
dragonfly
FINTECH

Blockchain Technology, the New Paradigm

Abstract

A blockchain is a system to share distributed data in a robust and mathematically secure way. Due to the ubiquity of data at the core of many real-world systems, blockchain technology is already revolutionizing data processing in many domains. Blockchain technology, its subtle nuances, improved functionalities and features are discussed. Dragonfly Fintech is a company that utilises the salient features and functionalities of our improved blockchain technology, and introduces them into the financial industry with the aim of realizing a holistic, end-to-end system in the area of financial settlement and mobile payments. This includes the use of this technology for banking compliance and governance as its key offerings.

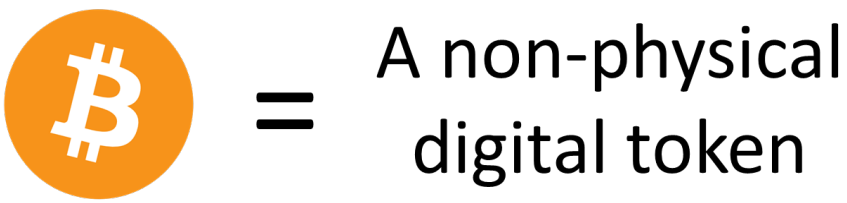
Introduction

Blockchain technology is changing the way finance, trade, and commerce are done. In fact, the implications of blockchain technology do not stop there, as it can be used for streamlining many more business processes outside the financial domain.

Blockchain technology was first introduced almost 8 years ago by Satoshi Nakamoto, the inventor of Bitcoin. The irony is, while this technology has been in existence for almost 8 years, not many can differentiate between blockchain technology, Bitcoin, and the Bitcoin blockchain technology. For the novice, these 3 terms are used interchangeably without reference to the actual differences between them. Most will equate this to just Bitcoin. Due to its use in the criminal underworld, many automatically equate Bitcoin to something that should not be touched with a ten-foot pole. This wrong notion of Bitcoin being something bad, calls for another topic of discussion, which we will not delve into in this article.

It is important to look at the profound underlying differences between blockchain technology, Bitcoin, and the Bitcoin blockchain, and in particular, the blockchain technology. Semantically, they are 3 different types of things we are referring to.

Let's first take a look at what Bitcoin is. Bitcoin is a unit of value. Its value is derived from nothing more than the perceived value that is market determined. Now, Bitcoin is non-physical in that there are no physical coins, and everything is transacted in a virtual environment. People who own Bitcoin actually store it in a digital wallet, somewhere in a storage disk or with a service provider. Bitcoin is not



Value of a Bitcoin is market determined. A transfer of a digital token between two parties represents a transaction to be recorded in a Ledger, simply called, a Blockchain.

entirely anonymous, but for most purposes, it is anonymous enough to be used for activities that are thought to be illegal—money laundering, crime, terrorism, and fraud—and therefore, Bitcoin is not well received by the financial industry or the population at large.

So, how do we keep track of Bitcoin transactions? How are transactions verified so that there is no chance of double spending the same coin? How can a person who owns a Bitcoin in her wallet actually knows that the Bitcoin belongs to her?

In the traditional management of funds, there exists a ledger, such that when money moves around, the value and balance of each transaction is entered into the ledger. Fraud can happen by fixing these numbers in the ledger and changing entries. Banks are entrusted to keep account of these ledgers. They are regulated and therefore they are believed to be trustworthy. But what if a group of banks are entrusted to manage one single ledger such that any transaction that can be verified by the majority is said to be true and correct? In other words, if more than 50% say that the transaction is true and correct, then this is entered into a giant global ledger and "cast in stone." The rest of the banks who do not agree (i.e., the minority) are either kicked out (fraudulently acting perhaps) or kick themselves out, or are forced to agree to the transaction and continue with correcting their ledger to reflect the same as everyone.

What if all these banks keep a same copy of the transaction ledger and agree or disagree to every entry into the ledger and keep updating it concurrently across, with the assumption that if any transaction gets more than 50% agreement in the consensus, it gets entered into the ledger? Those that fail to get consensus, will get their transactions rejected and voided.

In the current financial system, it is rather hard to implement such a system whereby all banks come together to form one big giant consortium and get everyone to sit together to agree to every transaction. It is impractical and not feasible. However, if we put a microscope to what the financial system is doing, they are in fact doing this somewhat. These include International Settlement systems and large Automated Clearing Houses. At the country level, each central bank will have their own country's settlement system. These are in fact ledgers of some sort. But they are largely disparate and form a complicated, and complex fabric of networks and systems. They create multiple gateways to talk to one another, creating a giant mess. This itself, creates transaction latency which is unnecessary, and increases costs.

Following the global financial crisis in 2008, Bitcoin was invented so that we could "unleash" ourselves from financial slavery, very much based on the ideals of libertarianism. When Bitcoin was invented, it was based on the need to create a giant ledger, where no one has absolute control, and whereby all entries are automatically accepted or rejected. There was also a need to ensure that numbers and transactions are irreversible and immutable, a foolproof public ledger system. In summary, Bitcoin was invented with the following in mind:

- A currency as a medium of exchange

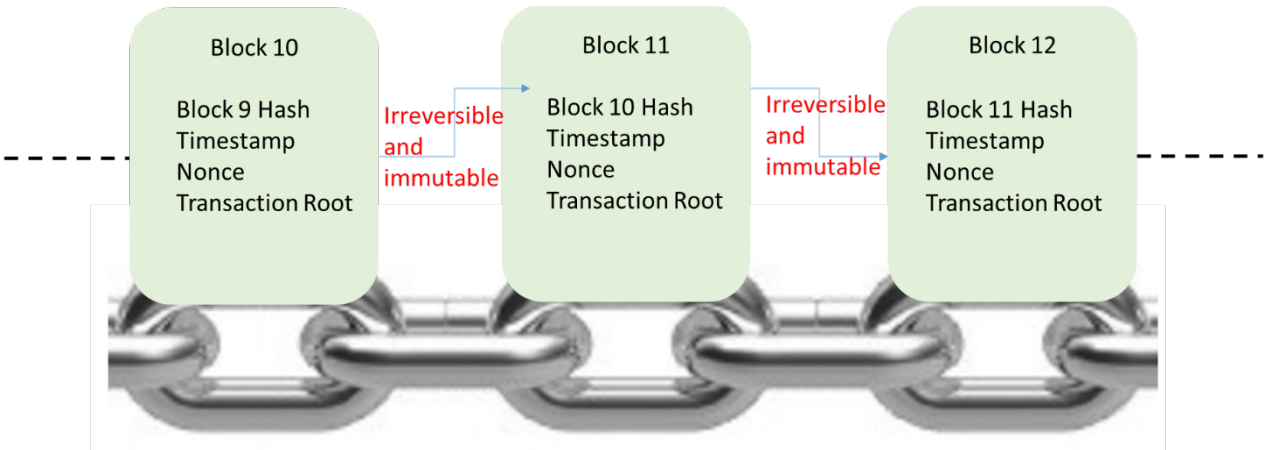
- No one controls this currency
- In order to obtain this currency, one must mine it, very much like real world digging and mining for gold, but instead, uses computer systems to do so
- Have a system to secure and verify transactions based on cryptographic public and private keys
- Have a public ledger to secure the creation of Bitcoins (i.e., mined coins)
- A ledger system to keep account of transactions, and that is immutable and irreversible
- A system that cannot be destroyed by any authority and exists as a peer-to-peer system on the Internet; the participants are the system

Bitcoin, the medium of exchange, was the main thrust in its creation. It is an amphibious medium of exchange, bearing all the qualities of a digital currency while also having the properties of a commodity. It took the world by storm and threw regulators off balance as it cannot be classified as fiat money. It remains largely unregulated.

Because it is unregulated, people have purportedly used it for terrorism, crime, fraud, and money laundering. But if looked at in the larger context, conventional fiat money, such as U.S. dollars, is by far an even larger base for all those crimes. They go into the trillions. Bitcoin is in no way anywhere close to that, even if we used all the Bitcoin available for illegal activities. There are more reasons why Bitcoin is "dangerous." The bottom line is, Bitcoin (and all similar initiatives known as altcoins, such as NEM), is actually a very powerful invention that all governments fear.

Bitcoin Blockchain Technology

Now, to the more interesting part, which is the decentralized ledger, more commonly known as the blockchain. Bitcoin needed a blockchain to manage its transactions. Public/private key cryptography is used to manage and maintain the blockchain. Cryptography is a proven technology that has existed for thousands of years, including smoke signals that the Native American indians used in the days of yore. The cryptography today is much more sophisticated and uses computers to generate the outputs. For the purpose of our discussion, suffice it to say that cryptography uses a form of unique digital signature or seal to verify transactions



Blockchain - each block of transactions (as they become recognised as valid transactions) is tied to the previous block by way of a hash, following a sequence. Changing any previous transaction value in the chain to cheat, will change the sequence, thereby changing the entire blockchain integrity, just like how DNA is unique to an individual and cannot be changed. Each block of transactions is periodically generated, e.g., every 10 minutes.

(i.e., to ensure that a transaction is true and correct between two parties), and subsequently to prove ownership of a transaction when it gets put onto the Blockchain (i.e., to enter the transaction into a ledger, making it immutable and irreversible).

Before a transaction is confirmed (i.e., entered into the giant ledger maintained by all nodes in the peer-to-peer network), it undergoes a couple of steps:

1. Each participant (i.e., a computer node) bids to create and confirm the next block of transactions (the mining process) with only one successful node being allowed to do so.
2. A simple majority of nodes agree to a set of transactions for that block.

In the bidding process, and in order to have the privilege to provide proof for the records in the ledger, all nodes undergo a puzzle solving competition. Known as mining, the first one that gets a puzzle solved gets to confirm the batch of transactions into the ledger.

In the block creation process, a set of verified transactions are batched together as a set of transaction records, and cryptographically signed. When it is signed, it uses the output of the signature (called the hash) from the last batch of transactions, thereby creating a link from the preceding batch of transactions to the current batch of transactions, essentially creating a chain of batches of transactions, where the links are cryptographically signed and sealed. Any breakage of the link is like breaking the seal and therefore rendering the chain as tainted. The end result, is a tamper-evident set of records.

Every participating node will keep a record of the same set of confirmed transactions and they will check against each other to ensure everyone else is keeping the same set of data at all times. The term blockchain comes about from each batch of transactions being a block of transactions that are linked to previous blocks of transactions like a chain. Hence, the word blockchain. A blockchain is therefore a database of transactions from which the ledger of transactions can be built. Blockchains that live on a public, peer-to-peer network are in the public domain and everyone can see all transactions, albeit it is hard to identify exactly (but not impossible) who the transacting parties are unless one is a party to the transaction.

We have defined what a Bitcoin is, and we have further explained in layman terms, what the Bitcoin blockchain is. The Bitcoin blockchain is a complicated mathematical process that has many complicated intricacies. It has proven itself to be a very solid solution. Since its creation in January, 2009, it has not been breached and is working solidly as a proof of concept, running 24 hours a day with zero downtime.

Although contentious among so-called Bitcoin “maximalists,” Bitcoin is essentially a proof of concept. It has demonstrated that:

- It is possible to create an alternative to fiat currency, where no one party controls its issuance
- Blockchain technology can be used efficiently and securely for many uses beyond just Bitcoin transactions
- Cryptography can be used to create immutable and irreversible records
- Distributed transaction management can be made simple

However, as Bitcoin is a first generation product, there are many flaws in its design, mainly stemming from poor usability. These include:

1. Slow transaction confirmation time—depending on the required certainty of a transaction, it takes about 10-60 minutes to confirm or verify a transaction in practice
2. The software is hard to use, often requiring third party enhancements and services
3. Requires a long time (in days) to start up a standalone wallet, which is impractical
4. Solution is not user friendly and is targeted at only expert computer users
5. Lacks real life usability, which often has to be augmented by third parties, which adds to the bulkiness of the solution and opens the door for security holes
6. The existence of a myriad of third party offerings, disparate as they may be, creates a situation where the solutions offered are not holistic
7. Require expensive machines to run its nodes and is therefore wasteful in the use of electrical energy and capital costs

A recent proposal to make changes to the Bitcoin project has been met with factions wanting the project to be changed in their own ways. This resulted in months of unfruitful debate, ending in indecision. The very tenet of the concept of a decentralised consensus where no one entity or a group of cabals can rule the Bitcoin blockchain was put to test and shown to have failed miserably. It is no surprise. After all, this was meant originally to be a proof of concept, but instead it took off as a solution and a claimed panacea, which, with the benefit of hindsight, does not seem to have been realistic. In the meantime, the bad publicity of Bitcoin is not doing it any more good.

Emergence of blockchain technology as a class of technology in its own right

No financial institution will want to have anything to do with Bitcoin because of its bad publicity and the risks in doing business using Bitcoin from the perspective of having to deal with regulators. Hence, Bitcoin did not quite take off. Unfortunately, much money has been invested into the Bitcoin project. Many are not seeing it going anywhere. In their desperate attempts to promote its use and therefore protect their investments, many have started promoting the use of the blockchain. They have branded this as the Bitcoin blockchain. The fad is now focussed to working on the benefits of the Bitcoin blockchain technology. More people, including financial institutions are putting their money into the Bitcoin blockchain technology. Many will again fall into the trap of this new hype. The Bitcoin blockchain is a first generation proof of concept. It is “old” and not quite

useable for industrial applications. Liken this to an old Ford Model "T," compared with the cars of today.

It is undeniable that the blockchain technology is very powerful. The existence of the term *Bitcoin blockchain technology* came about because, since late 2013, a slew of new software solutions emerged that emphasised the use of the blockchain technology more so than the coin itself. They called themselves *Crypto 2.0*. Bitcoin had to follow suit, and hence the term Bitcoin blockchain technology came about and was made popular. However, this is just old wine in a new bottle, with external embellishment.

So, what is Crypto 2.0, and more specifically, blockchain technology that should be? Blockchain technology is now the new branch of technology and covers all projects based on the original concept of the Bitcoin blockchain technology. It has since morphed itself into many varieties that are more powerful and useable than the original Bitcoin Blockchain technology. In short, Bitcoin blockchain technology has taken a backseat with the emergence of newer blockchain technologies today.

The NEM project blockchain technology solution

The first known new blockchain technology came about in late 2013, called the NXT project. Its bidding for creating blocks and confirming transactions took a different approach. The method of confirming batches of transactions are similar in nature. i.e., they use cryptography. But the construct and architecture of the blockchain gives more flexibility to its use. The NXT project shed new light on the potential of blockchain technology. However, because its development was haphazard and not well engineered or coordinated, it has since been used more like a technology playground rather than finding practical uses in the real world. Though, great ideas have undeniably came out of it as an experiment.

Of particular interest is the NEM blockchain project. First put to use in mid-2014, this project has more coherence and was specifically designed and targeted at real world use. It is also being professionally engineered, with excellent coordination involving thousands of people. Among the superior features that NEM has over the old Bitcoin blockchain technology are the following:

- Faster transaction confirmation or verification time—1-10 minutes, (customised and centralised transactions can be instant).
- Higher transaction handling capacity – 2 transactions per second (tx/s) and tested to go beyond 100 tx/s in a *permissioned* blockchain (more about this later).
- System-level multi-stage verification transactions (also called multi-signature transactions) – Liken that to multi-party approval of a transaction before a transaction can be confirmed. Particularly useful for financial institutions where this is a necessity for multi-stage approvals of a transaction to satisfy compliance and governance measures.
- Ability to create different types of fungible digital currencies, thus realizing a multi-currency environment.

- Ability to create any arbitrary digital asset. This could be useful beyond the digital realm and into the real world by proving ownership of objects (e.g., a car registration) or identity or certification (e.g., driver's license).
- Use of a thin client in a standard client-server architecture. What this means for users is that they do not have to wait long for the system to boot up and then transact. It is a fast booting system that can be used immediately. It is especially suited for mobile devices, where it can be directly connected to the blockchain without an intermediary, unlike the Bitcoin blockchain project.
- Completely different architecture from the old Bitcoin blockchain architecture, in that it uses a tiered architecture, synonymously known as web architecture (or client-server) with browser-based solution (or standalone), and fully secure.
- The design of the architecture allows for solution extensibility and flexibility.
- Allow the use of different programming languages to interact with the blockchain directly.
- Spam resistant filter, server reputation system, and a peer-to-peer network time service are all features that are unique to NEM and have not been implemented before.
- Use of inexpensive and low-power machines to maintain the network (as opposed to using the Bitcoin blockchain solution)—lower capital and operating costs.

As opposed to the original Bitcoin blockchain design, this next generation blockchain technology takes blockchain technology one notch up. Solid engineering practices and system stability make it more suited for real world financial use.

The NEM Blockchain project is currently the best designed project and was developed from ground up. It was developed taking into consideration the following:

1. Pitfalls from previous projects
2. The need to ensure that the solution will fit real world financial systems

It is one of the few projects in the cryptocurrency domain that actually ignores most of the libertarian and techno-centric bells and whistles that have no real world application. Its main purpose is to satisfy the requirements of real world use cases.

Most financial institutions fall into the trap of “simply” choosing the defacto Bitcoin blockchain and work on it. Soon, they will realise that they are actually walking up the wrong path when they find that the Bitcoin blockchain that they know, has problems that are hard to work around in practice.

The NEM blockchain project recently made a special blockchain called a *permissioned blockchain* (named Mijin; www.mijin.io). Permissioned blockchain is a technical term used to describe how a single entity can maintain their own independent blockchain that cannot be joined by anyone on the outside, thus

allowing the entity full control of the blockchain. Financial institutions in particular will find this approach more palatable and suitable for their use.

The transaction handling capacity for a permissioned blockchain has been tested to scale to 1000 tx/s easily. This depends primarily on the latency of the network. If the nodes are connected at 10 mbps, this can be easily achieved. In any case, it is worth noting that a country like Malaysia with a GDP of about $10,000 per capita, potentially does about 100 tx/s as a country. Hence, for a bank to do 100 tx/s, it is a lot, i.e., about 3.154 Billion tx/annum. Current NEM technology can thus easily scale to handle entire countries.

Utility of a Crypto 2.0 blockchain

A Crypto 2.0 blockchain and the technology it employs can be used for a myriad of things. These could include the following:

- A multi-currency international settlement system
- An equity settlement system, cutting down the requirement of a T+3 to same-day or instant settlement
- A mobile payment solution
- Record keeping and proof of ownership, e.g., titles, cars, etc.
- Identity management
- Compliance and governance management
- Workflow process management
- Loyalty point management
- Event-triggered contracts, e.g., fixed-deposit auto renewal with an auto interest payout
- Hire purchase financing management

In fact, the blockchain can be used for anything that requires a ledger to keep a record of transactions, be it financial transactions or text transactions (i.e., stored data such as a title or a specific instruction message).

Bank account transactions have certain requirements where funds can be frozen or reversed. On the surface, with the blockchain being an irreversible and immutable ledger, this might not be suitable. The NEM project has provided this flexibility with the all-important multistage verification solution. For example, if an account is frozen, the bank, through its processes, can prevent a transaction from being verified, effectively freezing an account until further actions have been taken.

Similarly, with regards to reversing a transaction, the transaction can be reversed by making a special transaction to send the amount back to the originator or to a specified account. This can be done through the use of a specially designed master key system in the bank to create a reversion of a transaction.

The NEM Blockchain method of multistage verification gives much flexibility on the use of the Blockchain to address a bank's special needs.

By the same extension, this powerful feature can be used for many more use-cases where multistage verification is the norm, across all industries.

Barring all the intricacies of a banking system, of which most of them revolve around the need for compliance and governance, the blockchain technology represents the crux of multi-party settlements and transactions, involving Bank-to-Bank (B2B) settlements as well as B2C, and C2C transactions. The underlying requirement of a banking system is a solid ledger and the blockchain technology sits at the core of it.

Suffice it to say then, that in the coming years, the blockchain technology will evolve into a powerful core solution for banking systems from the cost and ease of integration standpoint. It may not entirely replace current systems immediately, but it should in the long term phase them out.

The Dragonfly Story

Dragonfly Fintech (DF) uses the core technology of the NEM project to address seven key strategic implications of the current financial industry by using the blockchain technology. These are:

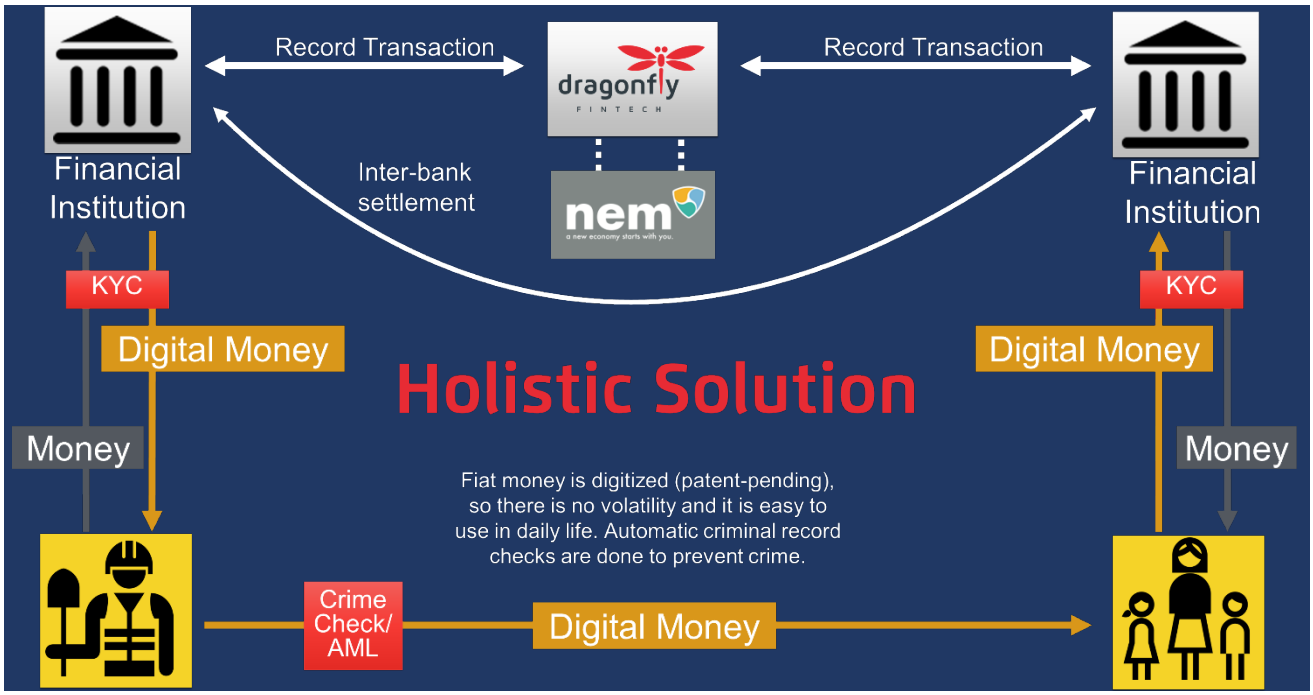
1. Compliance should be managed at the transaction level.
2. It should be easy to integrate a new system with existing systems through a simple interface.
3. Near real time transaction confirmation is required to minimize liability from fraudulent transactions.
4. Ability to handle high transaction capacity to the order of 1000s of transactions per second.
5. Ensure that the bank is in full control of the blockchain.
6. The ability to enable transactions to be carried out in different currencies.
7. There is a need to provide secure, instant access to the service, with no down time.

At least 60% of the cost of a transaction is said to be from compliance and governance issues. Given the disparate nature of the financial industry in South and South East Asia, and exacerbated by the fact that much of the populace is unbanked and underbanked, this is a major challenge for many of the countries in the region. The idea is to provide a multi-stage service.

The blockchain to be deployed by DF has been tested to run consistently at 100 transactions per second (3.15 billion transactions per year), which will satisfy most banking needs currently. But DF shall also work on scaling to thousands of transactions per second.

In a permissioned blockchain, nodes are run by the banks themselves and they will put in the necessary security features to ensure that these nodes are protected from being simply accessed by anyone. With a majority of nodes that are fully trusted, transactions can be instantly approved.

Blockchain technology is new, but the computer cryptography that goes with it is at least 40 years old and is well proven and tested. The blockchain has been fully weathered and exposed to the world at large for 8 years. No one has ever come close to hacking the blockchain. It is important that government regulators understand that most of the compliance and governance processes still reside within the banking environment and have not changed. It is only a method of storing transaction records in a cryptographically secure environment.



DF's blockchain solution supports multiple currencies, and each digital currency can be in different currency types in an e-wallet. This allows for easy borderless transactions, which is the core of its offering in the unbanked and underbanked regions, especially migrant worker remittances. Having said that, our solution does not preclude a banked customer from using it in an ecosystem where merchants will accept mobile payments, including using Near Field Communication (NFC) or chipped devices. Case in point is when a sophisticated user can spend money whether in the home country or in another country, where a merchant will accept mobile payment using the DF solution. With multi-currencies, the user can pay in whatever currency the merchant accepts.

NFC devices are devices that are now being deployed by Apple Pay and found in most smartphone devices. They operate in the same manner as Bluetooth devices but they are more suited for "touch on" transactions at the point of sale.

DF is well aware that to integrate with the banking system is a nightmare. As such, it is important that a good set of libraries or Application Programming Interfaces (APIs) are put in place that adhere to standard industry practices. DF's approach is to provide such an API set so that legacy systems can integrate directly with the blockchain using any programming language which is compliant to the industry standard. DF's set of APIs work directly with the blockchain.

Finally, no bank will ever allow its system to be shared. The existence of a permissioned blockchain offering by DF makes it acceptable to banks, and the regulators. No bank will share its blockchain, and in this instance, the blockchain will be under their full control and purview.

Conclusion

DF is ready to roll out its core engine solution for a global payment, clearance, and settlement system. Further, because of the intricacy and complexity involved in the rollout, a Platform as a Service (PaaS) paradigm is the way forward. Our core offering is holistic and leverages on superior and inexpensive technology, while at the same time, assuring seamless integration with the client's business processes. DF is a world leader in the field of blockchain technology for the banking industry, having worked on this since 2013, filing a provisional patent in 2014, and has a well-tested core blockchain technology that has been running for close to 17 months. Essentially, DF is at least 2 years ahead of its competition.