Whitepaper on Distributed Ledger Technology Platform for Business Innovation

June 2018
# Table of Contents

1. Executive Summary ........................................................................................................... 4
2. Distributed Ledger Technology Overview ........................................................................... 6
   2.1 *Introduction of Distributed Ledger Technology* .......................................................... 6
   2.2 *Powering Business by Blockchain* ............................................................................... 7
      • Simplify Business Process .......................................................................................... 7
      • Identify Trusted Business Partners .......................................................................... 7
      • Seize Business Opportunity ....................................................................................... 8
   2.3 *Business Implications* .................................................................................................. 8
      • Fraud Detection ........................................................................................................ 8
      • Double Spending ...................................................................................................... 8
      • Traceability ............................................................................................................... 9
      • Business Collaboration .............................................................................................. 9
      • Ecosystem ................................................................................................................ 9
      • Process Automation ................................................................................................. 9
   2.4 *Security and Data Privacy* ........................................................................................... 10
      • Key Management ..................................................................................................... 10
      • Certificate Authority ............................................................................................... 10
      • Enrollment Certificate Authority .......................................................................... 11
      • Transaction Certificate Authority ....................................................................... 11
      • TLS Certificate Authority ..................................................................................... 11
      • Identity Management ............................................................................................... 11
      • Data Encryption ...................................................................................................... 11
      • Privacy Preserving .................................................................................................. 13
3. Use Cases .............................................................................................................................. 14
   3.1 *Property Mortgage Business* ..................................................................................... 14
   3.2 *Manufacturing Business* ............................................................................................ 15
   3.3 *Retail Distributor Business* ....................................................................................... 17
   3.4 *Insurance Business* .................................................................................................. 18
   3.5 *Healthcare Business* .................................................................................................. 19
4. Governance and Regulation ................................................................................................. 20
   4.1 *Roles and responsibilities* .......................................................................................... 20
   4.2 *Developers* ................................................................................................................ 20
1. Executive Summary

In 2008, a Distributed Ledger Technology (DLT) was conceptualized in a paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System” \[1\]. The paper suggested how some mature technologies, such as decentralized peer-to-peer networks, asymmetric-key cryptography, hashing algorithms and Byzantine Fault Tolerance design, could be chained together to form a database that put records in a block in a disruptive fashion. In January 2009, the first Bitcoin system which was built on the DLT, made its advent in “a system for electronic transactions without relying on trust” \[1\]. Since then, DLT is gaining popularity and adoption by various types of industry as DLT supports distributed databases and enables participants to store and share information in a secure manner \[4\].

DLT allows network databases to interact with each other smoothly and securely without a central party from which each participating party seeks acknowledgement. It is with this versatility, traceability, decentralization, transparency and efficient sharing of data that DLT transforms the way organizations conduct and deliver their businesses. The DLT’s revolution introduces huge impact to the information world. First of all, digital currencies built on DLT use decentralized control to exchange digital assets and transform the society into a cashless one. The total digital currency market value has reached more than $370 billion in December 6, 2017 according to Coinmarketcap.com data \[2\]. This figure has surpassed the stock market value of JPMorgan Chase, the largest bank in the United States, with approximately $366.8 billion value on that day.

In Hong Kong, the Hong Kong Monetary Authority (HKMA) had conducted a research on DLT and released the Whitepaper 1.0 \[3\] and Whitepaper 2.0 \[4\] on Distributed Ledger Technology in November 2016 and October 2017 respectively, aware of the potential use of DLT in the banking sector and public service sector in the future, and burnishing Hong Kong’s credentials as a global trading hub with its development of proof-of-concept prototypes for property evaluation, trade finance and digital identity management using DLT.

MoneySQ Blockchain Limited, is a pioneer in Hong Kong to launch a business platform supported by Blockchain technology called, “trustME”. It is a breakthrough business platform, which supports the development of Guangdong-Hong Kong-Macao Greater Bay Area and provides SMEs in China, Taiwan and Hong Kong with the opportunities of using Blockchain technology. There is a significant development and commercialization on the Blockchain initiatives, training, certification and applications aiming to allow business to take advantage of this technology to create a more robust and secured application that serve both private and public users by lowering uncertainty and improving trust among the society. As such, MoneySQ has commissioned the Hong Kong Applied Science and Technology Research Institute (ASTRI) to conduct a research project on how Blockchain technology is shaping the business model and challenge organization to rethink and transform their businesses.

This whitepaper aims to bring out the impact of DLT technology on business and how it can utilize the unique characteristics of DLT to gain a competitive edge. We use this whitepaper to introduce Blockchain technology and demonstrate some real-life use cases. Chapter 2 provides a broad overview of DLT and its association with Blockchain. It illustrates the design, collaboration model, business implication and opportunity when adopting DLT technology for business. Chapter 3 describes five use cases based on
Blockchain technology in property mortgage, manufacturing, Supply Chain distribution, insurance and healthcare businesses. **Chapter 4** addresses the necessary governance and regulatory requirements along with the roadmap for the future of Blockchain technology. The paper concludes with the reflection on how Blockchain is disrupting the current business model by offering a higher-security and transparency platform that transforms the way business is conducted.
2. Distributed Ledger Technology Overview

2.1 Introduction of Distributed Ledger Technology

Distributed Ledger Technology (DLT) is a computer system that utilizes advanced cryptographic technology and peer-to-peer distributed networks to create secure, collaborative and reliable applications in a cost-efficient and trustworthy manner [3]. This technology plays a critical role in various applications such as digital currency and payment systems, identity management, asset ownership, contract automation, digital rights management, and healthcare management etc. It is considered a disruptive financial technology (FinTech) that can potentially cut out some expensive costs in the legacy computer systems and provide process automation and information digitization. The relationship of DLT and Blockchain is illustrated in the following diagram where Blockchain is a subset of DLT.

[Diagram: Relationship of Distributed Database, DLT, Blockchain and Permissioned Blockchain]

Blockchain technology has the potential to redefine enterprise ecosystems and economies. In 2017, 33% of organizations already active on Blockchain are experimenting with a business model that connects people, resources and organizations in an ecosystem [5]. Many organizations are learning and experimenting this technology by connecting multiple entities across multiple processes.

Blockchain is a distributed ledger that is used to maintain a continuously growing list of records, called blocks. Each block contains a timestamp and a link to the previous block. By its nature, Blockchains are inherently resistant to modification of data once they are recorded. The data stored in any given block cannot be altered retroactively without the alteration of all subsequent blocks and a collusion of the network majority nodes, thus making it a viable solution for decentralized database and applications.
2.2 Powering Business by Blockchain

- **Innovate Business Process**

Prestigious organizations that have dived into Blockchain area from prototype research to real-world practice are surprised to find that in order to implement a Blockchain project, it requires a high degree of planning, internal lobbying, re-engineering of business process and substantial effort to make it a success.

Like any other new technologies, for any organizations to engage in Blockchain, they need to identify the key objectives, focus on the real demand from users, agree on the business workflow, start from small scale, and take into account the governance and regulatory issues. Although the key objectives may be similar from cost reduction, process automation to workflow performance improvement, the potential friction may still arise from time to time. Collaboration is needed between multiple organizations, from business line to technology division. Leaders need to consider how they can work together for greater mutual benefits.

New technology deployment always involves changing of current systems. Legacy system owners or operators may be reluctant to change. Blockchain systems can run side by side with legacy systems and replace them only after the expected Return of Investment (ROI) is realized.

- **Identify Trusted Business Partners**

What value a partner can bring to the Blockchain network should be evaluated carefully because not all partners will bring positive contributions to the network. Does the candidate partner possess the ownership of the source? Will it become a barrier if this partner is not involved in the Blockchain network? What value will it gain from the network? The critical success factor is to have a mutual understanding and agreement before the collaborative network is formed.

Although it is tempting to turn to your most trusted partners, however, it may not always be necessary. Increasing the level of trust between organizations is precisely what Blockchain is designed to do even without the traditional business collaboration with the existing trusted partners. Six in ten organizations that are already active in Blockchain expect the technology to increase transparency and trust in data and transactions [5].

In Blockchain, no single organization is granted supreme control of the network. The privileges to access the data in Blockchain are equally or evenly assigned among all the predefined organizations. No organization needs to trust any organization in the network as every organization bears the same goal in mind: every organization has control but no organization is in total control.

The trustless trust in Blockchain is achieved by the technology instead of relying on any specific organization’s providing trust of safety, correctness or consistency. The trust in Blockchain network is native, in other words, Blockchain network itself creates the trusts by the technology by default.
• **Seize Business Opportunity**

Every new venture represents both a challenge and an opportunity. Embarking a Blockchain business network is no exception. Organizations need to examine their existing business flow to gain the most benefits from the Blockchain projects. Here are some common questions that organizations may ask.

How can I transform the current business rules to build up an ecosystem? How can I resolve arguments among partners? How can I encourage different parties to collaborate smoothly? How can I establish trust in transactions and processes?

How organizations incentivize other industry players to join the network to create a global ecology system? What value will the new entrant bring? Governance and regulation on the Blockchain network should be established and amended accordingly as the business expands. The roles and responsibilities for each organization, especially for data privacy and sharing, should also be considered.

Blockchain platform grants the data access rights only to the related parties to retrieve sensitive data by adding multiple channel feature. In addition, a large enterprise may own multiple ledgers, one for each business unit for example. This isolation of peers and ledger in the form of segregated channels allows network participants who prefer private and confidential transactions to coexist with potential business competitors on the same Blockchain network [6]. For many enterprises and financial institutes, permissioned Blockchain can meet the business requirements which are not possible with public Blockchain platform. In addition, using cloud services is recommended since cloud environments allow enterprises to shift from a highly centralized operating model to a secure ecosystem model.

### 2.3 Business Implications

Below sections illustrate how the characteristics of DLT such as tamper-resistant, transparency and decentralization can facilitate some business implications.

• **Fraud Detection**

The tamper-resistant characteristic of DLT could inspire logging key information in an unalterable block to enable fraud detection in sorts of scenarios. For example, the personal information or organization information could be pinned into the digital asset transaction, every spending of the digital asset could come along with the payer’s digital signature, monitoring the clear path of this digital asset circulation such that any fraud could be detected.

• **Double Spending**

Double spending means spending the same digital assets more than once in digital asset world. DLT provides the power to prevent such double spending issue by its transparency characteristic. Since all the asset transactions are witnessed and verified by all the participants in DLT, nobody can spend the same asset more than once.

In traditional fiat currency systems, there is some counterfeit money which carry the same serial number
as the real one. In this scenario, the “double-spending” of this piece of counterfeit paper money is double spending the “serial number”, which is hard to be figured out by community. DLT opens a door for the world on how it can help to change the currency issuing and circulation business.

**Traceability**

Essentially, Blockchain is a shared and distributed database system that every participant in the network can witness and update. As such no individual participant can change the history of any logged transaction, interrupt the flow of transactions, or unfairly manipulate the order of transactions. All actions or events could be traced or retrieved from the ledgers which preserve an ultra-origin source for possible disputes resolution.

**Business Collaboration**

DLT can be used in cross-department business collaboration to make the process more accountable and auditable. With the unique feature of DLT where the most up to date information is done in real time and secured across the entire network, different business department can share the same information or perform verification to reduce potential business risk. In addition, as all transactions are traceable; it will greatly facilitate and reduce audit effort. For example, an employee can submit a procurement form to the DLT and DLT will notify his supervisor to approve it. If the supervisor approves the application, it will go to next level management approval. If not, the form will be rejected and sent back to the applicant. All these actions are recorded into Blockchain no matter how many levels in the approval system, it will bring simple way for risk management or audit department to trace all the records.

**Ecosystem**

DLT ecosystem involves two types of DLT platform: permissionless and permissioned. The former type is operated by public nodes, and is open to anyone. The typical representative is Bitcoin platform which debuted as a digital currency and payment system since 2008. The latter type, which has as an example of the Hyperledger Fabric version 1.0 from the Linux Foundation in which only authorized nodes can join the network and thus supports higher throughput, faster, and more secure transactions.

In permissionless platforms, more digital currencies are created for payment or asset exchange and fork of major chains such as Bitcoin or Ethereum is emerging on the market that contribute to the rapid growth of this DLT ecosystem. A continuous effort is made to improve the transaction throughput to cater for such a rapid transaction demand. These permissionless platforms inspire business implications on how to use them in variety of digital payment methods.

In permissioned platforms, using a Blockchain implementation as a media for secured sharing of information attracts plenty of attentions in many industries. Different permissioned platforms focusing on different characteristics of DLT as emerged on the market are to fulfill different business requirements.

**Process Automation**

One of the best things about Blockchain is that it could be used for process automation in the form of smart contracts (a.k.a self-executing contracts or Blockchain contracts). In this way, contracts could be converted
into computer programs, stored and replicated on the DLT system and supervised by the entire network. This help participating parties to exchange information, asset in a transparent, automated, fairly, conflict-free way without a third-party involvement thus correlate to the decentralization characteristic of DLT.

Take an example of a car rental business between two parties. The deal agreement and delivery date could be stored in smart contract. After payment by cryptocurrency, the borrower gets a receipt and the digital entry key which comes by a specified date. If the key doesn’t come on time, the smart contract releases a refund. If the key and fee are both ready, smart contract sends the fee to lender and key to borrower respectively when the rental date arrives. The smart contract works on the If-Then condition and is validated and witnessed by all the DLT network participants, so a faultless delivery can be expected.

2.4 Security and Data Privacy

The security feature of Blockchain can be viewed at both macro and micro levels. At the macro level, Blockchain network is a peer-to-peer (p2p) network covering large geographical area with many collaborating peers. Failure of some peers will not affect the whole Blockchain network within the tolerance threshold level configured by the specific consensus algorithm. The process of logging new transactions to the ledger needs to perform a consensus endorsing mechanism, which can prevent malicious entities from logging forged transactions into blocks.

At the micro level, Blockchain platform uses hash technology to detect any alteration made to the original data. Hash function is a mathematical unidirectional function which summarizes the raw data, no matter how large it is, to generate a fixed-size short data named “hash value”. Any alteration on the source data will cause its hash value to change correspondingly. Key cryptography technologies such as Advanced Encryption Standard (AES), Rivest Shamir Adleman (RSA) and Elliptic Curve Cryptograph (ECC) algorithms are also applied to encrypt and sign the data exchange through the Blockchain network.

Below sections illustrate a permissioned Blockchain platform security design in general.

- **Key Management**

A permissioned DLT platform has two major roles: controlling access to the network and the content of each transaction. These two roles usually require a membership service provider and a cryptographic key manager. A membership service provider controls the admission of members to the network. A cryptographic key manager controls key generation, distribution, usage and storage. If transactions in the network are encrypted, the cryptographic key manager, together with the membership service provider, determines which users will be granted rights of access to the transactions in plain form.

- **Certificate Authority**

The Certificate Authority (CA) provides two different certificate services to DLT users, including user enrollment, transaction certificate authority and TLS-secured connections between users or components of the Blockchain, from front-end to back-end.
• **Enrollment Certificate Authority**

The enrollment certificate authority (ECA) \(^6\) supports new users to register with the DLT network and enables registered users to request an enrollment certificate for data signing with Elliptic Curve Digital Signature Algorithm (ECDSA) providing the public keys to be embedded in the certificates.

• **Transaction Certificate Authority**

The transaction certificate authority (TCA) \(^6\) enables network participants to bind every transaction with a temporary pseudonymous credential, such that other participants can only infer the temporary identity from the transaction and the origin identity may not be leaked. The activity or transaction history of the members can be separated from each other by issuing a temporary or one-time credential.

• **TLS Certificate Authority**

In addition to enrollment and transaction certificates, users will need the Transport Layer Security (TLS) certificates to secure their communication channels. TLS certificates can be requested from the TLS certificate authority (TLSCA).

• **Identity Management**

Two-factor authentication can be used for identity management. For example, mobile phone number will be a compulsory field upon account registration through the web portal. SMS message verification will be adopted as a second factor authentication to improve the security. Google Authenticator with QR code will also be provided in the administration panel to allow a higher level of authentication.

With two-factor authentication, the full privileges of a subscriber account can only be accessed after two levels’ verification, one is email verification and the other is SMS or Google Authenticator verification. When subscriber wants to perform sensitive operation, such as stopping/restarting DLT network, adding new nodes, two pieces of information—the password and the six-digit verification code that’s displayed on Email, SMS or Google Authenticator should be provided together.

With a password-only protection mechanism, it is no longer secured enough to protect the account. A two-factor authentication adds an extra layer of security, significantly enhances the security of the user ID and all the information stored in the DLT. Once logged in, user will not be asked again for a verification code unless user logs out completely from the DLT or needs to reset the password.

• **Data Encryption**

Any type of information or digital asset can be stored in a Blockchain regardless of its application. Information stored in the Blockchain is encrypted and digitally signed by the creator to ensure its authenticity and accuracy. Blockchain platform can adopt AES 256 algorithm as symmetric key encryption and RSA 2048 as asymmetric key encryption for the data encryption protection while ECDSA can be applied for digital signature algorithm. The primary benefit brought by elliptic curve cryptography is a smaller key.
size which helps to reduce storage and transmission overhead. An elliptic curve cryptography group could promise the same level of security afforded by a RSA-based system with a large modulus and correspondingly larger key. Smart contract for data encryption is also provided for other developers to change encryption mechanism on demand in their own DLT network. Here is the general practice for a data communication activity.

1. The network participant uses the public key of RSA 2048 algorithm to encrypt the symmetric key of AES 256 algorithm and then uses its ECDSA private key to sign the encrypted data.
2. Over the first-time communication, the client sends the encrypted and signed data to the server. The server authenticates the signature first, if it is authentic, then the server uses the private key of RSA 2048 to decrypt the data and get the symmetric key of AES 256 algorithm.
3. And then the client uses the AES 256 algorithm to encrypt and operate the subsequent business data communication.

The combination of AES 256 and RSA 2048 algorithms enhance the security and promise an approximate impossible decryption of the ciphertext for an unauthorized party over current computational power in the world.

In DLT, the blocks’ conjunctions are built with a hash function, which is used to transform data of arbitrary size to data of fixed size. Tiny changes to the data will change the hash value dramatically and in an unpredictable way thus making it impossible to derive the original information from the hash. By facilitating hash mechanism, each transaction is represented by a hash value and the summary of hash values form a Merkle tree. Transaction hashes are appended to the bottom of the Merkle tree as leaf nodes which are built upward until it reaches the top of the tree, called the Merkle root as the final node. Merkle tree not only dramatically enhances the speed of verifying transactions but also reducing the amount of block information required to prove the existence of a transaction within the block \[3\]. With the combination of cryptography and digital signatures, Blockchain provides proof of identify and authenticity of the creator and that data stored in Blockchain is well protected.
• **Privacy Preserving**

Strong data encryption and sufficient access control mechanisms are the necessary elements to protect privacy in a permissioned DLT network. The cryptographic technology will always be needed over time to provide refined protection. The elliptic curve cryptosystem has the property of safeness, high speed in encryption and occupies small space. In addition, sensitive transaction information in a DLT network should be treated with confidentiality, and access to such information should be restricted to authorized parties only.

The common practice is to store the hashed value only in the Blockchain. Even one managed to obtain the hashed value from the Blockchain, it is meaningless as it contains only a random representation of the information. With data encryption, digital signature algorithm, key management and three types of certificate management, together with multi-channel support and channel separation which will be explained more in the Appendix section can be applied in Blockchain to ensure data privacy and security at both macro and micro levels. Blockchain also makes use of the hash function as described above to make it extremely difficult to reconstruct the original data as only the hashed value of data is stored in the Blockchain. Even one is managed to decipher the hash value, it is meaningless in its own form as only partial information of the original data is contained in the hash value.

The faster quantum computer is a threat to current cryptography world, including Blockchain technology. However, substantial research has been carried out to protect the data safety against this quantum threat. For example, the first quantum-secured Blockchain technology adopting quantum signature to tackle the identity of each participant has been tested in Moscow[10].
3. Use Cases

The previous chapter provided a high-level overview of DLT. In this chapter, we will describe how business can adopt Blockchain technology and turn it into a business advantage. As shown in the following diagram, Blockchain can be integrated into many industries. There is virtually no limitation for its application.

![Blockchain Integration Diagram]

Illustration: Blockchain can be integrated into various industries

The benefits of distributed ledger ecosystem push the frontier of financial technology into everyday life and extend far beyond the financial and public service sectors. Below are just some of the businesses where Blockchain can overcome the current business issues and make a substantial impact to the business.

3.1 Property Mortgage Business

At present, the property mortgage industry is facing plenty of challenges like long processing time due to manual verification of documents. For example, for a mortgage applicant, it will usually take several days for applicant to receive the application result. In addition, data integrity issues, fraudulent financing and lack of transparency due to lack of standardized contract and data format are commonly exhibited in the current mortgage industry.

Can current inefficient mortgage process be improved? Blockchain could be a good technology to overcome
these problems. With Blockchain, the processing time can be greatly reduced as all necessary documentation and verification could be retrieved and performed almost instantly. The authenticity of the application can also be verified across the network thus reducing the risk of fault.

With these advantages of Blockchain for the mortgage industry, it will surely revolutionize the business. The below procedure illustrates how end-to-end process flow of a property mortgage business can be operated assuming MoneySQ as a platform provider:

1. Loan applicants/agents submit loan applications via MoneySQ Blockchain web portal.
2. Smart contract in Blockchain will review the application for duplicating finance and any fraudulent factors, and alert will be sent out if these factors are found.
3. MoneySQ pre-qualification team will check the loan application and update the result, if it is qualified, the applications will flow to Banks.
4. Banks retrieve the loan details, pre-qualification result and supporting documents from Blockchain, then make a loan offer or reject the application.
5. Loan applicants will get the latest application status update right away.

The decentralization characteristics of Blockchain combined with business automation would be a major step toward to a more optimized workflow for the property mortgage industry.

### 3.2 Manufacturing Business

As one of the world’s largest import/export harbor, many enterprises in Hong Kong run their businesses on manufacturing products and selling them all over the world. Supply chain control is an essential business tool for these enterprises. Wholesaler, manufacturer, banks, forwarders are involved globally where banks act as intermediary providing assurance and liquidity services. However, traditional processes involve labor-intensive and time-consuming work because of the due diligence checking, and heavily rely on multi-party paper documentation to mitigate business risk. Various consortiums around the globe have carried out different types of proof-of-concept work using Blockchain’s tamper-proof, transparent, decentralized characteristics in attempts to streamline the manual processes for business automation, improving operational efficiency, reducing errors, and increasing convenience for all parties.

In Blockchain, a pre-defined smart contract could be negotiated and instantiated on the Blockchain system among all supply chain parties. A holistic view of the contract terms for a trade transaction and the flow of goods from manufacturers to wholesalers will allow instant sharing of information thus lowering potential business risk. Here is the main process for a supply chain business.

1. Wholesaler and manufacturer agree on a trade transaction on open account terms at a specific date and time. The wholesaler creates a Purchase Order (PO) and sends it to a manufacturer for confirmation.
2. The manufacturer prepares the goods based on the PO and notifies forwarder for goods delivery.
3. When the goods have been transported to the export terminal and inspected by customs, they are transported by freight to the wholesaler.
4. Once the goods have been well received by the wholesaler, the wholesaler confirms the trade transaction is a success and notifies the bank to remit the money to the manufacturer and then provides invoices, bills of lading and other transport documents to the wholesaler via a document courier.

In this scenario, manufacturer, wholesaler, clearing agent, customs, forwarder(fright/shipping), bank and retailer can all join in to this platform to build up a complete supply chain ecosystem to generate the network effect.

Similarly, for the wine industry, the current challenges are that there are a lot of bogus wine in circulation worldwide. The source of this problem is that there is no central authority or standardized industry practices one can verify the provenance of the wine. The usual way is to rely on an experienced or educated expert to evaluate each wine for signs of authenticity within the wine industry. Examining wine is an expensive and time-consuming practice, and this practice is still a risky maneuver since it is highly subjective to individual’s sense.

DLT could help to make the wine verification process in a more objective manner. As an example, imagine there is a DLT platform established in the winery industry, winery, auction house, wholesaler and retailer can all join the platform. Each participant holds a replicated ledger that records all the wine transactions since day one the bottle of wine is sealed.

As shown in the above figure, starting from the producer, a bottle is assigned a unique digital ID etched in the glass or simply printed on the label when it is created. Every time the winery created a distinct bottle, a transaction record will be logged in the ledger with the winery’s digital signature. When the bottle is sold, the winery as part of that transaction will also give the transaction block information in the ledger to the new owner. As the wine changes hands again and again, the digital ID and transaction block information is passed along, keeping a life history of that wine on the DLT network.

Wholesalers, retailer and other industry players would also leave their digital signatures on each wine
transaction. The caretaker that ultimately receives the wine from the retailer will use the retailer’s public key to verify the onchain transaction by scanning the smart tag (either QR Code or NFS) in the bottle.

The Blockchain solution allows traceability starting from the manufacturer’s site through transportation to distributor, importers, warehouse, merchants, transporters, auction houses, retailers. All these points can be referred as intermediaries and are completely traceable.

### 3.3 Retail Distributor Business

Utilizing Blockchain, retail distributor can digitize all the product information and log a permanent record of transactions in order to trace the food products from farms through the whole supply chain. In addition, it also provides a way to capture online consumer who purchases the product for consumer behavior analysis.

---

**Illustration: DLT based tracking comparing traditional paper-based way in Retail distributor business**

This could prove to be a great business advantage for food safety in the world, when digital information such as farm origin, slaughterhouse, packing and processing record and shipping details are digitally attached to the food product, it will be grouped together and stored in the Blockchain.

The Blockchain existence in product tracking brings obvious advantages comparing to traditional paper-based product tracking system in terms of cost, effectiveness and traceability. Most importantly, the instant share of information of the products will bring the retail distributor a greater convenience for inventory control and capital optimization thus reducing the risk of over stocking at the same time.

There is an increasing trend that consumers want to know that the ethical claims from the manufacturers about their products are authentic. Blockchain provides an innovative new way to verify that the backstories...
of the products we are purchasing are genuine. Transparency and tamper proof will come with Blockchain in terms of timestamp of a date and location on the goods which correspond to a permanent product identity stored in the ledgers. With mass data contained in numerous devices and multiple networks throughout the supply chain, the Internet of Things (IoT) combining with Blockchain technology will create a tamper-proof, distributed filing system and real-time records.

3.4 Insurance Business

The insurance market is another industry which is revolutionizing its old systems and benefiting from the Blockchain technology. Double claiming or lack of trust between insurer and customer are two typical issues in the current industry. Blockchain may overcome these issues with its transparent and trustless characteristics. Transparency prevents the double claiming while trust on technology instead of insurers will bring more confidence to consumers.

For instance, with an insurance Blockchain platform, passengers simply choose their flight by selecting a destination airport, and the date of their departure. Then they apply for a policy showing the probabilities of flights being delayed more than 30, 60, 120 minutes, or canceled or diverted altogether.

Illustration: Smart contract checks the flight time table and execute the insurance terms automatically

Blockchain plays two key roles here. Firstly, it maintains an accessible and immutable record of the insurance contract within a smart contract or “smart insurance”. Secondly it serves as a mechanism for triggering the payment to the client once 30, 60 or 120 minutes mark is passed. The payment process is activated automatically by events coded in the smart contract.

The smart contract is the party that decides if the insurer should indemnify the policy holder and trigger a payment request. The use of a smart contract to trigger claims will add trust in the whole process. Smart contract is basically a program code which will trigger automatically based on pre-defined condition and self-
executed the agreement between two or more parties. Smart contracts avoid the delays and expenses incurred by existing paper contracts as well as the intermediaries. With smart contracts, intermediaries can be eliminated thus saving the time and cost.

### 3.5 Healthcare Business

In the current healthcare industry, there is a substantial amount of duplicated medical tests conducted on patients and isolated treatments history. The source of this problem is that there is no central authority or standardized industry practices that one can verify the provenance of the medical record.

Blockchain could help to address the interoperability currently present in the health care system. As an example, with a Blockchain platform established in the healthcare industry, hospitals, clinics, and laboratories can all join the platform and access a shared ledger where the source of truth of medical transaction is stored. In addition, the transaction information is encrypted and digitally signed to guarantee its authenticity and accuracy.

![Illustration: DLT information sharing center lowers the medical cost](image)

Every time a piece of medical record is created, a transaction record will be logged in the ledger with the participant’s digital signature and the record is immutable and cannot be changed or removed. When the patient visits another hospital for treatment, the hosting hospital can access the patient’s complete medical records in Blockchain. It will help to provide better treatment and save the medical cost.

In conclusion, Blockchain platform can be integrated into a wide range of industries. The previous five use cases are just samples of what Blockchain can bring to the industry. It could also play a key role in global application such as personal identity management, property evaluation, digital asset management and so on.
4. Governance and Regulation

It is unavoidable that with any introduction of new technology, it also brings in new types of risk, and DLT is no different. For instance, denial of access or denial of service attacks and other cyber-attacks may still happen in DLT and cause its operation to fail. It is of paramount importance that proper governance and regulation are established if DLT is to be successfully implemented [3].

4.1 Roles and responsibilities

Different groups of people are involved in DLT networks. They can be grouped by their functions with different roles and responsibilities.

4.2 Developers

Developers are responsible for implementing the DLT smart contract to represent business flow, including setting up endorsement policies and putting rules in place.

In addition, developers should ensure that the changed source code is adequately tested and passed the User Acceptance Test (UAT). Importantly, proper software documentations must be version controlled and kept updated to ensure that ongoing systems operation and support can be carried out by DLT operators smoothly.

4.3 Operators

Operators must be capable of overseeing the operational status of the DLT network. Any attack attempt to alter the transaction history or inject malicious transactions should be proactively alerted and identified by other peers. All this information will also be logged and summarized in a bird eyes’ view in DLT dashboard. Operators should be aware of the warning appearing on the dashboard and investigate the system logs for further information.

Operators should also have the capability of conducting business continuity planning, disaster recovery, closely follow the conduct codebook on adding, deleting and revoking new nodes in the DLT network.

4.4 Users

Users of DLT network plays an important role in making the DLT network alive and operational by conducting different kinds of transactions in the network [3].

A private key represents the user identity in the public network, specifically, the ownership of digital assets. The private key usually should be presented when transferring asset to others, storing them or its alternative key phrase in an offline place, or called “cold storage” such as a USB device or paper is a good practice. Identity thefts or other perpetrators often choose the online private key storage, i.e. hot wallet, as
the first choice of attack. Users should bear in mind that safely and securely storing of the private key is the only way for anti-theft and asset protection.

4.5 Report and audit

Reporting and auditing of financial activities are the key aspects of regulation by overseers. In reality, the financial institutions have the obligation to prepare reports on a regular or ad hoc basis. DLT enables regulators or auditors to directly access transactional information stored on the DLT through supervisor node for monitor or governance purpose in a near real-time fashion. Regulatory reporting and financial reporting (e.g. the filing of tax returns) can be made possible through the supervisor node[4].

4.6 Regulatory compliance

Financial and banking stability and sustainability are the most important objectives of all regulatory authorities. The increasing adoptions and applications of DLT are dramatically attracting attentions by the regulatory authorities.

In general, principles for technology business continuity planning, disaster recovery, risk management and other relevant guidelines are equally applicable in DLT implementation and deployment. In addition, the decentralization and multi-geography nature of DLT platforms make the regulatory compliance issues more complex. However, DLT is still evolving and in a not too distant future, we believe there will be a more standardization on the governance model and regulatory guideline.
5. Conclusion

This paper provides a description of Blockchain technology and how it could revolutionize the way business is conducted today. It also reveals some business innovation with use cases employing Blockchain technology to streamline the business workflow and possible collaboration amongst partners to create an ecosystem that could benefit all participants. As Blockchain can provide a distributive, permanent ledger that is immutable, transparent and securely record transactions, it can apply to virtually any industry such as Banking and Financial payments, Supply Chain, Insurance, Health Care, Transportation, Retails and Real Estate.

Internet connects people while Blockchain connects people with trust and privacy. Big data on cloud provides a fertile soil to digital marketing and AI to grow, while Smart Contract makes innovative business model possible. To consumer, applications integrated with Blockchain technology can provide a seamless operation and a whole new user experience. Organizations adopting Blockchain can take full advantage of it and create a business advantage by exploiting its feature like security, authenticity, trust and instantaneous data access.

We hope that organizations who are new or planning to explore Blockchain will now have a better understanding of Blockchain and what advantages it can bring to your business.

MoneySQ Blockchain Limited uses Blockchain technology to develop the first business DLT platform in Hong Kong, named “trustME”. Through tight collaboration with Microsoft cloud system expert, Deloitte as the Blockchain implementation leader and Hong Kong Applied Science and Technology Research Institute (ASTRI) Blockchain team to provide the best practices, knowledge and processes on system security, technical advisory and platform architecture design. With this close consortium, trustME creates an ecosystem that is built with a permissioned DLT network in such a way that data privacy and security requirements are enacted allowing business to run their critical applications knowing that the platform is secured, transparent, trusted, immutable and provide operation efficiency. MoneySQ believes its works will go towards supporting the development of Guangdong-Hong Kong-Macao Greater Bay Area and provides SMEs in China, Taiwan and Hong Kong to transform their business with Blockchain technology.
6. Reference

4 See “Whitepaper 2.0 on Distributed Ledger Technology” at http://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/infrastructure/20171025e1a1.pdf
9 See “Ethereum Within the Insurance Industry - ETHNews.com” at https://www.ethnews.com/ethereum-within-the-insurance-industry
Appendix – Enterprise Level Blockchain Application Practice

The business ready Blockchain platform needs to cater for the full life cycle (develop, administration and operate) of a multi entities DLT network. It is designed to achieve enterprise levels of security, data atomic, scalability, and high availability to meet business demanding from different industries.

System Architecture Overview
The system architecture at the enterprise platform level requires robustness, scalability and seamless integration. Blockchain platform has taken all these design principles into account. The diagram below illustrates the system architecture of permissioned Blockchain platform.

- **Interface Layer** - Enables clients and business applications to run on top of Blockchain via Application Programming Interface (API).
- **Service Layer** – Enables new nodes or organizations’ enrollment, registration, revocation procedures during network operation. Also, it is responsible for the management of various policies specified in the network, such as the endorsement policy and account management policy.
- **Block Layer** - Responsible for reaching an agreement on the correctness, the order, and the confirming the group of transactions that constitute a block.
- **Resource Layer** - Responsible for scheduling resource for each node’s run time environment overhead, world state, history and index data storage.

Permissioned Blockchain platform grants the data access rights only to the related parties to retrieve...
sensitive data by adding multiple channel feature. In addition, a large enterprise may own multiple ledgers, one for each business unit for example. This isolation of peers and ledger in the form of segregated channels allows network participants who prefer private and confidential transactions to coexist with potential business competitors on the same Blockchain network \[^6\]. For many enterprises and financial institutes, permissioned Blockchain can meet these business requirements which are not possible with public Blockchain platform. In addition, using cloud services is recommended since cloud environments allow enterprises to shift from a highly centralized operating model to a secure ecosystem model.

**Multi-Channel Support and Channel Separation**

Inspired by the concept of publish-subscription messaging queue, a channel is like a topic that restricted peers may subscribe to and become participants of the channel. Only participants of a channel may transact on that channel, and transactions on a channel are not visible on the other channels.

Permissioned Blockchain extends the channel management setting and supports multiple co-existing channels in a Blockchain network with a tailor-made ledger per channel for data protection and isolation \[^7\]. This feature allows for multilateral contracts where only the authorized participants with a certificate on the channel can submit proposal, endorse, order, or commit transactions on that channel. As a result, a single peer can maintain multiple ledgers without sacrificing privacy and confidentiality.

![Illustration: Multi-channel and channel separation](image)

As shown above, Peer 1, 2, and N subscribe to the red channel and operate the corresponding red ledgers among them. Peer 1 and N subscribe to the green channel and operate the green ledger with the absence of Peer 2 because it is not in the green channel. Peer 2 and N are in the yellow channel and operate the yellow ledger without the attendance of Peer 1.

Its consensus mechanism is also unique. Instead of implementing consensus on a system level, consensus is implemented at individual level. Different types of consensus are supported. However, transactions are
validated only by designated validating nodes.

In practice, business logic may be transformed into applications, which constitute business agreements in the form of smart contracts. DLT serves as the platform where the smart contracts can be executed. The agreement is endorsed, validated and stored in the ledger, then executed in DLT’s secure environment by designated peers on the segregated channels.