NEM CATAPULT

LON WONG
Dragonfly Fintech Pte Ltd.
NEM Core Team Member
E-mail: lwong@dfintech.com
November, 2016

Abstract: A major challenge for financial institutions is the inherent inefficiencies of multiple ledgers within their systems. A blockchain solution with multiple ledgers for multiple assets provides a transformation approach to addressing this issue. We present the all new Catapult blockchain solution platform based on the original NEM technology and concepts. An open platform, the solution is designed to bring down the cost of implementation and ownership, and is a solution that will power the present and future needs for blockchain driven solutions. The Catapult solution is architected to allow for easy integration with most applications, and therefore is agnostic to existing banking standards. It allows for interoperability between blockchain instances thereby permitting shareable and non-shareable data to co-exist in a homogenous environment. This paper is intentionally written to address a wide spectrum of readers.

Keywords: Catapult, Mijin, NEM, Tech Bureau, Dragonfly Fintech, blockchain, smart contract, permissible chain, open system blockchain, banking standards, multi-ledger.

Table of Contents

1. INTRODUCTION

The NEM blockchain technology has been around for more than two years. Designed with mainstream applications in mind, it is the intent, therefore, that the NEM team should develop a solution based on what it can do in the most extensible manner. The focus of the NEM project has always been to unleash the power of the blockchain technology as a priority and quickly allow projects to build applications on top of this platform and realise the power of the blockchain technology.

We are of the opinion that blockchain technology is trying to find its place in the industry, but lacks uniformity in approach and standards. From what is available in the market space, one can immediately conclude that most blockchain initiatives revolve around the blockchain ledger, all with subtle variances on how the blockchain is run, and with slightly different flavours.

Our approach takes a different twist. Functionalities and features of a powerful blockchain are not our only emphasis. We have incorporated equally important elements that are hitherto subject to much neglect. These include:

1. allowing any solution to sit on it independently;
2. an abstraction layer with a full suite of APIs, allowing for ease of integration, and thereby harnessing the power of the blockchain ledger; and
3. scalability.

The purpose of this paper is to describe how NEM achieves this and how NEM as a solution, is a best of breed solution that not only serves a very important role as a blockchain technology but also sets a new standard for blockchain technology.

2. RELEVANCE

Blockchain technology is a ledger solution. Naturally, as a ledger, its distinct feature is particularly relevant to the financial industry, too. All financial institutions use the ledger as the single most important element in its core banking solution.

Unfortunately, it is a well-known fact that many applications built upon the ledger for various banking services are designed based on proprietary ledgers befitting each service application.

Over the years, the number of ledgers and applications grow and reconciliation becomes a massive problem.

A compounding effect and risk exist when banks start to transact among each other, each with a plurality of systems that may or may not be compatible. Built over decades, these systems have become a monolithic mash that is too expensive and almost impossible to streamline. The best way forward for any bank to add new services and solutions is to continue to patch them onto their existing systems. Workarounds are often made by making sure these solutions fit into existing platform solutions.

From a technology standpoint, middleware becomes a thick layer that binds this monolithic construct with a potpourri mix of traffic and information traversing across all different ledgers, applications, and services. It not only poses operational risk, but it also takes a lot of the resources which the bank could otherwise do without in managing problems and errors in these transactions.

There is a need to standardise the existing core banking solution to make it more efficient. Currently, standardisation happens at the middleware layer and systems rely on this middleware layer to talk to one another.

Transaction arrangements between banks are being served by an external messaging system, often conforming to a standard. A dominant service is the SWIFT[1] messaging and transaction system. Designed more than 40 years ago, the SWIFT system is a proven piece of technology, albeit it is extremely inefficient by today's standard, requiring some of these messages to be managed manually as it goes through multiple hops and switching.

Such a solution can be slow and tedious while posing some operational risks. Banks and corporations spend hundreds of millions of dollars every year to use the SWIFT system. When dissected, the Internet is just as good a message routing system, more efficient and much cheaper to use. However, the effort to switch is a mammoth task, requiring everyone to participate and to switchover, which in itself, is an expensive exercise and resource consuming.

For all intents and purposes, there is enough evidence to suggest that the plurality of systems coupled by disjointed monolithic

[1] Society for Worldwide Interbank Financial Telecommunication

systems within financial institutions contribute much to the operational risks and inefficiencies that we are witnessing today.

3. GOALS

It is not as if these problems that we are seeing were problems of recent times. It has been a perennial issue, with a compounding effect each passing year as financial services and offerings get added onto the core banking system. This is further exacerbated by each new service offering getting more complex and complicated.

The blockchain technology poses a possible long term solution to reducing costs; improving efficiency; allowing settlement finality; increasing efficiency of compliance efforts; providing greater auditability and traceability; enhancing structured processes (recently, termed as smart contracts); and cutting multiparty dependencies on global and local transactions.

By providing a blockchain platform that can satisfy the unmet needs above, any financial institution would see the benefits immediately. The blockchain platform is a standard by itself and allows any add-on application to integrate with it using an industry standard compliant instruction set.

We have been analysing the financial industry for 3 years, long before the industry itself took cognisance of the impact of blockchain and the role it can play.

Our 3-year long analysis and assessment point to a very important conclusion from where we now unveil this blockchain platform as an important means to an end. These goals were drawn upon the following important conclusions:

- Smart contracts have long been in existence in all financial institutions. They have been programmed into the core banking solution (automated) or acted upon manually based on agreements and protocols between parties, internally or externally. These smart contracts cost financial institutions billions of dollars to set up the infrastructure over the years, and to be able to transcribe that to a new platform will incur much more resources, time, and risks. It is a complicated web of work that is not quite possible to just change instantaneously. NEM has recognised this and is approaching it in another manner.

The approach here is to make the smart contract an external component, whether centralised (i.e., status quo with existing systems) or decentralised. The outputs of these smart contracts will then enter their transactions into the ledger through a secure transaction process.

- Build a platform that is inexpensive to deploy with minimal risk, time, and resources, while at the same time allow a financial institution to carry on business as usual with minimal interruptions – enabling organic growth.

- Create a blockchain platform with multiple ledgers for multiple use cases – mutually exclusive or not – and at the same time, allowing transactions between ledgers to be frictionless.

- Create one single abstraction layer for all the ledgers in this same blockchain to be integrated into any existing core banking system and solutions.

- Recognise privacy and allow each financial institution to control and manage its very own blockchain platform.

- Allow for seamless cross-platform transactions, payments, and settlements through direct transactions without the need to implement an expensive, standards and protocol driven messaging system. The end result is a reduced infrastructure system with settlement finality as well as less reconciliation work, risks, and errors.

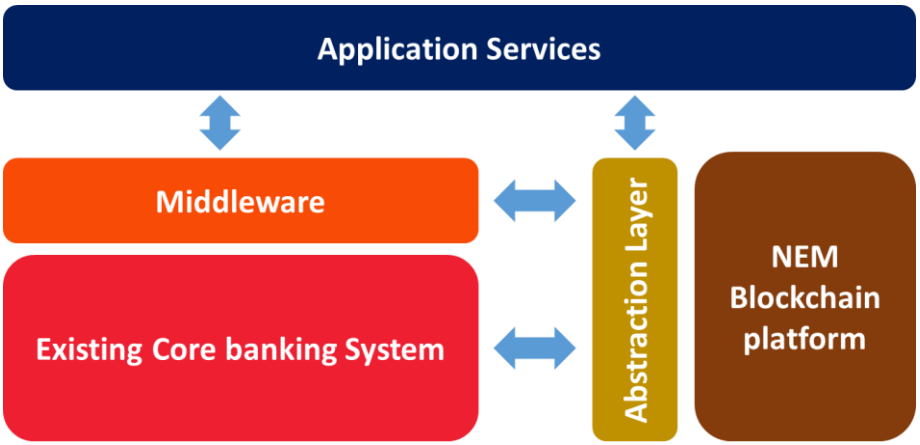

Figure 1. Blockchain Platform added initially as an adjunct solution to be built over the long term as the core ledger system.

4. CATAPULT

Catapult[2] is a second iteration and an extension of the NEM blockchain technology that was launched in March 2015. It is scheduled to be released in various stages, starting from the first quarter of 2017. Its predecessor is Mijin, which itself had undergone vigorous tests. Mijin and Catapult are permissible blockchains. The development difference is that Mijin is an extension of the NEM public blockchain. The second version, Catapult, shall be the reverse, i.e., it shall be an extension of the private chain into the NEM public chain. It is specially designed to add more functions and features to support the financial industry where critical features and functions are required of the blockchain.

4.1. FEATURE HIGHLIGHTS

Catapult is re-written entirely new in the C++ language, borrowing the core concepts from its first generation NEM release, augmenting these concepts from lessons learned, and amending and extending these concepts to enhance the offering. The end objective is a high performing, secure enterprise-class solution with open connectivity. Some of the more notable feature highlights that are being developed now for Catapult include:

- High scalability, design based on the industry standard tiered web architecture commonly found in enterprise computing, a holistic offering yet to be seen in any blockchain solution
- Introduction of a high performance and highly scalable API gateway server layer with an open integration architecture
- High throughput message queues for real-time analysis and big data analytics of transactions
- Use of nosql database at the API layer, which is more suited for high speed messaging
- Embedded escrow service for exchange of assets on the blockchain – a special transaction contract
- High transaction rates (in excess of 3000 transactions per second)

[2] Catapult and Mijin are developed and marketed by Tech Bureau, Corporation as a permissioned ledger. Both Catapult and Mijin shall be released as part of NEM's Open Source solution at a later date.

- Permissible access to accounts, i.e., each person can only access what she can see.
- Interoperability – allow external decentralised or centralised applications or smart contract solutions to transact using the blockchain.
- Business Rules – rules where object states can result in an indisputable transition to a new state as a result of a definite and conclusive action, specifically on the calculation of transaction charges based on a predefined set of irrevocable and immutable input criteria.
- Metadata – Accounts and assets shall have configurable metadata fields.

In addition to the above, the existing functions and features already present in the current release of NEM, will be enhanced and ported across to the Catapult project. These include:

- A built-in messaging solution
- A process activated or manual sign-off function for transactions, with multiple approvals, where needed.
- A multiple ledger with multiple corresponding assets in one blockchain
- Every account can hold multiple assets from multiple ledgers in the same blockchain so that these accounts can be used for all products and services the bank is offering, e.g., one account can be holding USD, EUR,GBP, Gold, Interest Rate Swap, ETF units, etc., each with its own history of transaction records and balance.
- Every account can be controlled by the financial institution – allowing for compliance and AML control mechanisms to be implemented in order to manage these transactions
- Freezing accounts
- Transaction reversal with full audit trail and accountability

The end result of the Catapult solution is a strong and highly customisable blockchain solution that can be utilised by financial institutions as a basis to form its core operating platform in the long term.

The principle behind the design is to provide a universal and core blockchain solution as the basis for the greater system of a bank. Further, it is premised on not creating a disequilibrium to the existing system but allow for sub-system migrations over time. Outlier and non-critical solutions can be ported across without

risking the banking system. New and older uncomplicated products and services can be developed, or ported, and launched using the blockchain.

This bespoke and yet highly flexible solution allows the bank time to get accustomed to it and implement solutions on the fly while not losing out on its growth path towards a blockchain driven system.

Its API gateway allows the blockchain to be easily dovetailed into other centralised (new or existing solutions) or decentralised (new consensus driven solutions implemented by other initiatives) systems including smart contract systems, internal process driven solutions, settlement, payment, and clearing systems.

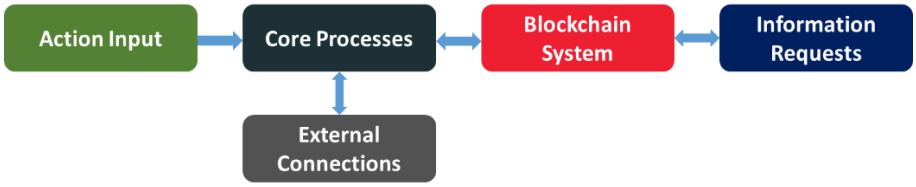

Figure 2. Principals of design. Simple and yet highly flexible

4.2. CONSENSUS

The Catapult blockchain platform is, like most things blockchain, driven by a consensus mechanism. It consists of a network of nodes (either permissioned or permission-less) networked together in a peer-to-peer (P2P) configuration. Transactions are broadcast out and each P2P node will record these transactions and verify them as they come in. At periodic intervals, called the block time, these transactions are grouped together and the transactions undergo a hash process (digital fingerprinting) linking it to the previous block, and then added on as a new block of information in the blockchain. The permissioned ledger does not have mining per se, and follows a controlled Proof-of-stake algorithm, while the permission-less (Public Chain) is based on an algorithm called Proof-of-importance[3].

Built into the NEM blockchain solution is a mechanism (Eigentrust++ reputation management algorithm) for ensuring each P2P node is reputable and therefore not fraudulent.

[3] NEM Technical Reference - https://www.nem.io/NEM_techRef.pdf

The NEM blockchain solution also created an all new P2P time synchronisation algorithm to ensure that each node is synchronised with one another in the right time slot.

4.3. PERSPECTIVE - USE CASES

The blockchain is intentionally designed as an open system satisfied through a set of industry standard JSON RESTful APIs. Therefore it is standards agnostic and is compatible with any application that conforms to a messaging standard such as ISO20022, or the FpML markup language. Catapult treats them as processes with defined outputs to update or broadcast transactions into the ledger. This method of integration and interoperability allows for the reuse of legacy applications and solutions.

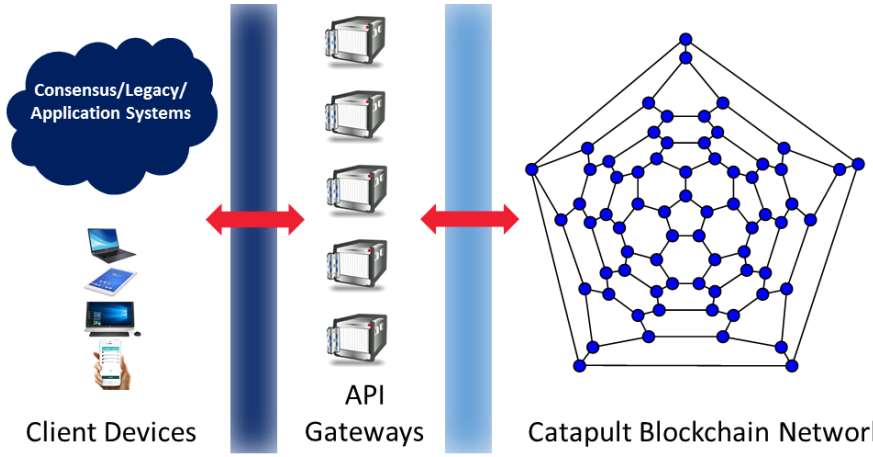

Figure 3. Tiered Architecture with API Gateways to integrate with other systems, or directly with thin client devices. Agnostic in standards.

4.3.1. Mutual Fund – Transfer Agent

We now examine a typical contract and settlement solution for a mutual fund purchase.

In a typical mutual fund scenario the actors are:

1. Mutual Fund Manager
2. Transfer Agent
3. Customer

The legal contract of the mutual fund spells out certain key points that results in the value of the sale and purchase of each unit of asset in the mutual fund. These include, but not limited to:

1. Net Asset Value (NAV) derivation
2. Investment details and conditions
3. Dividends
4. Discounts
5. Management fee
6. Trustee fee
7. Transfer fee
8. Commissions

This legal contract in the traditional sense would have been translated into a calculator application of which the outputs would result in one or multiple writes into the database followed by a series of actions, automatic or manual.

The buy and sell process initiates a request which is either manually processed or automatically triggers a series of operations. These operations eventually result in an outcome. In a buy process, the outcome is:

1. Await a settlement period
2. Upon settlement, make transfer of units
3. Issue a certificate of ownership

The function of a Transfer Agent is to manage the sale, purchase, and distribution of these assets. The job can be tedious and expensive.

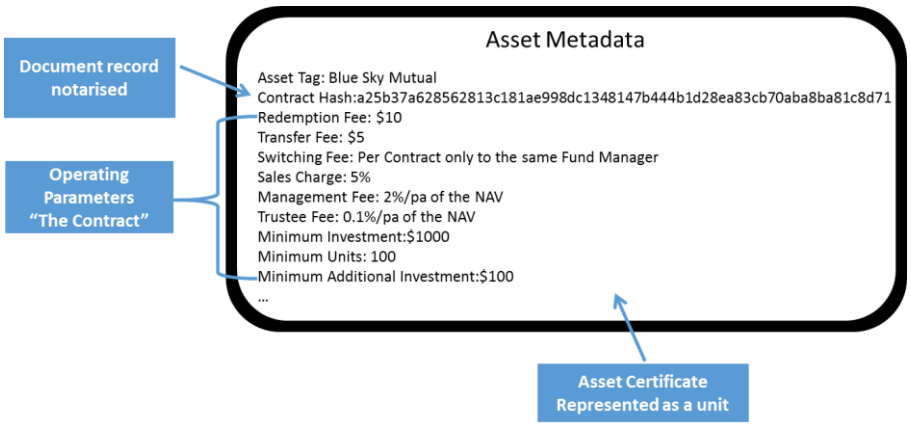

Figure 4. The asset certificate is translated into an asset and is configured into the blockchain.

Every unit holder, when she buys units of a mutual fund, will get certificates, each representing one unit that she owns in the blockchain. Each transaction becomes immutable and irreversible.

Calculation of fees and dividends thereof will be extracted from the blockchain from another application via an API call.

The original contract document, with its hash stored in the blockchain, could be stored in a distributed file system. Order processing could be another solution of which the outputs will transact with the blockchain via an API call. User balance can be accessed by the user with the same front end application to read from the blockchain through an API call. Analytics again, can be implemented on top and data extracted from the blockchain through an API message queue call. Payment and settlement is done through the user account directly with the blockchain.

The blockchain system is border agnostic and can be multiple ledgers sitting in the same set of nodes. This gives rise to a very powerful system that transgresses beyond the shores of a country and allows for multiple countries to operate, each with their own set of regulated rules - pertinent to the country of offer - and conditions (smart contracts) that can be implemented in a decentralised or centralised manner.

Smart contract templates can be built and applied across to any fund, independently.

Blockchain solution has its settlement mechanism that can easily be automated, cutting down settlement time to almost instantaneous, and without intervention.

While this solution is already available in version 1 of the NEM project, Catapult will enhance its performance and take it to the next level based on the aforementioned improvements.

4.3.2. Interest Rate Swap Arrangement

When two parties decide to exchange interest rate contracts, there is first an agreement. It is made between the parties concerned and the quantitative outcome would have been affirmed. This agreement is digitally notarised and a hash digest is stored in the blockchain while the agreement is put onto the distributed file system.

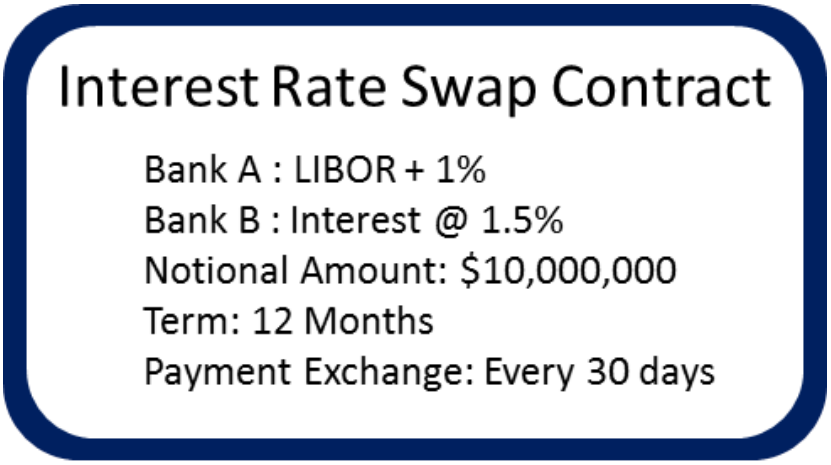

Figure 5. An IRS agreement with the quantitative outcome.

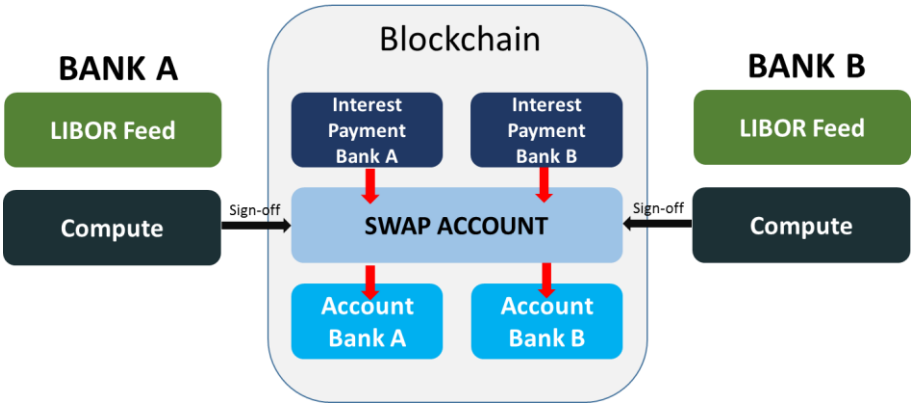

Figure 6. Interest Rate Swap on the blockchain.

The computational outcome can be commonly agreed based on a templated decentralised smart contract, or separately computed by the participants. In any case, the blockchain will trigger the pay-offs based on the outputs of these computed actions.

4.4. EXTENSIONS

The above are two of many use cases that can be implemented using the NEM blockchain. In a financial institution, everything revolves around a ledger which is a core element to all processes. Often, the cause of reconciliation issues, delays, risks, and failures is the absence of a central ledger system with multiple sub-ledgers that can work together in a homogenous platform. Even if there is a central ledger system requiring sub-ledgers to

individually update the central ledger, it can be an integration nightmare, usually causing more issues.

Identifying the root cause of these problems and providing the necessary platform not only takes away much of the risks and problems, but will also allow financial institutions to take on new and more complicated service offerings that have otherwise been too costly to do.

The NEM technology solves that issue and the design guarantees absolute finality and integrity of transactions that are immutable and irreversible. Any reversal of transaction can only be done by an opposing transaction, and which can be controlled with a full audit trail.

The existence of API server gateways enable the blockchain to act as a core to applications that require the use of a ledger. It is therefore, an open system and allows for standard conforming applications, including legacy and new decentralised smart contracts to integrate with the ledger seamlessly.

The design of Catapult is premised on a single private blockchain for each entity or financial institution. There is a parallel project[4] within the NEM initiative to develop a special routing system to allow interoperability across entities using a common shared ledger system. This common shared ledger system brings out the power of the NEM blockchain technology and enables seamless transactions, thereby disintermediating the need to have multi-hop settlement and payment systems. It opens up a new dimension where payments are straight through transactions from account to account with minimal messaging.

The option of each financial institution being able to operate its own single private blockchain allows privacy of data to be confined to the financial institution. The existence of a shared ledger system allows financial institutions interoperability so that they can settle and make payments with one another seamlessly.

In fact, the shared ledger system can stand on its own, offering a seamless solution that does not require any bank to own a private blockchain to be able to participate. It is, after all, a ledger of records and transactions, allowing for settlements and payments.

---

[4] Dragonfly Fintech is the developer for the homogenous cross-chain interoperability solution to link multiple instances of blockchains together.

It calls on a slightly different set of rules, away from traditional methods of settlement and payment. Additionally, it conforms to regulatory frameworks that are put in place today.

It can be seen that the NEM blockchain technology is an offering that helps in the transition of financial institutions from using traditional solutions into one that is powered by the blockchain technology.

The NEM project team strongly believes this is the way forward for transitioning. It gives rise to a low entry barrier for financial institutions to embrace the blockchain technology while at the same time, it also allows a financial institution to work on the blockchain technology and be familiar with it.

5. SUMMARY

The Catapult project is in its late stage development. It shall be released in multiple stages where the features highlighted in section 4.1 will be added on at each stage. It is scheduled for its first release in Q1, 2017. The enhancements of the solution are unique and powerful, setting a new standard in blockchain design.

Its powerful abstraction layer makes it agnostic to existing banking standards, the intent of which is not to disrupt currently installed solutions, but instead to dovetail into these existing systems seamlessly. Current systems running standards complying solutions - such as FpML and ISO20022 –will only need to make use of the outputs to integrate with the blockchain via the abstraction layer. This method of deployment allows financial institutions to migrate their systems in a timeframe that better suit their business operations – as soon as they minimise their need for some of these standards – into the blockchain platform. At the same time, the Catapult solution can then be used by financial institutions to enable growth, expansion, and creation of new products, leveraging on the use of the blockchain for faster and inexpensive deployment.

6. OTHER INITIATIVES - A COMPARISON

Catapult is a uniquely positioned solution and is a second iteration of its first solution, Mijin. Most other projects are derivatives and add-ons to existing blockchain solutions, which makes it rather clumsy as a holistic offering.

We present here 3 initiatives that may be relevant to what the NEM project is working on. While Ethereum and Bitcoin are in production phase, Corda is still in the conceptual stage at the time of writing.

6.1. ETHEREUM[5]

This project premise on a virtual machine, having its own programming language to run smart contracts that are loaded onto the blockchain. A smart contract once loaded onto the blockchain, is immutable and irreversible, and the ramifications can be severe if there is a bug. Additionally, it often relies on external data known as orcales, to feed inputs into the program to change its state. These changed states are written onto the blockchain storage.

Our solution has no smart contracts as we are of the opinion that this should be left to the bank to decide how they will want to incorporate that as a separate exercise. In a way, we are optimising the blockchain to do exactly what it is designed for, i.e., a ledger solution, and a multi-ledger solution at that with lots more features that are not only suited for the financial industry but generic enough to suit a spectrum of applications outside the financial industry. In a way, we have also built some smarts into the blockchain that can be used readily, with certainty and more often used. These include our multsig solution and the smart escrow solution where there is no need for a third party to facilitate a transfer. This smart escrow solution is based on two parties signing off before assets can be exchanged. If either party does not sign, there shall be no exchange of assets.

The very existence of smart contracts in an immutable and irreversible state can only lead to much resources wasted on the deployment of it, especially if it needs to be 100% full proof and tested. This is never usually the case in any software solution project. The more complicated the project is, the more prone it is

[5] https://www.ethereum.org/

to have bugs. A slight mistake can result in a systemic failure, and no financial institution should even consider that as a possibility.

Square pegs will never fit perfectly into a round hole. Having a smart contract on a blockchain is one such example. As it is now, most financial institutions already have well defined centralised smart contracts that they have been using for years. These are all controlled and they can be stopped, corrected of bugs, and run again. Outputs are final and definite. Any such bilateral or multilateral contract is cross-verified between multiple parties. A smart contract on blockchain is not possible to do that, i.e., the smart contract cannot be replaced with another program after being put onto the blockchain.

A smart contract cannot work in isolation. It still relies on external inputs or oracles. It cannot execute in a void and reliance on third party input has a trust issue, which in the first place is meant to be trustless. It is a paradox because the main value proposition of a decentralised smart contract solution was to be a trustless smart contract platform, which is not possible. In fact, having smart contracts in a blockchain could increase the cost of implementation exponentially. The end does not seem to justify the means.

6.2. BITCOIN[6]

Bitcoin is a blockchain project and is a proof of concept on the use of a decentralised blockchain to manage transactions. Catapult has the same end point objective of hashing and storing transactions on the blockchain, like the Bitcoin project. In fact, most blockchain projects follow this same principle

Where NEM differs is the method of competing for the right to create blocks of data onto the blockchain. Other differences are:

- System Architecture – NEM is much more scalable
- NEM does not have unspent transaction output (UXTO). It follows the standard ledger convention of using an account with multiple balances of assets - multiple ledgers in one account - inside it. All inputs and outputs go through this single account.
- Business logic – Bitcoin is a plain ledger. For example, NEM has on-chain signing of transactions - do not rely on additional centralised servers to queue transactions for

[6] https://bitcoin.org/en/

signing before broadcasting onto the blockchain - which gives it a very powerful utility.

- Bitcoin does not have an inherent, purpose built multiple ledger solution
- Bitcoin does not have a node reputation management solution as part of its core offering
- Most of Bitcoin offerings are workarounds patched on solutions that require dependent third party providers, thus introducing another layer of concern for service level and quality dependence, security, performance, and reliability.
- Machine competition – Bitcoin is designed with mining in mind. They have proof-of-work as a necessary element to secure the blockchain. For a permissioned blockchain solution, there is no need to compete in order to mine a block. NEM's approach has been a simple and yet very powerful way of securing the blockchain, requiring much less computing and energy resources to manage and maintain it.
- Transaction throughputs of Bitcoin are too low to be practical for a financial application. Their transaction rate per second is single digit in magnitude. NEM's Catapult transaction rates are 4-figure.
- Bitcoin confirmation time takes too long and is not suitable for the financial industry.

6.3. CORDA[7]

Corda is in concept stage and it appears that they are following the route of Ethereum with some subtle differences in the way they manage oracles and having stateless functions in a shareable ledger. They are proposing to use Java Virtual Machine to develop their solution. If at all, it appears that NEM could use the outcomes of these smart contracts to drive processes and outputs into the Catapult ledger system.

[7] https://r3cev.com/blog/2016/8/24/the-corda-non-technical-whitepaper