as shares soared. Closer to the authors' immediate network, in a recent conversation with a colleague who is the CIO of one of the largest investment management firms in the world, he shared that almost every technology presentation made to the Investment Committee includes at least one slide that has a tie-in – real or imagined – to Blockchain.

> "Our fundamental approach to blockchain is … think about a customer issue that we want to solve and then work backwards and say how we should solve it. And, frankly, 80% of the time the answer is not a blockchain answer, people think it is, it ends up being an infrastructure issue or a business model issue. But then focus on the 20% of the where blockchain is really a good solution." [1]
>
> *- Umar Farooq, Head of Blockchain, JPMorgan Chase*

So what, then, is Blockchain?

There are already a number of technologies that have made use of the networking capability of the Internet to enhance their functionality when coupled with the browser. Is Blockchain really new, or is it the "same old same old, just a new name?" How is it different from a database (how is it similar to a database)? What is Google Sheets? It seems to have some of the attributes of Google Sheets as well – so, are there differences?

In order to gain a better understanding of Blockchain, it makes sense to revisit some of the characteristics, and attributes of some of the existing technologies, namely, databases and Google Sheets. Each of these technologies are designed for different uses and functions. Most started out existing in private networks but have evolved to take advantage of the technology of the internet. Some are centrally run on servers while the existence of the internet has made it possible for newer technologies to exist and collaborate via peer-to-peer networking. In this article, we will examine the strengths and weakness, functionality and robustness (security) of databases, Google Sheets, and Blockchain. These three technologies will be compared along the following dimensions:

- Speed
- Maturity of technology
- Access to use
- Public or private network
- Use cases
- Privacy and security
- Backup and Business Continuity
- Cost in terms of energy consumption

The description will provide some background of the evolution of each of the technologies and provide understanding of the roles they play in each use-case and the business problems they were designed to tackle.

Databases

Early Years

Databases have been around for more than half a century. Ever since computers were invented and became widely used, the need to store all the data became apparent. Data were stored on cards, then tapes and later disks. Each company implemented their own system of storage based on the media the data was stored in. Magnetic tapes were the first ubiquitous mode of storage and were read sequentially until the advent of the magnetic disks.

Magnetic disks, since they spin and are read by a moving magnetic head, enabled random access. This then spurred the invention of different file storage formats, using different modes of organizing the data – for example, hierarchical design. From these rudimentary designs, a concept of storing data as a group evolved into the databases we know today.

Different Protocols

Databases have been used to store an abstract representation of objects in the real world using hierarchical mapping or tables and relationships. The data are arranged and accessed in a logical way using supporting software called "query languages." Different database vendors developed their own method and languages using different logical schemes for storing and reading/extracting data so that users could report off of them. For example, data in some databases are stored logically in a hierarchy using a binary-tree scheme, wherein the data are related in a parent-child kind of relationship. To access any data, one has to start from the top of the tree. Databases based on this scheme saw some commercial success in the early days of computing until the advent of the relational database.

Relational databases were proposed by Dr. Edgar F. Codd, an Oxford-educated mathematician working at the IBM San Jose Research Lab in the early 1970s. The framework behind relational database theory was based on proven set-theory. Relational database are a collection of data items organized as a set of formally-described tables from which data can be accessed or reassembled in many different ways, without having to reorganize the database tables. IBM was one of the first to commercially offer a relational database based off of Codd's work.

In the early days, only text and numbers were stored. As computers started supporting different kinds of data – sound, image and videos – vendors developed new data schema to support them. Today's database can store images, video, sound files, and objects.

Google Sheets

Google Sheets and associated products are built on Google Drive, which is essentially a peer-to-peer sharing technology. Google Sheets is a poor man's version of Excel. What it lacks in functionality is made up for in terms of collaboration and sharing. A Sheets owner can invite others to share and

collaborate in working on the Sheet. The Google Drive technology underpinning this application handles security and operations – including editing and version control - among the various concurrent users.

Google Sheets, then, is an Excel clone except that it allows the owner to let others view and even edit the data stored on it. It is a spreadsheet and, as such, stores data, namely, text, numbers, charts, and objects as a database would.

This technology is the middle ground in terms of openness between databases (strictly controlled) and Blockchain (as we will see, fully open). It relies on the owner to provide access and, depending on the level of control, others may be allowed to view if an authorized user were to share it with others.

Blockchain

Blockchain has been called a database - if one is willing to apply the term database loosely. But a Blockchain is more – and also less – than a database in some respects.

Definition

A popular definition of Blockchain is that it is an open, distributed public ledger used to record transactions on a peer-to-peer network. Transactions recorded on Blockchain are open to everyone on the network and once verified as correct by peers in the network and written into the Blockchain, the information is immutable.

The open verification by peers in the network, immutability of the transactions and its visibility to everyone on the network are key differences compared with legacy database technology. There is another key difference, which will be discussed later, and it has to do with what is stored and how it is stored in the Blockchain using a computer method called hashing.

Transactions in Blockchain

The Blockchain is the mechanism for storing valid and proven cryptocurrency transactions, the most common cryptocurrency being Bitcoin. For purposes of this discussion, we will employ Bitcoin as a proxy for all cryptocurrencies. That said, one cannot describe Blockchain without reference to Bitcoin (i.e., the underlying cryptocurrency of the Bitcoin Blockchain).

A transaction on the Blockchain occurs when someone spends or receives Bitcoin. The transaction records the owner of the bitcoin, the recipient(s) of the bitcoins, the amount involved and any unspent Bitcoin returned to the original owner (think, “change” you receive in a cash purchase). Transaction records transferring of ownership of bitcoins. Transactions are secured.

Owners of bitcoin has a wallet holds an address, which is a string of 34 letters and numbers. The wallet keeps records of all the owner’s transactions and therefore balances. This address is known to everyone in the network, hence it is the public key. This public key has a corresponding private key and both are generated using a cryptographic algorithm. The owner has to guard securely the private key as once exposed, others can use it to steal the owner’s bitcoins

Is Person A wants to send bitcoins to Person B, Person A will "sign" the message by entering the amount, the recipient (i.e. public address) and together with the private key into a computer program and it generates a transaction, signed with the owner's signature, which gets send out to the Blockchain network for validation.

The transaction will be validated once it confirmed that Person A is the owner of the bitcoins and can spend the said bitcoins, etc., making the transaction a valid transaction which can be added to the Blockchain.

The data/messages in a transaction are first passed through a "hashing function", which is a complex mathematical equations that reduces everything into a 64-character long string of letters and numbers. This helps reduces the amount of storage needed to be stored on the Blockchain. The has also servers another useful function of detecting tampering to the data. The hashing function will always produce the same 64-character string each time, provided the original input has not be changed. If even a single bit is changed, a different 64-character string will be produced. This is how the Blockchain confirms that a given transaction has not been tampered with. One additional note, the hashing function is one way only. You cannot obtain the original message by passing the hash-string through the hashing function.

As stated previously, the transaction as sent to the Blockchain network is unverified or unconfirmed. A process called "mining" is used to prove that the transaction is valid. Mining is the process that validates transactions and causes it to be added into the Blockchain.

Mining and adding block to Blockchain

Miners use powerful computers to solve a complex cryptographic problem. Once a solution is found, the miner broadcasts the solution to the rest of the peer-to-peer network and if a majority of the members (nodes) in the network confirms the solution, a block of transactions is then added to the existing Blockchain. The transactions in the block become part of the official Blockchain.

The miners are rewarded for their efforts in verifying the blocks with Bitcoins. Thus mining is the process by which Bitcoins are created in the network. The miners may also receive additional fees provided by the transaction owners as incentives for working on their transactions.

Like a Database

Blockchain exists initially to record Bitcoin transactions in an open, distributed and public ledger running on a peer-to-peer network. The various computer programs that work together to create blocks in the Blockchain can be extended and applied to other applications beyond recording Bitcoin transactions.

The private key/public key signing function is useful for proving ownership. Hashing algorithms used to package transactions can be used to enforce copyrights of books and songs or other intellectual property. Finally, the immutable nature of transactions in Blockchain and its independence from any public, private or government control is a safe-guard against fraud and collusion.

Hence, many new uses have been proposed for Blockchain. Blockchain transactions can track work in progress in the production cycle; track goods in the supply chain; store medical records; store titles and deeds to land and other properties; manage student transcripts; store copyrights to books, art and songs; register votes and voters; and, other applications not yet identified. The ability to convert any digital information into a 256 bit cryptographic hash that is part of the Blockchain ecosystem makes it possible to store all kinds of data (this can be extended even further into something called "Smart Contracts," the topic for a future treatment by the authors).

In fact, to prove that you can store practically anything in the Blockchain, someone has store an image of Nelson Mandela together with a tribute to him into the Blockchain. The address below encoded the image of Nelson Mandela.

This gives Blockchain some of the characteristics of a modern database. In technical terms, a Blockchain is a "linked-list," which is a well know data structure in computer science.

Comparison

Given the brief descriptions for each of the technologies provided above, it is interesting to compare them along the criteria defined.

SPEED AND PERFORMANCE		
BLOCKCHAIN	**GOOGLE SHEETS**	**DATABASE**
Slowest. A Bitcoin block with transactions are confirmed and added to the Blockchain every 10 minutes.	Almost instantaneous depending on network traffic. Generally the number of users is small which also improves performance	Almost instantaneous depending on network traffic and number of users. Expect performance in the sub-seconds.
MATURITY OF TECHNOLOGY		
BLOCKCHAIN	**GOOGLE SHEETS**	**DATABASE**

Implemented in 2009, from Satoshi Nakamoto's seminal paper. It started as a distributed public ledger for recording bitcoin transactions. The technology is still evolving with new uses being suggested for it.	A newer technology that was designed to rival Microsoft Excel in terms of providing shared collaboration among users. Does not have the full functionality of Excel but makes up for it in terms of ease of use and shareability.	Most matured of the three technologies. It is the most ubiquitous and is used in all platforms and powers practically all industry and businesses. A stable and reliable technology that businesses can base their operations on.

ACCESS TO THE TECHNOLOGY		
BLOCKCHAIN	**GOOGLE SHEETS**	**DATABASE**
Blockchain as originally conceived is entirely public. However the technology has be used by entities both private and public to create Blockchains that are open to selected members of the public. Anyone with a computer can join the Bitcoin or Ethereum network by downloading the whole Blockchain using the appropriate software and have access to read all its contents of the Blockchain. Anyone can create new blocks to the chain provided they can prove the correctness of the transactions by finding a solution to difficult cryptographic problem and having the solution verified by a majority (51% or more) of the peers (nodes) in the network. Update or modification of the transactions in any of the block in the Blockchain is not possible. The data in the block of the Blockchain is immutable.	Anyone can create a google sheet and can invite users to read/update or add to it. Users have to be invited to participate and given access rights by the owner.	Access is centrally controlled. It is the most restricted in terms of having access to the data. a) A network administrator provides user login to the network that houses the database. b) A database administrator has to provide access to the database and the data in it. c) Finally the owner of the database has to grant rights to read, update, add and/or delete data in the database d) Not all tables and even fields can be seen by the user unless permitted.

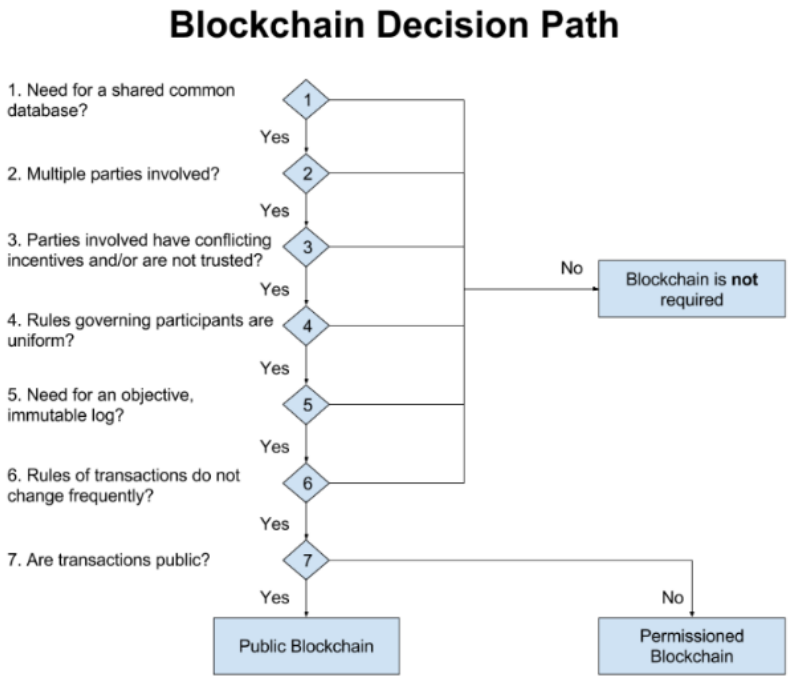
PUBLIC OR PRIVATE NETWORK		
BLOCKCHAIN	**GOOGLE SHEETS**	**DATABASE**
The Blockchain is stored on every peer (nodes) on the network. Every peer on the network has a copy of the Blockchain. The Blockchain does not reside on any one or two locations, but is in thousands of computers worldwide.	Anyone with a Google account can create them and the sheets are housed in Google cloud servers. Owner of the sheet can provide access to other users with rights as defined by the owner. The sheets can be thought of as being housed in a private cloud based network but access for all intends and purpose is public.	Databases are on private networks in most cases. However, the technology has advanced whereby the databases resides "in-the-cloud" managed by companies like Microsoft or Amazon in remote locations. The network may be public but access behaves like they are on private network. Access is only granted with the proper credentials (e.g. id/password).
USE CASES		
BLOCKCHAIN	**GOOGLE SHEETS**	**DATABASE**
Blockchain is a distributed ledger and is used to record transactions involving money and in this case, cryptocurrency. Public Blockchains like Bitcoin or Ethereum make it attractive as a ledger to not only record cryptocurrency transaction, other types of transactions as well. Finance is the first to apply Blockchain technology. However there is considerable interest in extending the technology to other areas of industry such as supply chain, healthcare, real estate (title, deeds), education (transcripts) etc. Storing large amount of data is not recommended on Bitcoin Blockchain due to the 1MB block size limit. Ethereum Blockchain does not have a block size limit but may be costly to store large data blocks.	Google Sheet is used where spreadsheets are used. It has the added feature of allowing collaboration among users. Spreadsheets are used to organize and manipulate mostly numeric data. Spreadsheet are used in many industries and businesses	Database technology is used in all businesses and industries such as retail, wholesale, healthcare, education, government etc. The economy depends on this technology to store all the data it needs to run smoothly. In other words, it is the foundational application for practically all of the economy and governments.

PRIVACY/SECURITY		
BLOCKCHAIN	**GOOGLE SHEETS**	**DATABASE**
Blockchain are on all computers on a network, hence it is fully open and public to all (public) or invited membership (private). Anyone can access the Blockchain and read its content. The security of the transaction lies in the private/public keys cryptographic algorithm used to encrypt the data in it. The private key ensures authenticity as only the owner of the private keys can sign and prove ownership. The public key ensures that others can access the data to read/verify. These two elements provide the security and authenticity. Security and authentication in the Blockchain is achieved using technology and without having any central authority acting as the gatekeeper. However privacy on the Blockchain is not fully guaranteed as it is possible using the proper tool to follow the transaction trail and owner(s).	Sheets are shared resources granted by the owner thru sharing of the document. There are settings to limit the share ability of a Google Sheet. An owner can establish a sheet wherein only s/he grants access (read/write) privileges or can allow those who s/he invites to collaborate to also share access privileges. Security, then, is very loose and open. The owner has to take extra steps to secure access to the files they own.	Databases have built in security behind a number of layers. The first layer is access to the server itself via login/password granted by the system administrator. The second is access to the database itself granted by the Database Administrator. Finally, there is access to the data in the database itself. Users can be granted read, write (insert, update, delete) access to the table or columns as designated by the database owner. Hence privacy is quite robust

BACKUPS/BUSINESS CONTINUITY		
BLOCKCHAIN	**GOOGLE SHEETS**	**DATABASE**
Blockchain has back-up inherently built into it. Every node/peer on the Blockchain network will have a copy of the latest Blockchain from the beginning of time. Every computer in the Blockchain network has a copy of the Blockchain, so backup is done without the need for any procedures or human intervention.	Most installations subscribe to Google cloud services and off-shore the tasks of maintenance, backup and recovery to Google. The company is responsible for all the server administration tasks. Alternatively they should also download the documents and store it on their own PC or some other network PCs just to be safe.	Databases are backed up periodically so that in case of failure, the data can be restored. The hardware supporting the database also has redundancy so that in the case of hardware failure, the database system switched used only the non-faulty disks. Database system supports replication of the database at different physical remote sites so that the system can pick up from where it left off if the original site is shut down due to some catastrophic event. All these backup and recovery processes have to be set up by the administrators and the sites carefully chosen. This will add additional costs to its operations.
ENERGY CONSUMPTION		
BLOCKCHAIN	**GOOGLE SHEETS**	**DATABASE**
Under the current proof-of-work algorithms, a large amount of electricity is consumed to prove a transaction is correct so that it can be added to the Blockchain. Even when the most modern ASIC (i.e., Application Specific Integrated Circuit) boards are used, the energy used is growing larger due to the algorithm inherent in Bitcoin Blockchain. Alternative methods have been proposed to find a way to reduce this energy overhead.	Minimal energy needed. A home PC will suffice to access the sheets, while the server is housed in the "cloud" and is not considered an energy "hog." In fact it may be less that all the individual database servers.	Minimal energy needed to run a database server. The use of "cloud" based database services will eliminate the need for banks of servers especially in commercial settings, e.g., Amazon AWS.

Conclusion

The three technologies – namely, database, Google Sheets, and Blockchain – are means of organizing and sharing data through a network. Each has their strengths and weaknesses, and are designed to meet certain use cases. When used as intended, the strengths of the products will help meet the user's needs. Users should be careful when labels are attached to them – as, for example, calling a Blockchain a database. Doing so can cause misunderstanding and misapplication of the product. Therefore, it is prudent to examine one's needs and requirements before choosing a solution to solve the issues at hand – sometimes the old "tried and true" is better suited to a solution than that "bright, shiny new object." The diagram below provides some guidelines to help you determine whether or not blockchain might be a solution to address your specific needs.



Source: EdX Blockchain course, March 2018

That said, Blockchain does have the potential to radically change the way business is conducted ... something substantive and positive. This is an evolving technology and it parallels the early days of the internet. The internet was built on open standards that are free to anyone. Similarly, Blockchain is built on open standards like SHA-256, private and public key signature protocol (ECDSA) and they all rely on the open standard internet protocol. The openness of the protocol has resulted in new and exciting developments to improve and expand on the utility of Blockchains and their related cryptocurrencies.

Examples of research to improve or enhance Blockchain include faster transaction confirmations (e.g. Lightning Network) and Smart Contracts. As of this writing (January, 2018), processing speed on the

Bitcoin Blockchain is set at a rate of one block per 10 minutes, whereas processing speed on a credit card network – e.g., VISA, MasterCard, Discover – is 56,000/second.[2] Lighting Network aims to confirm transactions at speeds that match that of credit card transactions. Smart Contracts, which are like distributed applications with logic to automatically execute codes and processes when certain conditions are met thereby removing any middle-person or agents.

Career Implications

The Blockchain ecosystem is a growing one and presents opportunities for trained professionals in a variety of functional areas. The potential for a human capital shortage in Blockchain-related jobs has been estimated to be as great as over 350K in the next five years. Blockchain opportunities range across a variety of potential career areas: business aspects (e.g., developing Blockchain-based business models across a variety of industries); computer science (e.g., network security, front end developers, dev-ops roles); back office processing (e.g., finance, accounting); communications (e.g., messaging the roll out of new companies, enhancements to Blockchain technologies), and; jobs that do not even exist today. Professionals who want to enhance their ability to avail of these opportunities can start to build out their skill sets to encompass Blockchain-related knowledge at both the macro level –– what it is, generally – and micro level – how I can augment my core skills to position myself to be a part of this coming Blockchain revolution.

About the Authors

Peter McAliney, Ph.D, is Executive Director of Continuing and Professional Education at Montclair State University, the second largest public university in New Jersey. Prior to his work at Montclair State, McAliney spent thirty years in the private sector. In his early career, McAliney focused on the application of technology in financial services, utilities, supply chain, manufacturing, media, and healthcare. The insights he developed working with the human side of technology and aligning business processes to support a rapidly changing competitive environment, along with his research on social networking theory and distributed work, led to management consulting roles advising senior leadership designing organizations that would accommodate the requirements of provisioning a 21st century workforce. At Montclair State, Dr. McAliney is working with the private sector, professional organizations, and his colleagues in the academy to equip an increasingly diverse workforce to acquire the skills and develop an appreciation for lifelong learning they will need to support their career success.

Phone: 973-655-6824
email: mcalineyp@montclair.edu
web: www.montclair.edu/cape

Mr. Ban Ang, is a Director in the Continuing and Professional Education unit at Montclair State University. Mr. Ang spent a decade in the Oil and Gas Industry with a subsidiary of Exxon-Mobile in Malaysia. Leveraging his analytical expertise, his focus shifted to financial services when he came to the United States where he worked with a number Wall Street investment banks and hedge funds. He developed both front-end and back-end systems supporting different financial products, such as commercial paper, derivatives, bonds and stocks. Additionally, he worked on systems assessing asset risk exposures and asset pricing, supporting and reporting to the CIO and CRO.

After leaving Wall Street, Mr. Ang continued his technology role in the education industry. At Montclair State University, he has used his data expertise in addressing the issues involved in student retention and persistence. Recently, he has been chartered to investigate the role of Blockchain applications in both education and for use by students to obtain employment in an emerging blockchain-enabled economy.

Phone: 973-655-3151
email: angb@montclair.edu
web: www.montclair.edu/cape

References

1. La Roche, J. (2018, February 7). JPMorgan's Farooq: Blockchain will have a radical impact on some of our businesses. In *Yahoo Finance*. Retrieved from https://finance.yahoo.com/news/jpmorgans-farooq-blockchain-will-radical-impact-businesses-220312432.html?_fsig=sFQsDYKaVDofxkO6LY8m5Q--

2. Vermeulen, J. (2017, April 22). Bitcoin and Ethereum vs Visa and PayPal - Transaction Per Second. In *MyBroadBand*. Retrieved July 10, 2018, from https://mybroadband.co.za/news/banking/206742-bitcoin-and-ethereum-vs-visa-and-paypal-transactions-per-second.html