Blockchain and Finance: Two Peas in a Pod

กิตตินันต์ พิศสุวรรณ[1]

คณาจารย์โรงเรียนบ้านโนนเรือตอเรือ

In 2008, an unknown developer named Satoshi Nakamoto created Bitcoin. Bitcoin was the world's first digital, peer-to-peer cryptocurrency. The most fascinating thing about it is the blockchain technology which powers it through. More and more industries are discovering the sheer utility and benefits of incorporating the blockchain technology within their system. One of those industries happens to be the Finance industry. Before we get into how the blockchain technology can potentially disrupt the finance industry, let's gain a brief understanding of what the blockchain is.

1 เนื้อหาและบทความเป็นความรับผิดของ ศาสตราจารย์ ดร. กิตตินันต์ พิศสุวรรณ Harvard Business School เท่านั้นสถาบันฯ บุคคลอื่นไม่มีส่วนรับผิดใด ๆ คณาจารย์โรงเรียนบ้านโนนเรือตอเรือเป็นเพียงบุคคลแนะนำ แก้ไข ให้เนื้อหาสมบูรณ์เท่านั้น ไม่มีความผิดใดๆ

Blockchain and Finance: Two Peas in a Pod

What is Blockchain Technology

A blockchain is, in the simplest of terms, a time-stamped series of immutable record of data that is managed by a cluster of computers not owned by any single entity. Each of these blocks of data (i.e. block) are secured and bound to each other using cryptographic principles (i.e. chain).

The reason why the blockchain has gained so much admiration is that:

- It is not owned by a single entity, hence it is decentralized
- The data is cryptographically stored inside
- The blockchain is immutable, so no one can tamper with the data that is inside the blockchain
- The blockchain is transparent so one can track the data if they want to

The Three Pillars of Blockchain Technology

The three main properties of the Blockchain Technology which has helped it gain widespread acclaim are as follows:

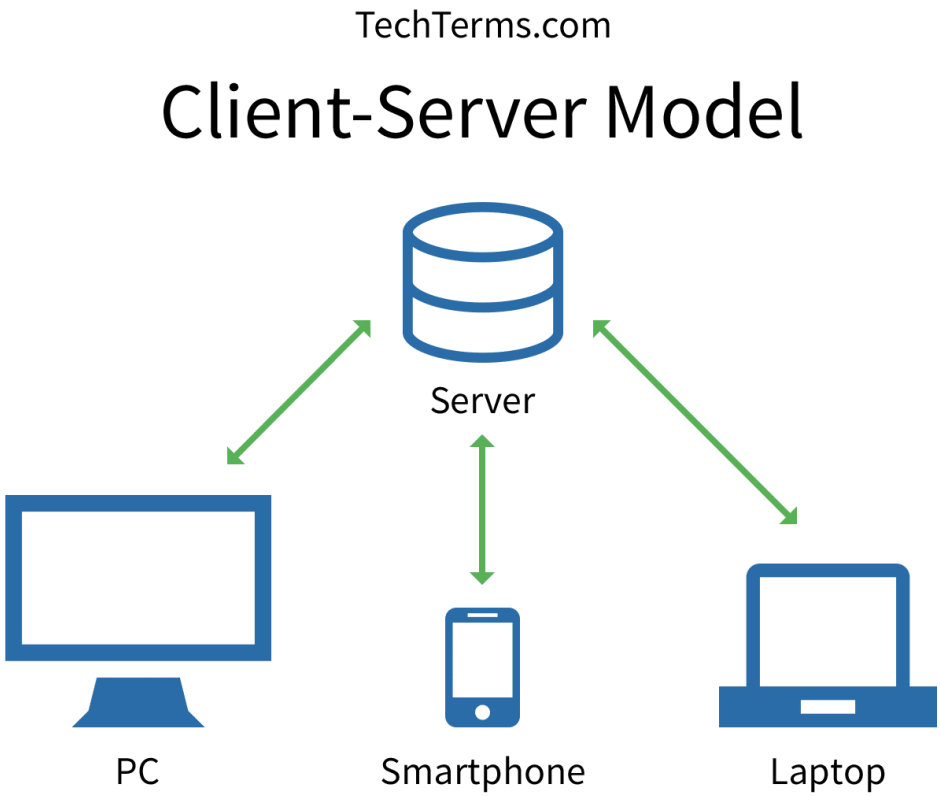
- Decentralization
- Transparency
- Immutability

Pillar #1: Decentralization

Before Bitcoin and BitTorrent came along, we were more used to centralized services. The idea is very simple. You have a centralized entity which stored all the data and you'd have to interact solely with this entity to get whatever information you required.

Another example of a centralized system is banks. They store all your money, and the only way that you can pay someone is by going through the bank.

The traditional client-server model is a perfect example of this:



When you google search for something, you send a query to the server who then gets back at you with the relevant information. That is simple client-server.

Now, centralized systems have treated us well for many years, however, they have several vulnerabilities.

- Firstly, because they are centralized, all the data is stored in one spot. This makes them easy target spots for potential hackers.
- If the centralized system were to go through a software upgrade, it would halt the entire system
- What if the centralized entity somehow shut down for whatever reason? That way nobody will be able to access the information that it possesses

- Worst case scenario, what if this entity gets corrupted and malicious? If that happens then all the data that is inside the blockchain will be compromised.

So, what happens if we just take this centralized entity away?

In a decentralized system, the information is not stored by one single entity. In fact, everyone in the network owns the information.

In a decentralized network, if you wanted to interact with your friend then you can do so directly without going through a third party. That was the main ideology behind Bitcoins. You and only you alone are in charge of your money. You can send your money to anyone you want without having to go through a bank.

Pillar #2: Transparency

One of the most interesting and misunderstood concepts in the blockchain technology is “transparency.” Some people say that blockchain gives you privacy while some say that it is transparent. Why do you think that happens?

Well... a person’s identity is hidden via complex cryptography and represented only by their public address. So, if you were to look up a person’s transaction history, you will not see “Bob sent 1 BTC” instead you will see “1MF1bhsFLkBzzz9vpFYEmvwT2TbyCt7NZJ sent 1 BTC”.

The following snapshot of Ethereum transactions will show you what we mean:

TxHash	Block	Age	From		To	Value	[TxFee]
0x2d055e4585ae2a...	5629306	16 secs ago	0x003e3655090890...		0x2bdc9191de5c1b...	0,004741591554641 Ether	0.000294
0xb4d37c791ff4cde...	5629306	16 secs ago	0x6c3b4faf413e0e4...		0xf14cb3acac7b230...	0,744767225 Ether	0.000294
0x9979410dcb5f4c...	5629306	16 secs ago	0x99bcd75abbac05...		0x2d42ee86390c59...	0,016294 Ether	0.000294
0x189c4d4aae09be...	5629306	16 secs ago	0x175cd602b2a1e7...		0xd39681bb0586fb...	0,01 Ether	0.000294
0xda0e9bbb11fb77...	5629306	16 secs ago	0x73a065367d111c...		0x01995786f14357...	0 Ether	0.00150007
0x6be498fafad9acb...	5629306	16 secs ago	0xa3eb206871124a...		0x8a91cac422e55e...	0,029594 Ether	0.000294

So, while the person's real identity is secure, you will still see all the transactions that were done by their public address. This level of transparency has never existed before within a financial system. It adds that extra, and much needed, level of accountability which is required by some of these biggest institutions.

Speaking purely from the point of view of cryptocurrency, if you know the public address of one of these big companies, you can simply pop it in an explorer and look at all the transactions that they have engaged in. This forces them to be honest, something that they have never had to deal with before.

However, that's not the best use-case. We are pretty sure that most of these companies won't transact using cryptocurrencies, and even if they do, they won't do ALL their transactions using cryptocurrencies. However, what if the blockchain technology was integrated...say in their supply chain?

You can see why something like this can be very helpful for the finance industry right?

Pillar #3: Immutability

Immutability, in the context of the blockchain, means that once something has been entered into the blockchain, it cannot be tampered with.

Can you imagine how valuable this will be for financial institutes?

Imagine how many embezzlement cases can be nipped in the bud if people know that they can't "work the books" and fiddle around with company accounts.

The reason why the blockchain gets this property is that of cryptographic hash function.

In simple terms, hashing means taking an input string of any length and giving out an output of a fixed length. In the context of cryptocurrencies like bitcoin, the transactions are taken as an input and run through a hashing algorithm (bitcoin uses SHA-256) which gives an output of a fixed length.

Let's see how the hashing process works. We are going to put in certain inputs. For this exercise, we are going to use the SHA-256 (Secure Hashing Algorithm 256).

INPUT	HASH
Hi	3639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8
Welcome to blockgeeks. Glad to have you here.	53A53FC9E2A03F9B6E66D84BA701574CD9CF5F01FB498C41731881BCDC68A7C8

As you can see, in the case of SHA-256, no matter how big or small your input is, the output will always have a fixed 256-bits length. This becomes critical when you are dealing with a huge amount of data and transactions. So basically, instead of remembering the input data which could be huge, you can just remember the hash and keep track.

A cryptographic hash function is a special class of hash functions which has various properties making it ideal for cryptography. There are certain properties that a cryptographic hash function needs to have in order to be considered secure. You can read about those in detail in our guide on hashing.

There is just one property that we want you to focus on today. It is called the "Avalanche Effect."

What does that mean?

Even if you make a small change in your input, the changes that will be reflected in the hash will be huge. Let's test it out using SHA-256:

INPUT	HASH
This is a test	C7BE1ED902FB8DD4D48997C6452F5D7E509FBCDBE2808B16BCF4EDCE4C07D14E
this is a test	2E99758548972A8E8822AD47FA1017FF72F06F3FF6A016851F45C398732BC50C

You see that? Even though you just changed the case of the first alphabet of the input, look at how much that has affected the output hash. Now, let's go back to our previous point when we were looking at blockchain architecture. What we said was:

The blockchain is a linked list which contains data and a hash pointer which points to its previous block, hence creating the chain. What is a hash pointer? A hash pointer is similar to a pointer, but instead of just containing the address of the previous block it also contains the hash of the data inside the previous block.

This one small tweak is what makes blockchains so amazingly reliable and trailblazing.

Imagine this for a second, a hacker attacks block 3 and tries to change the data. Because of the properties of hash functions, a slight change in data will change the hash drastically. This means that any slight changes made in block 3, will change the hash which is stored in block 2, now that in turn will change the data and the hash of block 2 which will result in changes in block 1 and so on and so forth. This will completely change the chain, which is impossible. This is exactly how blockchains attain immutability.

So, now you know the three pillars of blockchain technology, let's look into how it can change the financial industry.

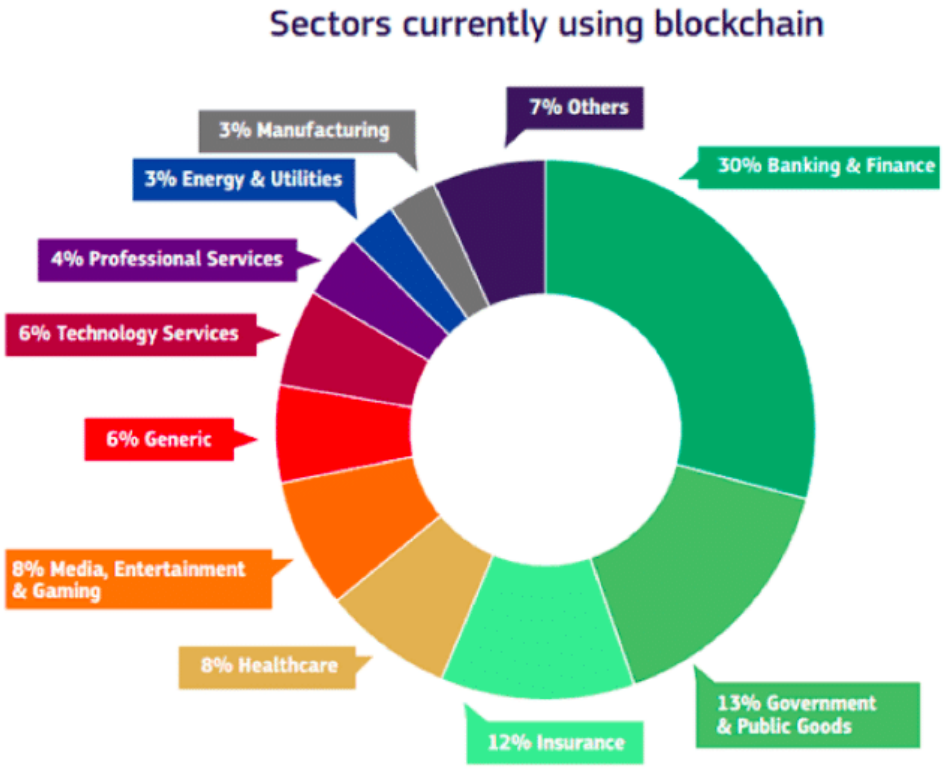
Blockchain and Banking

One of the sectors that the blockchain can actually improve is banking. Which is pretty ironic because cryptocurrencies were specifically created to bypass banks.

So, how strong can this synergy be?

The Harvard Business Review said that "**The Blockchain Will Do to the Financial System What the Internet Did to Media.**"

The best part is that it looks like the banking sector has realized the sheer potential of blockchain technology. If you look at the graph below then you can clearly see that the banking and finance sector leads the way when it comes to blockchain adoption.



So, this begs the question. Where exactly can the blockchain help the finance industry? Well, we have identified 3 specific areas. We are sure that there are a lot more, but let's focus on these three:

- Faster cross-border payments
- Cheaper KYC
- Trade Finances

Faster Cross-Border Payments

One of the biggest problems that the banking sector is currently facing is cross-border payments. On an average, an internal bank-to-bank money transfer can take up to 2-5 working days. This can be a problem in today's world especially when you consider how many people are now employed in remote location jobs.

If you have ever done any freelance work, then you would know how long SWIFT transfers can take if you are doing bank-to-bank transfer. Worse than that is if you get paid via PayPal.

If your company sends your payment on Friday, then you may have to wait till Tuesday to just get paid, because these financial institutes are always closed on weekends.

The reason why it takes so long for settlements is that there are a lot of middlemen involved who deal with the transactions in batches.

With Blockchain, settlements become user-optimized, which will save a significant amount of time and money, for both parties involved.

The blockchain completely removes the need for middle-men because the transactions are settled near instantly (if a permissioned chain is used).

In fact, that's not mere speculation, there is already a working PoC of how blockchain technology can exponentially reduce transaction times in these areas.

SAP recently collaborated with ATB Financial and fintech startup Ripple to send the first international blockchain payment from Alberta, Canada to ReiseBank in Germany. The bank used the SAP HANA Cloud Platform and the SAP Payment Engine application to take advantage of Ripple's pioneering blockchain network.

The $1000 CAD (€667 EUR) blockchain payment, which would typically have taken from two to six business days to process was completed in about 20 seconds. The proof of concept has since been enhanced, and we are able to complete the transactions in just 10 seconds.

From 2-6 business days to 10 seconds. Now, that is disruption!

Cheaper KYC

Let's looks at one of the biggest places where Banks lose a lot of money, Know Your Customer (KYC) regulations. Here are some pretty shocking stats that we got from this article.

- An average bank spends £40m a year on KYC Compliance. Some banks may spend up to £300m
- JP Morgan has reportedly spent up to a staggering £1.6 billion on their compliance department and employed more than 13,000 people to keep track of regulatory changes

- 70% of the 722 corporate correspondents, who took part in the survey by Reuters, said that client on-boarding can take up to 2 months while 10% claimed it can even exceed four months.

The two chief culprits are:

- The ever-changing regulation policies.
- Draconian methods which are still followed by certain banks. Some banks still do their compliance process using papers.

So, how will the blockchain technology change this space? Well, there are two ways that it can work.

Firstly, there is the concept of self-sovereign identity. Self-sovereignty is the idea that it is an individual's moral right to have ownership over their own body and life. Self-Sovereign Identity (SSI) is critical now, more than ever, because each and every company and entity has an online presence. Having so many siloed identities greatly increases the chances of online fraud or identity mismanagement.

By uploading your identity to the blockchain, you have full and complete control over yourself. So, how will that help with KYC? Suppose you have to go and open an account in a bank, the bank will simply ask you to give access to your identity instead of a centralized third party.

Secondly, the banks could be part of their own private and permission blockchain network (more on this later). Now suppose Alice has completed KYC regulations with Bank A, they can then simply upload the details on the blockchain. Since the blockchain is not owned by the central repository, anyone, who is part of the network can upload information and share it with everyone else.

Suppose Alice wants to open an account in bank B. Instead of starting the whole compliance process from scratch, they can simply access the blockchain and get the required KYC data.

The blockchain's KYC protocol can help in both intra-bank and inter-bank functions:

- Intra-Bank: The KYC which has been performed by the bank can be used by another branch of the same bank. This leads to a smooth transference of services.
- InterBank: The KYC performed by one bank can be used easily by another bank.

According to a report co-authored by Santander, it's estimated that blockchain technology could reduce banks' infrastructure costs alone by up to $20 billion a year.

Trade Finance

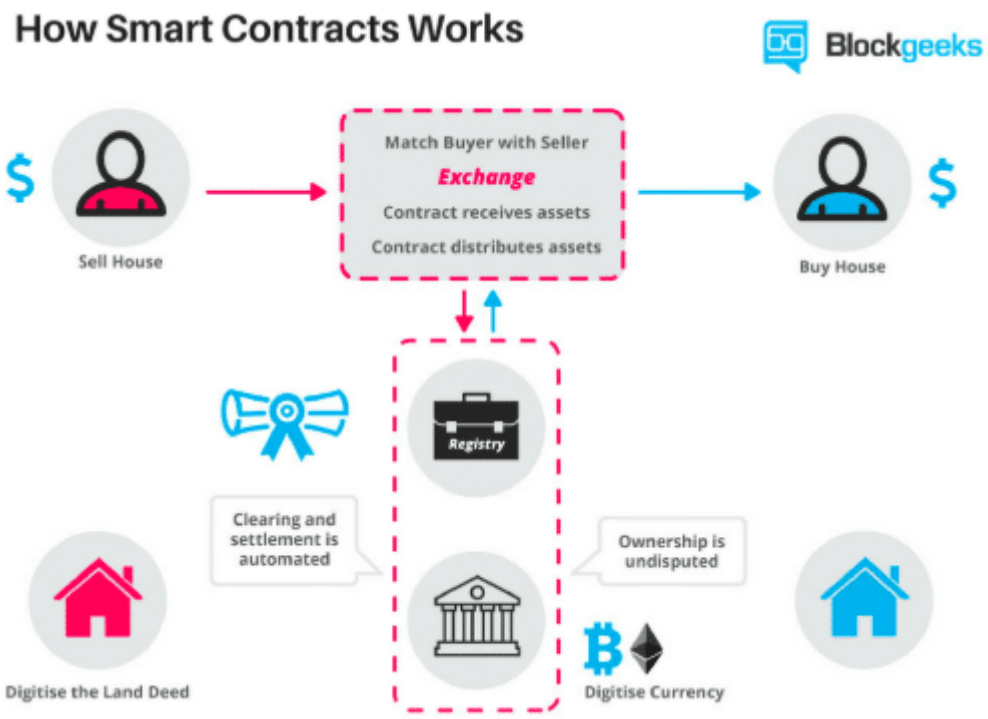
Charley Cooper, the managing director of R3 consortium, believes that trade finance is the ideal sector which can be disrupted by the blockchain. He said:

"Trade finance is an obvious area for blockchain technology. It is so old it's done with fax machines and you need a physical stamp on a piece of paper."

As of right now, there are a bunch of parties which are involved in trade finance. Unfortunately, these parties make the whole process very slow and cumbersome. They can't really trust each other, and the only way they can go ahead is by getting in even more middlemen like banks and clearing houses.

The way the blockchain can help here is via smart contracts.

Smart contracts are automated contracts. They are self-executing with specific instructions written on its code which get executed when certain conditions are made.



Smart contracts are how things get done in the Ethereum ecosystem. When someone wants to get a particular task done in Ethereum they initiate a smart contract with one or more people.

Smart contracts are a series of instructions, written using the programming language "**solidity**", which works on the basis of the **IFTTT logic** aka the IF-THIS-THEN-THAT logic. Basically, if the first set of instructions are done then execute the next function and after that the next and keep on repeating until you reach the end of the contract.

The best way to understand that is by imagining a vending machine. Each and every step that you take acts like a trigger for the next step to execute itself. It is kinda like the domino effect. So, let's examine the steps that you will take while interacting with the vending machine:

Step 1: You give the vending machine some money.

Step 2: You punch in the button corresponding to the item that you want.

Step 3: The item comes out and you collect it.

Now look at all those steps and think about it. Will any of the steps work if the previous one wasn't executed? Each and every one of those steps is directly related to the previous step. There is one more factor to think about, and it is an integral part of smart contracts. You see, in your entire interaction with the vending machine, you (the requestor) were solely working with the machine (the provider). There were absolutely no third parties involved.

Smart contracts on a blockchain, which execute automatically, will transfer title to goods and money, remove the need for banks to provide documents, such as letters of credit. What this does is it completely cuts out all the unnecessary middlemen and their fees. It also helps in creating an ecosystem which doesn't require any trust in any particular party.

A global trade finance platform named Batavia was launched by IBM along with a consortium of five banks, UBS, Bank of Montreal (BMO), CaixaBank, Commerzbank and Erste Group.

The consortium aims to support the creation of multi-party, cross-border trading networks by establishing Batavia as an open ecosystem that can be accessed by organizations big and small around the world.

Upcoming Obstacles

There are a lot of obstacles that the blockchain technology must overcome in order to gain adoption by financial institutes.

- Firstly, they suffer from scalability issues, which we have covered in length before. Financial institutes need to deal with millions of transactions per second and the current blockchain architecture is just not ready to cope with that demand.
- Blockchain technology depends on public key cryptography. One can unlock the assets sent to them only with their private key. There is a potential for those keys to be lost and misplaced. This allows its owner to change the ownership of assets recorded on the blockchain.
- There are still several interoperability issues that the blockchain needs to work on before it can be adopted widely by financial institutes.

Conclusion

It seems that the blockchain technology and the financial sector are made for each other. While it is true that they do have some obstacles to overcome, the fact is that the sheer utility that it brings into the space is seriously exciting. Let's wait and see the projects that are going to come out in the near future to know for sure. However, when all is said and done, it looks like the blockchain technology can seriously disrupt this industry in a positive way.

Reference :

https://blockgeeks.com/guides/blockchain-finance

https://blockgeeks.com/