December 13, 2017

Feature Report

Blockchain Technology

NOT RATED | Industry Research

Blockchain, a Chain of Applications! Go Beyond the Bitcoin Hype

Yanny Chu
(852) 2159 – 4505
Yanny.chu@hooraysec.com.hk

Blockchain Technology Backed by Foolproof Mechanism

Blockchain is a distributed database that utilises public ledger to share records among participants. Information in public ledger is hard to be tampered or erased as all participants own one same copy, whereas information stored in centralised database is easier to be manipulated. Hash function and corresponding hash items further improve the data quality to be stored in the public ledger.

Blockchain Market Grows Fast, Grows Diverse

Blockchain technology had not yet received much attention until Bitcoin has encountered a price surge since the beginning of 2017. Up to early December 2017, Bitcoin price has skyrocketed 22 times yoy. More new coins and tokens coming up in the market that even Bitcoin itself has two forks called Bitcoin Gold and Bitcoin Cash, which attracting investors by different features.

Proposing State-Issued Digital Currency on Blockchain

Central banks across the globe are now interested in issuing own fiat digital currency under distributed ledger technology (DLT) as infrastructure. DLT could deter certain financial crimes by making fiat money becomes more traceable and become immune to fraudulent transactions. The proposed digital currency is however still at a research stage that no concrete schedule and plan to be confirmed for now.

Smart Contracts on Ethereum

Ethereum is the most popular blockchain platform to support smart contracts, it provides open source codes for developers to design application and offers existing decentralised network. Smart contracts can be applied to diverse use cases as long as the use case consists terms and conditions, then computer program can digitalise and offer self-execution to the contracts in order to save costs, time and reduce operational risks from manual work. Smart contract could bring enormous business opportunities based on its versatility and interoperability.

Topic in FinTech: Blockchain, a Secure and Efficient Helper

'FinTech' is a broad term encompassing a wide range of applications of technology in the context of financial services. FinTech services include P2P lending, robo-advisory for clients' investments, electronic payment and settlement, big data analysis, cybersecurity and blockchain technology. FinTech is often asset-light, low-margin, innovative, able to scale, and unburdened by laws. Legal systems have not yet covered as FinTech is still new and immature. Moreover, FinTech targets to service customers directly and this B2C feature is different from traditional financial services businesses which are focused more on B2B.

Since finance industry is full of information, FinTech can help propel the sector with lighter regulatory constraints, bridges between service providers and social needs, as well as safer digitalised work processes. Blockchain, one of the attempting FinTech areas, seeks to provide a secure and efficient mean through the use of smart contracts, encryption and a ledger compilation. Blockchain together provides the capability to create and control digital assets and digital autonomous organisations. The autonomy fits in diverse applications, such as payment system to trace individual transactions, venture funding, legal services and so forth.

Bitcoin Hype: Put Blockchain on the Map

Harking back to 2009, when the very nascent digital currency, Bitcoin, came to the market, its backbone technology - distributed ledger did not receive much attention. Encouraged by the increasing popularity of digital currency and the outrageous surge in Bitcoin price, its backbone technology is now one of the hottest FinTech topics. Blockchain technology could develop new and revolutionary applications more than investment vehicles. Basically, it has two main streams which are digital currency (aka cryptocurrency) and smart contracts.

Two Main Streams in Blockchain: Digital Currency and Smart Contract

The development of digital currency is at a high speed that market demand on private cryptocurrency is now growing, not only Bitcoin is being invested but more ICOs coming up. Cryptocurrency also becomes a research interest in public sector, several leading countries have investigated possible uses of blockchain technology in banking and monetary systems for the trend towards cashless society and increase in money traceability and reliability to prevent financial crimes.

Smart contract is an application built on top of blockchain technology, and the application can be developed flexibly with open source code. Smart contract is per se an automation that will execute agreements once the terms are fulfilled. Automation leads to reductions in operational costs and risks. Blockchain technology can be widely adopted in different industries through its "smart contract" feature characteristics. Also, its interoperability triggers one business opportunity by another, making a

chain of applications. The potential applications range from medical industry to legal services.

How Blockchain Works?

Bitcoin as an Example to Illustrate Blockchain Technology

Blockchain is a distributed database that utilises public ledger to share records among participants. In such decentralized system, all executions and records entail verifications by consensus of a majority of the participants in the system. As a result, the information in public ledger is hard to be tampered or erased as all participants own one same copy, whereas information stored in centralised database is easier to be manipulated.

There are numerous cryptocurrencies employing blockchain technology to build a secure storage environment. This report uses Bitcoin to explain the execution and storing processes, so as to bring out blockchain technology features, variations in models, pros and cons of blockchain in terms of different applications.

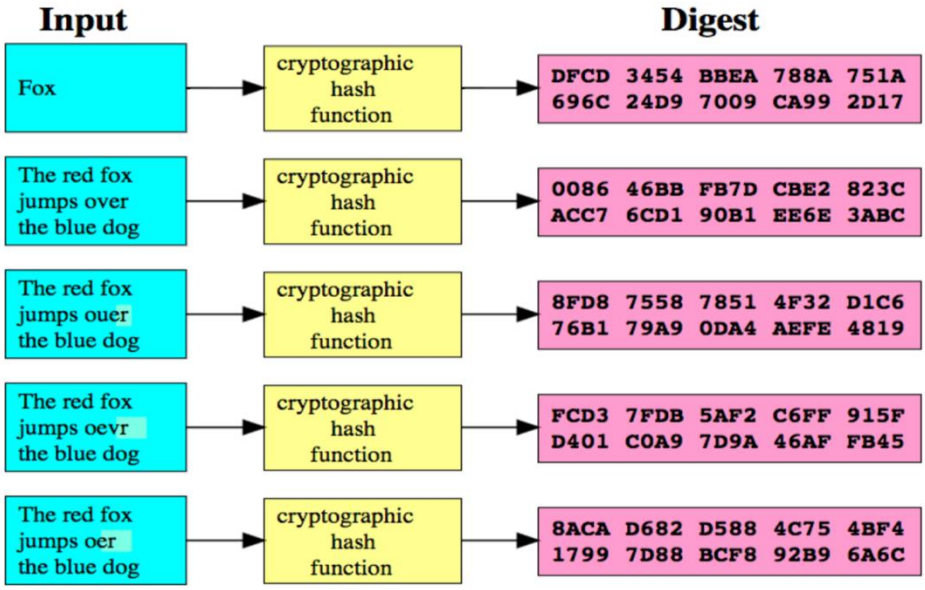
Important Bitcoin Components: Miners, Public Ledger and Hash Algorithm

Before going into details, three important elements will be first introduced. As Bitcoin relies on a peer-to-peer system, the first important item is "member" on the network. Members or peers here are actually computer nodes, aka Bitcoin miners which are responsible for verification of each transaction while synchronising and replicating the public ledger. Another important element is aforementioned "public ledger". Public ledger consists of numerous blocks containing transactions and chronologically links with one another in order, such that all records can be traced. The last component is hash algorithm which is used to maintain high security level.

SHA256 Algorithm in Bitcoin System

SHA 256 is one of the family member of Secure Hashing Algorithms, some other SHA algorithms are more fundamental, such as SHA-1 shown below. SHA is cryptographic functions designed to keep data secured by transforming the data into a fixed size string through a hash function, and thus the output string is known as hash value. SHA algorithms are designed to be one-way functions, meaning that once input data is transformed into respective hash value, it's virtually impossible to transform back into the input data. To prove the input data of a specific hash value, the only way is to use hash function to transform the proposed data again, input data is confirmed when its hash value is same as the specific hash value.

Exhibit 1: Transformation Process of SHA-1 Hash Function



Source: Web Science and Digital Libraries Research

Bitcoin employs SHA256 algorithm to generate a fixed size 256-bit (or 32-byte) hash. The hash function is well used to distinguish transactions as SHA256 is a function that can transform inputs to hash values with 256-bit length. SHA256 fits the Bitcoin system because the generated hash values would be the same for identical inputs, such that the information stored in each block can be read without confusion. Also, the possible number of hash value combinations generated by SHA256 is 2 to the power of 256, which is enormous enough for Bitcoin digest.

Bitcoin Technology Divided in Three Segments

Understanding of blockchain behind Bitcoin can be separated into three parts, which are the creation of Bitcoins, transactions and foolproof mechanism.

1st Part of Bitcoin Mechanism: Creation of Bitcoins

Bitcoin miners do not directly create Bitcoins but are are awarded in a mathematical game. By successfully solving mathematics, miners would be awarded a block containing a batch of Bitcoins, and then the block would link to the public ledger so that the new Bitcoins and the ownership are verified.

At the very beginning, the creation award was set at 50 Bitcoins per block mined. Yet block mining award halves every 210k blocks. Moreover, total number of Bitcoins in circulation is capped at 21mn, meaning that miners will merely act as artificial validators to update transactions in public ledger after reaching the circulation limit as miners will no longer be awarded new

Bitcoins by creating new blocks. Up to this point in time, approximately 80% of Bitcoins are mined and each Bitcoin block mining award decreases to 6.25.

Proof-Of-Work as a Requirement in Bitcoin Creation

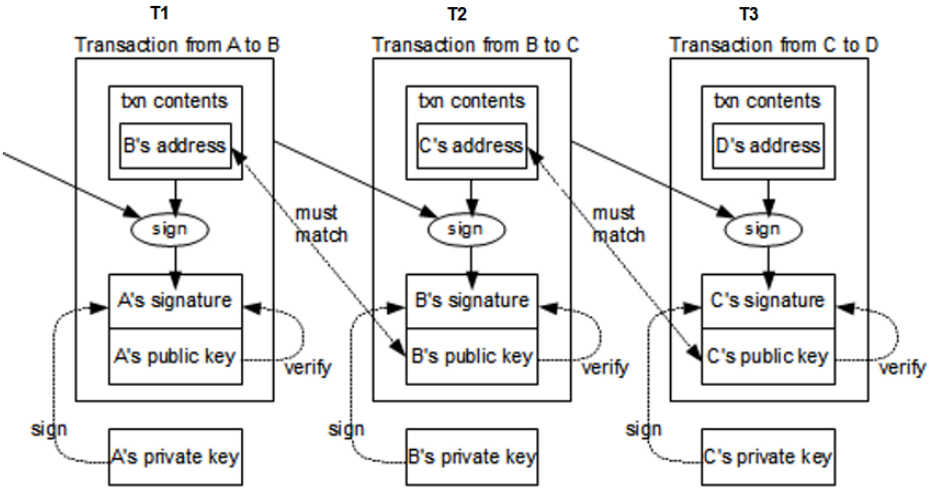
Creation of Bitcoins requires miners to solve mathematical puzzle. This mathematical puzzle is not trivial to solve and the complexity of the problem can be adjusted so that on average it takes ten minutes for a miner network to make a right guess and generate a block. Such mathematics task is called "proof-of-work". In fact, the calculation is neither meaningful to miners nor necessary in blockchain. The mathematics is merely designed by the inventor of Bitcoin in order to avoid abuse, although there are other choices as preventive measures. Since miners will shorten the duration with improved CPUs, Bitcoin would adjust the difficulties of the mathematical task to keep the required creation time unchanged.

The proof-of-work requirements, maximum number of Bitcoins and duration of creation process mentioned above are set by its inventor so that the entire system can fulfil its own objectives, in other word, there could be variations among cryptocurrencies as long as the corresponding inventors are allowed to flexibly design and make changes in protocols.

2nd Part of Bitcoin Mechanism: Transactions

Bitcoin has two types of transactions: Bitcoin ownership transfer and Bitcoin creation. The only difference in Bitcoin transfer and Bitcoin creation is the sender and recipient. While the first type of transactions only involve among Bitcoin participants, the latter type involves between the system and miner, as creation of bitcoin is a kind of awards offered by the system.

Exhibit 2: Bitcoin Hash Transaction Flow



Source: HashCoins (an ASIC-Based Cryptocurrency Mining Equipment Manufacturer)

Take transaction T2 as an instance, let's say, Sender B would like to transfer 100 Bitcoins to Recipient C. First, Sender B needs the Recipient C's address, which is actually the hashed version of Recipient C's public key (a string of numbers and letters). Next, Sender B is required to provide the source of 100 Bitcoins, as Sender B must be awarded from either the system (new Bitcoins) or receive from other miners. The source of 100 Bitcoins is marked in T1 in this case and Sender B would combine T1 and Recipient C's public key to generate a hash value, let's call it hash value X. At last, Sender B needs to authorise the payment by a digital signature, which also acts an irrevocable evidence for the transfer of ownership of the 100 Bitcoins. In order to create a digital signature, Sender B's private key would be used to encrypt the hash value X.

It is worth noting that a private key is also mathematically related miner's address, yet it is not the same as public key and cannot be reverse engineered from the corresponding public key so that the cryptography is secure.

Verification: Double Check the Hash Value

For transaction verification, the first thing validator (or miner) needs is the public key of Sender B, which could be found in T1 as Sender B was the recipient in previous transaction. Sender B's public key is used to decrypt the hash value x. Then, validator would then combine T1 and Recipient C's public key to generate a hash value, exactly the same as Sender B's hash computation while transferring the 100 Bitcoins. Since these are two identical hash computations, hash value generated by validator and hash value X should also be identical. If that is the case, T2 is deemed to be valid transfer of ownership of the 100 Bitcoins under the consent of Sender B.

3rd Part of Bitcoin Mechanism: Foolproof Features

Security issue is critical to blockchain technology. Hash function is one of the security features to make messages not easy to be read. Some other protocol designs provide further protections to maintain data quality, including proof-of-work which is set to substantially avoid abuses and timestamps as transaction marks to eliminate double spending.

Avoid Bad Transactions: Hash Function-Related Mathematical Puzzle

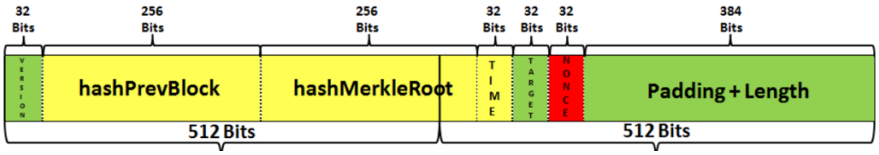
For the sake of security, proof-of-work is set to take about 10 minutes that miners are required to solve a mathematical task. The task is about generating a hash value that contain certain bits of zero, depending on the difficulty set by the system, for example, node can be required to find a nonce (aka random number) which when hashed with transactions and hash of previous block produces a hash with certain number of leading zeros, let's say 96 bits. The average effort required is exponential in the number of zero bits required but verification process is very simple and can be done by executing a single hash. As a result, success rate within a period of time

largely depends on the computational power of CPU. 'Proof-of-work' is then a factor to decide block intervals.

Avoid Double Spending: Timestamps

In order to build a foolproof distributed storage system, Bitcoin still needs to take a proactive approach to manage potential issues, for example, double spending and multiple chains.

Exhibit 3: Bitcoin Block Header



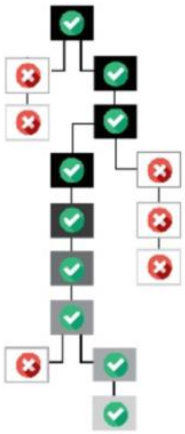
Source: University College London

Double spending in Bitcoin refers to the same batch of Bitcoins being spent more than once. In theory, if Sender B in exhibit 2 successfully transfers 100 Bitcoins from the same source T1 to two 2 recipients, Recipient C and Recipient E at the same time, Sender B would then be able to spend the same 100 Bitcoins twice. In reality, it is highly unlikely for Sender B to make two payments at the exact same time due to difference in network speed. Therefore, double spending can be eliminated by a complete transaction history as long as transactions are in a correct order. Bitcoin employs timestamp to mark every block. From the bitcoin block header above, it indicates that 32 bits in header reserved for timestamp.

Enhancement in Security: Pick the Longest Chain Record

Another potential issue is about multiple chain that the distributed public ledger ought to identically synchronise within every miner.

Exhibit 4: Resolution of Multiple Chains



Source: GDG DevFest

The network only accepts the blocks with tick labels as only the longest blockchain is valid. The rationale behind longest chain protective mechanism is based on an assumption that bad transactions are not likely to amass. As a result, the depth of block indicates the security degree of transactions and a transaction is called 1 block deep if no block linking behind. The confirmation of transactions depends on transaction participants, who might increase threshold with the importance of transactions. Therefore it could take up to an hour to confirm a transaction requiring great depth as there is only one block can be confirmed in the on average 10-minute block interval.

Under this scheme, regardless the quality of transactions, it is such a race to acquire higher computational power in order to outpace the others for higher odds to be accepted.

First Main Stream of Blockchain Application: Digital Currency

Digital currency has come under spotlight as Bitcoin price has nonstop skyrocketed to an unexpected level in 2017. Such cryptocurrencies have some common features, such as anonymity, volatile price performance and absence of corresponding regulations.

Bitcoin Price Boom: A Controversial Story Behind

Ironically, the feature of anonymity in Bitcoin system design is indeed the reason causing the Bitcoin price boom. It is true that distributed ledger can safely record the ownership of Bitcoins by public key (address), yet the record only links to digital ownership which is based on miners or computer nodes, rather than the identity of a physical person. Moreover, Bitcoin upholds decentralisation, emphasising shared ledger without a centralised authority, and thus the authority responsible for actual ownership is absent. It is because the legendary inventor, Mr. Satoshi Nakamoto's objective is to build a P2P system that can make 'one CPU one vote', such that the system is maintained and shaped by a group of miners. This objective also explained the reason for Bitcoin not focusing physical ownerships but computer nodes.

Anonymity Characteristic: Double-Edged Sword

Somehow, anonymity, borderless trade and the absence of central authority are double edged swords that these features on one hand appeals to investors, who could take a great advantage to make asset transfer in a more flexible and low profile way. On the other hand, it is such a money laundering loophole, and some parties doubt that the Bitcoin price surge is mainly attributable to money laundering and transactions related to illegal activities.

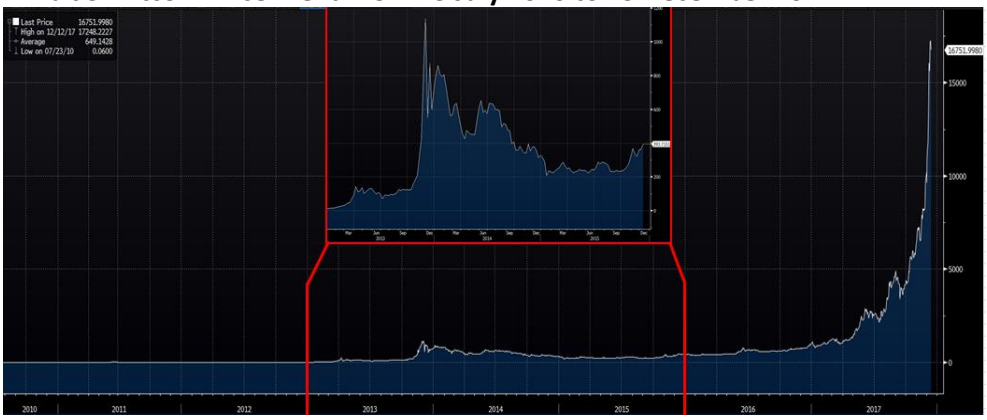
Cryptocurrency Becomes a Conduit of Financial Crimes

It is true that there have been numerous crimes involving Bitcoins were confirmed with enormous amounts of money. For instance, a digital currency exchange based in Zug, the lakeside town in Switzerland was confirmed to be utilised by money launderers, as well as a ringleader engaging in Bitcoin laundering for 6 years with the amount of US$4bn was arrested in July this year. There are similar laundering cases happening in other countries.

Bitcoin Price Was Seriously Hit by the 1st Hostile Move from China

China's government stays cautious on cryptocurrency due to its potential loopholes for crimes. The first move to restrict related activities happened in December in 2013, which incurred the following 2-year low price trend.

Exhibit 5: Bitcoin Price Trend from 23 July 2010 to 13 December 2017



Source: Bloomberg

It is obvious to see Bitcoin had encountered a long period of flat price trend from its advent, when one Bitcoin was worth only 5 to 6 US cents. Bitcoin came under the spotlight until December 2013, by that point in time, Bitcoin price skyrocketed to the level of USD1,200 in one month and then suffered from an approximately 80% crash in the following two years on the back of Chinese government's announcement against Bitcoin.

People's Bank of China (PBOC) made a statement in December 2013 to declare its stance that Bitcoin is not a real currency, and Bitcoin payment processors were ordered not to provide clearing services to such cryptocurrency exchanges. PBOC was not the only authority staying cautious on cryptocurrency, some other authorities and parties in financial industry across the globe suspected the surge of Bitcoin price was supported by money launderers, who had utilised Bitcoin's anonymity to undergo illegal transactions, such as drug dealing, ransoms to hackers, arms trafficking and so forth.

Strong Bitcoin Price Performance: Build Immunity to China's Move

Although the price has plummeted over 3 years, Bitcoin price has grown exponentially in 2017. By making a comparison between the price at commencement (US$0.05) and the current high (US$15,149.95 as at December 7, 2017), the increment of Bitcoin price is incredibly over 300k times. The strong growth momentum reflects that Bitcoin seems to be immune to the overhang posed from PBOC. It is because when PBOC further banned on ICOs and even clawed back the sales in Early-September 2017, Bitcoin price dropped by 30-40% right after the incident but then rebounded and continued to grow to the current high.

One possible reason of making less impact from China could be the shift of trading volume of Bitcoins. Before 2017, 90% of the Bitcoin trades occurred in China, but then some countries like Japan, provided legal support to Bitcoins, and thus greater demand has been stimulated outside China. On the contrary to Chinese government, Japanese authority is supportive to cryptocurrencies. This year, Japanese authority has approved 11 companies as registered cryptocurrency exchange operators, recognised Bitcoin as legal tender and started considering to set up own digital currency "J-Coin". As a result, Japan accounted for 46% of global trade volume, followed by the US for 25% Bitcoin trade, whereas China accounts for less than 12% according to the data in August 2017.

Stances from Other Countries: Gaining Global Legal Recognition

It is true that there is no global consensus on Bitcoin, while some countries such as China stays alert and acts conservatively, other countries officially approve Bitcoin to trade on exchanges and even accept Bitcoin as legal tender.

Exhibit 6: Digital Currency Exchanges in Different Nations

Stance	Country	Direction/ Advice/ Action
Friendly	Japan	Japan's Financial Services Agency has licensed more than 10 cryptocurrency exchange operators, removed the 8% consumption tax on bitcoin and enabled 260,000 retail stores to accept Bitcoin in July 2017. Moreover, Japan recognises Bitcoin as legal tender and has a relatively concrete plan to launch 'J-Coin', the official cryptocurrency in time for the Tokyo Olympics in 2020.
	Switzerland	Switzerland, particularly Zug, is known as 'Crypto-Valley' of the world. It is because FINMA (Swiss Financial Market Supervisory Authority) is lenient to cryptocurrency business in the sense that there is no special licenses needed. Therefore, some Crypto companies are jurisdiction shopping and moving to Switzerland, e.g., Xapo, a digital wallet and debit card provider.
	Singapore	The Monetary Authority of Singapore (MAS) confirmed that tokens would fall under its jurisdiction if they constitute products regulated under the Securities and Futures Act. Every cryptocurrency or token would be subject to the SFA regulation if it is deemed as a security. However, classification method is not decisive yet and MAS encourages issuers and intermediaries to consult for legal advice for now.
Neutral	United States	Cryptocurrency in the US is more certain that it has set up Fedcoin white paper, BitLicense regime for exchange and transmission in 2015 as well as guidance on SEC to regulate cryptocurrencies and tokens. US is further delving into more complicated issues, such as the diversity or consensus on digital currency among 50 states, potential new category of "crypto-banks", implementation of Fedcoin, KFC/AML related reporting and tax issues.
	United Kingdom	The FCA (Financial Conduct Authority) still needs to learn more from the regulatory Sandbox. ICO issuers currently act on own interpretation of rules. GDPR (General Data Protection Regulation) of May 2018 may create potential issues with 'right to be forgotten', allowing erasure of data. UK is at the very least not hostile to cryptocurrency since it granted a license to a digital currency payment company 'Circle'.
Hostile	Russia	While Bank of Russia expressed uncertainty and risk on cryptocurrency, Russia's President Putin then confirmed cryptocurrency will be regulated by July next year, which is Similar to MAS.
	China	Earlier in December 2013, PBOC first banned financial institutions and payment services from bitcoin-related business. After ICOs is regarded as illegal fund raising tool in September 2017, bitcoin exchanges were also required to shut down.

Sources: Sheppard, Mullin, Richter & Hampton and Autonomous NEXT

The price surge somehow forms a positive feedback circle with government support, as higher demand arouses more attention from authorities, which in turn authorities become more motivated to keep abreast with the market needs and enhance supervision through building official platforms, and thus the prices of digital currencies are boosted with higher availability in exchanges and investors' confidence.

Bitcoin Development: New Products and New Business Opportunities

Regardless the attitude of local authorities, one thing can be sure that Bitcoin or cryptocurrency is now gaining more and more popularity in public, it is now more than simply investment that Bitcoin, or other digital currencies are getting into daily life.

Development directly related to Bitcoin could be either on new product aspect and new business opportunity aspects. Moreover, it can be observed that public started paying rent in Bitcoins when owners accept, and some merchants accept Bitcoin as payment as well.

Bitcoin, Hard Forks, New Bitcoin Products

The features of digital currency like Bitcoin is indeed determined by protocol which could be altered. Bitcoin's hard forks refers to the one subjects to protocols that are not compatible with the original ones, in other word, hard forks are new products.

Exhibit 7: Comparison among Bitcoin, Bitcoin Gold and Bitcoin Cash

Comparison	Bitcoin	Bitcoin Gold	Bitcoin Cash
Supply	21 Million	21 Million	21 Million
Proof-Of-Work Algorithm	SHA256	Equihash	SHA256
Mining Hardware	ASIC	GPU	ASIC
Block Interval	10 Minutes	10 Minutes	10 Minutes
Block Size	1M	1M	8M

Source: BitcoinGold

A fork is the terminology referring to such modification and its exact meaning is 'a blockchain diverges into two potential paths forward that either with regard to a network's transaction history or a new rule in deciding what makes a transaction valid'. A fork could be hard or soft depending on the compatibility with older software.

Bitcoin cash and Bitcoin gold are of the products of two hard forks for different purposes and both of the new products are automatically and proportionally distributed to holders of Bitcoin. Since Bitcoin cash and Bitcoin gold remain 21mn as the maximum amount in circulation, holders of Bitcoin would fairly receive one Bitcoin cash / Bitcoin gold for each Bitcoin held at the beginning of the issuance.

Hard Forks: Bitcoin Cash for Growing Transaction Volumes

Bitcoin cash is an improved protocol as Bitcoin community addressed the issue on growing transaction volume. The community believed maximum size of a block should be increased in order to handle more transaction in one block, which in turn shorten the duration of a transaction. Bitcoin cash, which started trading in August 2017, has 8 times the maximum block size of Bitcoin, from 1Mb to 8Mb.

Hard Forks: Bitcoin Gold to Solve Dominance in Mining

Following Bitcoin cash, another hard fork Bitcoin gold was launched 3 months later. Bitcoin gold aims to maintain the legendary inventor Satoshi Nakamoto's tenet of 'one CPU one vote' such that the system could be per se decentralised. In Bitcoin market, the mining power becomes dominated by professional miners along with ASIC (application specific integrated circuit) products, making the current Bitcoin 'one ASIC one vote'. ASIC is designed specifically for mining that could compute SHA256 calculations millions of times faster than PC miners.

Such significant outperformance would squeeze PC miners out, therefore Bitcoin gold replaced SHA256 algorithm with Equihash algorithm. Equihash is memory orientated rather than relying on computing power and is most effectively solved by GPUs which are mainstream products available to PC miners. By doing so, Bitcoin gold mining is expected to be fairly decentralised again. Lastly, Bitcoin gold employs the same distribution rules as Bitcoin cash that holders of Bitcoin received same amount of Bitcoin gold as the amount of Bitcoin held and the maximum amount in circulation is unchanged.

Hard Forks: Bitcoin Fork Failure

Bitcoin itself attempted to undergo a fork in November 2017 as well. Replacing the original Segwit with Segwit2x is a kind of upgrade that changes the size of blocks from 1Mb to 2Mb so as to make improvements in speed and cost. Despite the failure of this fork, there may be more hard forks in the future whenever Bitcoin community believes an improvement should be made. In this fast changing digital currency world, it is full of business opportunities in improving investors' competition and making payment and mining more effective. Exhibit 8 displays some of the popular companies in respect of three main categories: mining, exchanges and payment system.

Bitcoin Development on Business Opportunities

When the market becomes more demanding and is having more new products, it provides numerous of business opportunities in the meantime. Three types of businesses grow especially prosperous with the increasing popularity of Bitcoin.

Exhibit 8: List of Companies Related to cryptocurrency

Categories	Company Name	Company Description
Mining related	AntPool	A mining pool based in China, provides mining services of several cryptocurrencies such as BTC, BCH, ETH, ETC.
	BitFury	BitFury offers hardware products and software services, including servers, ASIC chips, lightning network and PaaS (platform as a service).
	21 Inc	The group offers ASIC chips for mining and develops micropayment marketplace to trade APIs in digital currency.
Exchange operators	Coinbase	The largest bitcoin exchange that was the 3rd to be granted BitLicense (a virtual currency and money transmitter license) by New York Department of Financial Services in January 2017.
	Bitflyer	Both of the Japanese bitcoin exchanges received formal operating licenses from Financial Service Agency, the Japanese regulator.
	Quoine	
Payment System	Circle International Financial	The 1st P2P payment company to be granted BitLicense in September 2015. It is also a licensee of UK authority to provide services in Euro zone.
	Ripple	The group provides payment network and settlement infrastructure to financial giants, UBS and Santander for example. It issues own digital currency (XPT) for FX services and it was the 2nd awardee of BitLicense.
	Blockstream	The company develops Bitcoin application, particularly sidechains and software to facilitate interoperability between main chain and sidechain.
	Digital Asset Holdings	It is a provider of distributed ledger technology which is specially focused in financial industry.

Sources: Taiwan Institute of Economic Research and Autonomous NEXT

Digital currency investors are always in need of three complementary services: mining pools or hardware, exchanges and payment systems.

The first two categories are mainly referring to cryptocurrency holders. Mining related businesses help investors to improve computational power of their nodes by either subscribing the centralised mining pools or purchasing professional ASICs for their own computers. The hash rate of CPUs closely link to the mining results. Participants who have a cryptocurrency wallet would eventually exchange for fiat currency in order to recognise the gains, and thus exchange operators are required to support. Payment system targets institutional clients which aims to develop own decentralised network on blockchain technology.

Digital Currency: Fits Better As a Payment than Value Storage

So far digital currency is the most popular application of blockchain, yet the status of digital currency remains uncertain after a decade from its advent. Let alone illicit usages and speculation on price, investors who bought Bitcoin either treat it as a payment medium or value storage like gold. Although there are defeats of Bitcoin features for both usages, digital currency does fit payment gateway better than value storage.

For value storage, digital currency inherently does not resemble gold in the sense that gold has intrinsic value whereas Bitcoin does not. In other word, while gold by itself worth something as a kind of precious metal, Bitcoin could be sheer rubbish that have no value if something happens to the system or the market.

On the other hand, the underlying technology of digital currency is foolproof to make transaction records. By design of the underlying blockchain technology of Bitcoin, every miner theoretically acts as a validator, who is responsible to verify new blocks and keep the copy of whole blockchain, therefore it is hard for hackers to manipulate due to numerous records distributed in the system. Also, there are different kinds of hashes preventing issues including double spending and inconsistent blockchain records and thus all transactions could be accurately traced.

Digital Currency Use Case: Modifications Are Needed

Without doubt, security and accuracy are of utmost importance to the storage part of a payment system, however payment gateway would also require to have ability to process in a short time frame so that the gateway is able to handle large volume of transactions. Speed could be a potential challenge to blockchain as it takes time for the ledger to go through all nodes and make a copy. The duration is especially long for the one employing proof-of-work to verify the block, let's say Bitcoin, the system sets block interval on average to be 10 minutes. Also, requiring all nodes to store one copy might be space consuming. Fortunately, these traits could be modified when applying for payment system that covers an active or large transaction network. Notwithstanding, more easy-going proof-of-work and fewer nodes are at the expense of security level and often aspects to be considered if the payment network is used in public sector.

Digital Currency Use Case: Blockchain in Public Sector

In the age of digitalisation, spending habit of general public has dramatically changed that public's payment style is shifting from physical to digital. Digital transformation happens in different forms, some societies favour mobile wallet, whereas some prefer debit or credit cards.

It is such a global trend to move towards cashless society. According to the report for e-krona (Swedish version of state-issued digital currency) project, card payment in terms of number of transactions also encounter digitalisation that Sweden recorded linear growth in the past decade. China, as a developing country has slightly different style of retail consumption. Card and cash payment types are still dominant with 71% market share together but it has growing trends in mobile and internet payment which obtain larger market share in 2016, stated by a United Nations report. When electronic payment becomes more prevalent and consumers are increasingly adaptive to this new payment style, government started considering to issue digital fiat currency. A number of central banks launch pilots or research on state-issued digital currency, including Bank of Canada, Bank of England, the People's Bank of China, Riksbank of Sweden, Federal Reserve and so forth.

State-Issued Digital Currency: 4Ws

What is State-Issued Digital Currency?

One common definition for state-issued digital currency is an intangible form of money issued by central bank for general public. However, authority is free to decide the exact definition of state-issued digital currency based on its own objectives and status quo of the country.

Why State-Issued Digital Currency is needed?

Central banks around the globe get motivated to study state-issued digital currency because of two main benefits: a digital currency backed by central bank is supposed to be risk free and electronic payments are traceable that help deter some sort of financial crimes.

Isn't Monetary System Working Well?

People may wonder why central bank attempts to interfere the already smoothly functioning monetary system, in which credit card and mobile wallet are providing convenient services to consumers and gaining market share. In particular, credit card has a long history that its infrastructure is relatively mature and comprehensive. The biggest difference between mobile wallet and state-issued digital currency is the inherent credit risk that mobile wallet could collapse and run out of business. Credit card centre is also vulnerable to cyber risk and financial risk. Therefore, state-backed digital currency with blockchain technology is able to offer more protection to consumers and the society as a whole.

Who will Be Covered?

State-issued digital currency is expected to cover the whole society based on the common definition in prior section. However, some countries may be less revolutionary or more conservative on digitalising the monetary system that the serving circle may merely include central bank and commercial banks.

How Will State-Issued Digital Currency Serve the Target Group?

The state-issued digital currency system models discussed in this section assumes the digital currency targets general public. The implementation features depend on the direction that central bank would like state-issued digital currency to be. In fact, state-issued digital currency could be shaped more or less like cash. Exhibit 9 describes two possible models in which value based model favours cash.

Exhibit 9: Current Status of State-backed Digital Currency

Attributes	Value Based (Cash-like)	Register Based (Blockchain)
Physical Presence Required	Store digital money locally in an app or on a card, no need to create account in central bank	Store digital money in central bank, consumers can use card or mobile app as a linkage to account to make payment
Credit Risk	No credit risk, backed by central bank	No credit risk, backed by central bank
Offline Function	Support, as record is stored in a physical device	Does not support, as record is stored in central bank which needs to link to the storage point to update the balance
Anonymity	Provide anonymity with no personal account required in central bank	Selectively provide anonymity by setting the protocol, transaction below a certain amount could keep privacy
Protection/ Traceability	Serve as cash that lost card will not have any means to protect money inside	Central bank will keep record through distributed ledger
Usability	require card reader / smartphone to do transaction	Can be managed via apps or online
Relative Advantages	Less preparation work, cost and time to launch	More potential for future development, such as settlement finality (netting) and partial anonymity
Relative Disadvantages	Less upside potential that very limited new functions or value added service could provide	More preparation work to do, higher cost and more complex that may need to cooperate with third parties in order to share costs

Sources: Riksbank's e-Krona Project Report, R3 Report on Fedcoin

Only two potential models are discussed due to high diversity. State-issued digital currency system model is definitely not limited to only two options listed above, its features could be mixed between two models or other innovative designs as long as the model fits central bank's objectives best.

State-Issued Digital Currency: Permissionless Blockchain for Security

When it comes to financial crimes, let's say money laundering and tax evasion, anonymity is always a great helper to make authorities hard to detect and prove the illegality, this is also the potential reason for Bitcoin gaining popularity.

State-issued digital currency could make money more traceable by requiring public to open accounts in order to hold digital money. The traceability is even more extensive if central bank directly manages accounts.

However, the actual supervision over digital currency remains uncertain unless the whole implementation model is confirmed. It is because digital currency could be stored in card and act more like cash rather than money in deposit account. Also, the advent of state-issued digital currency does not mean to completely replace cash that both forms of currency might coexist. If this is the case, state-issued digital currency is less constructive as a deterrent to financial crimes.

Fiat Digital Currency: Bitcoin, Does Not Fit for Monetary System

Bitcoin has been established for about a decade and thus it could be deemed as the leader in the field. Bitcoin therefore enjoys larger-than-peers user base, more trading platforms, more comprehensive infrastructure and wider acceptance. Nevertheless, central bank does not use this existing private cryptocurrency straight away because Bitcoin fails to fulfil two pivotal criteria: price stability and monetary control.

Bitcoin Does Not Fit Monetary System: Price Volatility

As a matter of fact, Bitcoin is an extremely volatile currency to the extent that it is hard to be stabilised through pegging. Reminding the price trend of Bitcoin, it has rocketed by 16 times from approximately US$1,000 to US$16,000 in the first 11 months this year. Such significant price movements require enormous central bank's reserve to keep the peg, but still, the price level could be seriously affected by speculators around the world which then leads to a breakdown. As a result, it is better to establish a state-issued digital currency in order to safely remain the peg to fiat currency.

Bitcoin Does Not Fit Monetary System: Supply Rigidity

Another defect of Bitcoin is its supply rigidity, which is fixed at maximum equal to 21mn in circulation. Since digital fiat currency is in circulation, the digital money is considered as one of the sources of money supply, making it an element be taken into account when central bank implements monetary policy, such as setting reserve rate, interest rate and operation in open market. In light of the effect of money supply, central bank needs the digital currency to have creation and redemption mechanism to maintain the effectiveness of monetary policy.

State-Issued Digital Currency: Role of Blockchain

One thing worth noting is that although blockchain is one of the key elements in state-issued digital currency projects, the system is not necessarily employ blockchain as there are other technologies eligible to support the infrastructure. In addition, the inclusion or exclusion of blockchain may not directly affect end-users, general public, when it serves as the underlying technology for the digital money system infrastructure.

Blockchain technology is being considered by different countries because of the security feature. Its security level outperforms current centralised database due to increased number of storage points. Recalling the blockchain mechanism, its security feature is built by "distributed ledger technology" and "proof-of-work". Distributed ledger technology allows transaction record to be stored in numerous nodes (also known as miners in previous section), such that transaction records are hard to be manipulated and lost. Besides, the "proof-of-work" is an economic mean to protect the distributed ledger from being abused and attacked. In Bitcoin example, the 10-minute work and block interval can significantly deter malicious attempts.

Blockchain Could Cater To State-Issued Digital Currency

There are many possible ways to modify the blockchain protocol to cater to the use of state-issued digital currency. One possible solution could be authorising a group of nodes (aka permissioned blockchain) which does not need to go through the time-consuming proof-of-work process. In the meantime, the public ledger only goes through those authorised nodes instead of every node in the system, under the assumption that the group of authorised nodes is trustworthy.

Blockchain Is Not the Only Choice for State-Issued Digital Currency

Blockchain technology's advantage of more secure protection is at the expense of transaction time and storage capacity that make blockchain does not fit digital currency system purpose. Regardless the exact target group of state-issued digital currency which could be general public or commercial banks only, it is expected to handle large volume of transactions, therefore some countries consider not to adopt the blockchain system designed for Bitcoin.

Nothing comes without a price, when the transaction time and required capacity are reduced by shrinking the circle of storage nodes, the security level is relatively lower. To summarise, the digital currency system could be centralised, like the most prevalent design, or be completely distributed as Bitcoin, or partially distributed as permissioned blockchain which is just mentioned. None of the proposed system is perfect per se that there must be tradeoffs among time and cost and security. Authorities determine the specifications based on their own objectives, situations and applications.

When Will State-Issued Digital Currency Be Ready?

State-issued digital currency is still far from ready as the issuance is disruptive that every citizen would be affected, therefore governments are required to have exhaustive pilot runs and thoughtful plans to settle potential issues. Barriers to issuance could arise from the balance between costs and benefits, citizens outside the service range, complementary support from other countries and so forth.

Exhibit 10: Progresses on Stated-Issued Digital Currency in Different Countries

Country	Progress
Japan	J-Coin, cooperates with banks and is still in the early stages. It would be pegged to the yen and be spent through a mobile app. It plans to launch in 2020.
Sweden	Both MAS (Monetary Authority of Singapore) and Riksbank have close interests in state-issued digital currency. Their white paper include some related guidance and legal issues. Particularly, Riksbank of Sweden will soon take a stance on e-krona in 2018.
Singapore	
United States	Still exploring state-issued digital currency. No concrete implementation plan and progress.
United Kingdom	Bank of England has been engaged in the research in 2015, but it is still not certain if official digital currency will be launched.
China	China has completed trial runs on algorithms for digital currency and the test transactions between the central bank and commercial banks were successful.

Sources: Forbes, CNBC, Bloomberg

Most of the countries are still exploring the characteristics of official digital currency and potential issues. Therefore, it is not likely for central banks except Japan to issue fiat cryptocurrency in near future.

1st Barrier to State-Issued Digital Currency: Economical Feasibility

First of all, official digital currency must be economically feasible to the extent that the project should at the very least do not cause long term deficits. In other word, the financial benefits of official digital currency, which are to combat against tax evasion, terrorism financing and other financial crimes, should be equal or even outweigh the financial burdens risen from building infrastructure, promotion, additional labours for transitional period and related administrators.

2nd Barrier to State-Issued Digital Currency: Cross-Border Transactions

Without global support, the benefits of state-issued digital currency cannot be completely unfettered. In reality, currency is not an isolated exchange medium that flows of money across borders are inevitable. Therefore, the new form of currency might need global reconciliation. The need of reconciliation is easier to resolve at institutional level. Unlike general public who rely more on cash, the isolated digital currency could bring them into troubles especially during exchanging foreign currency.

3rd Barrier to State-Issued Digital Currency: Minority Group

Practically speaking, it is hard to get rid of cash as there must be a group of people not able or prefer to hold cash instead of electronic money. The poor or elderly will have lower accessibility to the new system when they are hard

to keep abreast with state-of-the-art technology. Also, counterparties of general public include numerous types of merchants and others could be on a very small scale, and thus government should offer universal education and support on the new currency or even make it as obligations for merchants to cooperate.

Surely, there are fields not yet mentioned that should be concerned for such new form or category of fiat currency. Digital currency is not yet ready until concrete plans to fill the loopholes and potential issues, in order to avoid chaos and make sure the issuance can function well.

Second Main Stream of Blockchain Application: Smart Contract

Smart contract is a type of applications built on a blockchain network and it is not merely about payment. Ethereum extends the use cases of smart contract by offering extensive open source code and existing blockchain infrastructure, realising more innovative ideas on the decentralised network.

Go Beyond the Bitcoin Hype: A Chain of Applications in Smart Contracts

In blockchain, every application can be seen as a smart contract. A smart contract can be understood as a digitalised contract, in which a set of terms and conditions are pre-defined, and the contract is expected to execute once it is fulfilled. As a result, even Bitcoin could be deemed as the basic application of smart contract. For Bitcoin or similar payment system, the terms and conditions are to provide payment destination and source of money, the transaction would be implemented once validators (nodes) offer authentication and the majority of nodes reach consensus.

Smart contracts in payment case contain transactions as message. However, the message could be anything other than transactions, this flexible feature makes smart contracts fit more complicated and innovative applications.

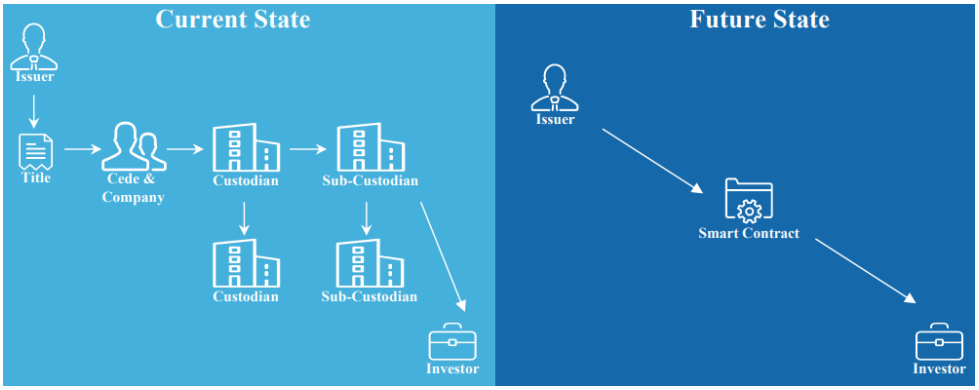
Making good use of smart contract concept, developers could program own smart contracts, transforming them into autonomous agents. Autonomy largely comes from following three functions:

1. Information storage, which allows application to manage registration or membership records in order to build a circle of participants.
2. Multi-signature function, which enables parties to take irrefutable position in the contract.
3. Execution, such that the agreement could be automatically executed whenever certain conditions are fulfilled.

Smart Contract Use Case in Finance Sector

The primary advantages of smart contracts distributed ledger technology are to simplify handling procedures which in turn to save manual handling costs. Also, systematic handling is able to enhance reliability with increased number of storage point and efficiency by sharing data.

Exhibit 11: Smart Contract Use Case in Securities



Sources: Chamber of Digital Commerce

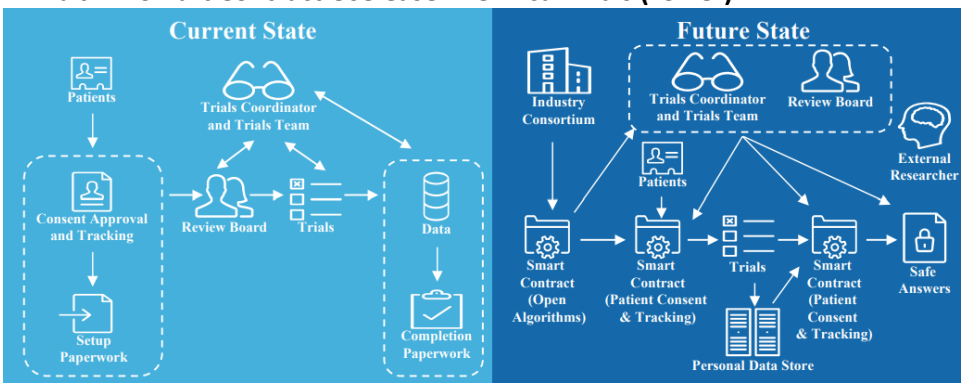
Procedures and paperwork on securities are originally laborious and full of intermediaries between the group of investors and that of issuers. By digitalising end-to-end workflows on a distributed ledger, such as payment of dividends, stock splits and corresponding voting, the processing time is significantly shortened, in the meantime, operational and counterparty risks are removed with automation.

SWIFT started considering to build a distributed ledger technology platform for cross-border payments in order to shorten the processing time frame and operational costs. The new platform is expected to process transactions in real-time such that banks need to monitor the funds in their overseas accounts via debit and credit updates and end-of-day statements.

Non-Financial Smart Contract Use Case

Smart contract is not limited to financial services. Due to the 'Turing Complete' feature in programming, developers can fit smart contract in any use cases as long as it is composed of terms and conditions and wishes to automatically execute.

Exhibit 12: Smart Contract Use Case in Clinical Trials (Lower)



Sources: Chamber of Digital Commerce

Clinical trials involve three main data fields to process. First, the board needs to track the patients who are consent to join the clinical trial program. Then, the trails coordinator is required to store result data of trials under each participant. Lastly, the trial data should be viewed by corresponding teams which are permissioned by both patients and the coordinator to access the data. The smart contract models for clinical trials could be further extended to support other functions, such as incentive program to automatically reward patients for sharing data.

The efficiency of health data collection is likewise improved by smart contract that some cumbersome steps could be replaced by a one-step end-to-end workflow.

Difference in ICOs and ITOs

ICO, initial coin offering, is a term more commonly used in new cryptocurrency businesses. Notwithstanding, ICO technically only refers to issuance of native cryptocurrency coin, which is a unit of value native to a blockchain. The blockchain with own native coins is primarily used as a medium of exchange with limited functionality beyond. On the other hand, the token in ITO (initial token offering) is the medium of exchange in DApp (decentralised application). An application has particular services and functions and it is not standalone since DApp is built and it is running on an existing decentralised network. Token's main functions are to allow token holders to use the services and use as a medium of exchange in the corresponding application.

Exhibit 13: Native Coins and Prominent Projects Built On ERC20

Categories	Name	Description
Native Coins	Bitcoin (BTC)	Both cryptocurrencies are used for payment under distributed ledger technology.
	Litecoin (LTC)	
	Ethereum (ETH)	A coin issued by an open-source public DLT (distributed ledger technology) platform, Ether is used to indicate the value of project tokens.
	Ripple (XRP)	XRP is used to support currency exchange and remittance network by Ripple.
DApps (ERC20 Tokens)	Storj (STORJ)	A decentralised cloud storage that rents out the extra space shared from participants.
	Civic (CVC)	Civic is a platform to process verification through a decentralised network. The Civic currency is designed to transact in these services.
	Gnosis (GNO)	Tokens are used to reward correct predictions in any topics/ issues.
	Status (SNT)	Status is an open source of DApp that covers messaging platform, payment system and mobile web browser. SNT is the token of Status and is giving holders the power to choose the development direction of this platform.

Sources: PitchBook, Autonomous NEXT

Not all blockchains of native coins can build DApps. In the list above, four popular native coins in which three of them are designed for payments and thus each of their blocks merely contain transactions. Conversely, the block in Ethereum contains code-based contracts that could be programmed as aforementioned 'DApps' and contracts on DApps are exactly the applications suggested in exhibit 13 that automatise work procedures. DApp could create own tokens for internal uses. Tokens could be constructed by the Ethereum token standard ERC20 (or ERC223, the modified version). Ethereum provides a highly flexible open source code for developers to build diverse and innovative DApps. Since building smart contracts on existing decentralised network effectively save cost and effort, there are more than 800 DApps up to this point.

It is noteworthy that Ethereum is not a unique way to develop decentralised applications. Since the underlying decentralised network merely serves as infrastructure, application could be based on networks provided by others or even set up on its own. The reasons for Ethereum as a dominant platform are its ready and open resources.

Legality on Cryptocurrency Related Activities in Other Countries

Currently, there is not a new set of regulations released to specifically identify the business model of ICOs or ITOs or cryptocurrency-related intermediaries. Most of the countries use makeshift regulations to handle this growing market. By applying existing regulations on securities or funds, these activities would then be under scrutiny as long as they are deemed as securities.

SEC provides a set of guidance called Howey Test to help issuers and related parties to know if the business constitutes regulated activities. A group of factors, ranging from ownership to the control, used to distinguish securities by Howey Test in exhibit 13. Most of the places follow SEC's way to manage

the new market with minor variations. For example, SFC, MAS (Monetary Authority of Singapore), ESMA (European Securities and Markets Authority) and FSRA (Financial Services Regulatory Authority in UAE) basically apply the regulations on securities to cryptocurrency market, the main difference is the method to identify whether it belongs to a security is on a case-by-case basis instead of sticking to Howey Test.

SEC's Howey Test, Putting ITO under Securities Laws

As a matter of fact, not all ICOs or ITOs fall into the regulatory precinct. Storj, a decentralized cloud storage platform mentioned in Exhibit 12 is one of the ITOs that should not be deemed as security according to Howey Test. It is because Storjcoin has actual functionality that is used to purchase storage space and reward the space contributors. For the ones not being classified as securities, authorities still encourage them to improve their practices with independent legal advices.

Exhibit 14: Howey Test by SEC

Categories	Investment/ Securities Features	Merely Functional Features/Rights
Ownership	Ownership interest in a legal entity, including a general partnership	Rights to program, develop or create features for the system or to "mine" things that are embedded in the system
Interest	Equity interest	Rights to access or license the system
Value Base	Share of profits and/or losses, or assets and/or liabilities	Rights to charge a toll for such access or license
Position	Status as a creditor or lender	Rights to contribute labor or effort to the system
Control/ Rights	A feature allowing the holder to convert a non-security blockchain token into a blockchain token or instrument with one or more investment interests, or granting the holder an option to purchase one or more investment interests	Rights to vote on additions to or deletions from the system in terms of features and functionality
Obligation	Holder of a repayment obligation from the system or the legal entity issuer of the blockchain token	Rights to sell the products of the system;
Bankruptcy Issue	Claim in bankruptcy as equity interest holder or creditor	Rights to use the system and its outputs

Sources: Sheppard, Mullin, Richter & Hampton and Autonomous NEXT

Notwithstanding, authorities are expected to eventually develop a set of regulations that are tailor made for cryptocurrency market in order to have an exhaustive scrutiny. Some more pivotal legal issues are being excluded for now: tax treatment, cybersecurity requirements, investor protection, AML/KYC, internal governance and so forth are the fields to be worked on.

Stay Positive on Future Smart Contract Development

Smart contracts are definitely a fast growing industry that up to Q3 in 2017, the average volume per ICO or ITO is US$7.9mn, almost double average volume yoy in 2016. Taking a glimpse of threat and opportunity, blockchain business is still likely to keep on growing prosperous in the future.

Limited Treats on Future Smart Contract Development

When it comes to threats, the most challenging barrier to the entire industry is regulatory risks as the market is still green, majority of the nations have not yet specifically set up corresponding laws. It is completely possible that these countries may strictly regulate against or even ban such activities like China. Cryptocurrency related businesses may be affected but regulatory risk seems not to be a serious adversity as authorities are not likely to kill a business type that does not give a major negative impact to the society. Moreover, unless the regulatory adversity is on a global scale, otherwise cryptocurrency / smart contract businesses could take advantage of regulatory arbitrage and continue to provide online services.

Great Upside Potential with High Interoperability

As a matter of fact, the nature of smart contracts brings myriad of opportunities to new businesses. Smart contracts are of 'Turing Complete' which supports developers' innovative ideas by offering a broad set of computational instructions. The compounding opportunities are the nature of smart contract businesses and interoperability feature, which always run in a sequence, triggering one business by another business. For instance, the smart contracts for bond issuance needs another off-chain system to support payment procedures, or there might be other one-stop smart contracts occurred as competitors that using on-chain digital currency to settle payment, the market would then need a smart contract to be the transfer agent, moving the account from one model to another, or a DApp that integrates smart contracts to manage several accounts at once.

Conclusion: Disruptive Technology, Takes Time to Implement

FinTech is a financial innovation through technology that brings great potentials to deliver substantial improvements in productivity and financial service quality. Blockchain is one of the FinTech segments that comes under the spotlight due to the Bitcoin price surge. Blockchain technology is a decentralised network to provide flexibility for developers to freely design the system and offer high security via asymmetric encryption, digest algorithms, multiple storage points and proof-of-work validation process. Blockchain technology has two primary streams that are digital currency (aka cryptocurrency) and smart contracts.

Bitcoin is the first and the most popular blockchain-based digital currency. The demanding cryptocurrency market fosters innovators to move forward that there are more cryptocurrency-related companies coming up, most of them are specialising in mining digital coins, operating digital exchanges and digital payment systems. In the meantime, more new products are launched, including Bitcoin Gold, Bitcoin Cash, and other ICOs. In addition, the fast emerging cryptocurrency market globally arouses central banks' interests in state-issued digital currency under blockchain infrastructure. Certainly, authorities will enlarge its regulatory coverage to this new territory in order to avoid related crimes and maintain good market order.

For smart contract, it is even greener business than digital currency to the extent that most of its potential applications are still at a conceptual stage or right after ITOs. Smart contract is highly versatile that it can be applied to most of the use cases as long as the case consists terms and conditions, and then the contract can be digitalised and self-execute under corresponding rules set by computer codes. Running smart contracts on a programming platform can bring a lot of business opportunities as smart contracts are able to interoperate with one another. Therefore, the need for one service could trigger the need of another service. Ethereum is the most popular blockchain application platform to encourage developers to build smart contracts on top of its decentralised network. Ethereum is not only Turing Complete that provides a programming platform for developers to design applications, but also offers existing decentralised network to make smart contracts securely implement on a blockchain infrastructure. Therefore, the emerging smart contract might bring a revolutionary improvement to the society in the future.

ANALYST CERTIFICATION

THE RESEARCH ANALYST, YANNY CHU, WHO IS PRIMARILY RESPONSIBLE FOR THE CONTENT OF THIS RESEARCH REPORT, IN WHOLE OR IN PART, CERTIFIES THAT WITH RESPECT TO THE SECURITIES OR ISSUER THAT THE ANALYST COVERED IN THIS REPORT: (1) ALL OF THE VIEWS EXPRESSED ACCURATELY REFLECT HIS OR HER PERSONAL VIEWS ABOUT THE SUBJECT SECURITIES OR ISSUER; AND (2) NO PART OF HIS OR HER COMPENSATION WAS, IS, OR WILL BE, DIRECTLY OR INDIRECTLY, RELATED TO THE SPECIFIC VIEWS EXPRESSED BY THAT ANALYST IN THIS REPORT.

BESIDES, THE ANALYST CONFIRMS THAT NEITHER THE ANALYST NOR HIS/HER ASSOCIATES (AS DEFINED IN THE CODE OF CONDUCT ISSUED BY THE HONG KONG SECURITIES AND FUTURES COMMISSION) (1) HAVE DEALT IN OR TRADED IN THE SECURITIES COVERED IN THIS RESEARCH REPORT WITHIN 30 CALENDAR DAYS PRIOR TO THE DATE OF ISSUE OF THIS REPORT; (2) WILL DEALT IN OR TRADED IN THE SECURITIES COVERED IN THIS RESEARCH REPORT 3 BUSINESS DAYS AFTER THE DATE OF ISSUE OF THIS REPORT; (3) SERVE AS AN OFFICER OF ANY OF THE HONG KONG LISTED COMPANIES COVERED IN THIS REPORT; AND (4) HAVE ANY FINANCIAL INTERESTS IN THE HONG KONG LISTED COMPANIES COVERED IN THIS REPORT.

RECOMMENDATION DEFINITIONS
BUY: SHARE PRICE EXPECTED TO APPRECIATE 20% OR MORE IN THE NEXT 12-MONTH
HOLD: SHARE PRICE EXPECTED TO APPRECIATE BETWEEN 5% AND 20% IN THE NEXT 12-MONTH
SELL: SHARE PRICE EXPECTED TO APPRECIATE LESS THAN 5% IN THE NEXT 12-MONTH
NOT RATED: NO SPECIFIC SHARE PRICE ESTIMATIONS ARE MADE

DISCLOSURES OF RELEVANT BUSINESS RELATIONSHIP
HOORAY SECURITIES LIMITED (THE "HOORAYSEC") AND ITS AFFILIATE HOORAY CAPITAL LIMITED (TOGETHER THE "HOORAY GROUP") ARE LICENSED CORPORATIONS UNDER THE SECURITIES AND FUTURES ORDINANCE (THE "SFO"), MAY, UNDER CIRCUMSTANCES PERMITTED BY LAW, PARTICIPATE IN THE OFFERINGS OF SECURITIES MENTIONED IN THIS REPORT.

HOORAY GROUP MAY, TO THE EXTENT PERMITTED BY LAW, OWN OR HAVE A POSITION IN THE SECURITIES OF (OR OPTIONS, WARRANTS OR RIGHTS WITH RESPECT TO, OR INTEREST IN, THE SHARES OR OTHER SECURITIES OF) THE COMPANY. HOORAY GROUP MAY ADD TO OR DISPOSE OF ANY SUCH SECURITIES OR MAKE A MARKET OR ACT AS A PRINCIPAL IN ANY TRANSACTION IN SUCH SHARES OR OTHER SECURITIES. HOORAY GROUP MAY FROM TIME TO TIME PROVIDE INVESTMENT BANKING, UNDERWRITING OR OTHER SERVICE TO, OR SOLICIT INVESTMENT BANKING, UNDERWRITING, OR OTHER BUSINESS FROM THE COMPANY.

HOORAY GROUP HAS NO MORE THAN 1% FINANCIAL INTERESTS IN THE COMPANY AS AT DECEMBER 13, 2017.
HOORAY GROUP DOES NOT ACT AS A MARKET MAKER FOR THE COMPANY ON DECEMBER 13, 2017.
NO EMPLOYEE OF HOORAY GROUP SERVES AS AN OFFICER OF THE COMPANY AS AT DECEMBER 13, 2017.
HOORAY GROUP ACTS NO INVESTMENT BANKING ROLES FOR THE COMPANY WITHIN THE PAST 12 MONTHS.

DISCLAIMER
THIS DOCUMENT IS STRICTLY CONFIDENTIAL TO THE RECIPIENT, AND MAY NOT BE DISTRIBUTED TO THE PRESS OR OTHER MEDIA, AND MAY NOT BE REPRODUCED IN ANY FORM, AND MAY NOT BE TAKEN OR TRANSMITTED INTO THE UNITED STATES OR PROVIDED OR TRANSMITTED TO ANY U.S. PERSON (WITHIN THE MEANING OF REGULATIONS UNDER THE U.S. SECURITIES ACT OF 1933, AS AMENDED), INCLUDING ANY BRANCH OR AGENCY OF A NON-U.S. PERSON(S) LOCATED IN THE UNITED STATES. FAILURE TO COMPLY WITH THIS RESTRICTION MAY CONSTITUTE A VIOLATION OF UNITED STATES SECURITIES LAWS. THIS REPORT MAY NOT BE SENT INTO CANADA OR TO ANY CANADIAN PERSON. THIS REPORT MAY NOT BE SENT INTO JAPAN. THIS REPORT MAY NOT BE DISTRIBUTED OR PASSED TO ANY PERSON OTHER THAN A PERSON WHOSE ORDINARY BUSINESS IS TO BUY OR SELL SHARES OR DEBENTURES, WHETHER AS PRINCIPAL OR AS AGENT. THE DISTRIBUTION OF THIS REPORT IN OTHER JURISDICTIONS MAY BE RESTRICTED BY LAW, AND PERSONS INTO WHOSE POSSESSION THIS REPORT COMES SHOULD INFORM THEMSELVES ABOUT, AND OBSERVE, ANY SUCH RESTRICTIONS. BY ACCEPTING THIS REPORT, THE RECIPIENT AGREES TO BE BOUND BY THE FOREGOING LIMITATIONS.

THIS REPORT HAS BEEN PREPARED BY HOORAY GROUP TO PROVIDE BACKGROUND INFORMATION ABOUT THE COMPANY. IT HAS BEEN PRODUCED INDEPENDENT OF THE COMPANY, AND THE FORWARD-LOOKING STATEMENTS, OPINIONS, AND EXPECTATIONS CONTAINED HEREIN ARE ENTIRELY THOSE OF HOORAY GROUP AND ARE GIVEN AS PART OF ITS NORMAL RESEARCH ACTIVITIES AND NOT IN CONNECTION WITH ANY OFFERING OF SECURITIES OR AS AN AGENT OF THE COMPANY, ITS SHAREHOLDERS OR ANY OTHER PERSONS. THE READER IS CAUTIONED THAT ACTUAL RESULTS MAY DIFFER MATERIALLY FROM THOSE SET FORTH IN ANY FORWARD-LOOKING STATEMENTS HEREIN. WHILE ALL REASONABLE CARE HAS BEEN TAKEN TO ENSURE THAT THE FACTS STATED HEREIN ARE ACCURATE AND THAT THE FORWARD-LOOKING STATEMENTS, OPINIONS AND EXPECTATION CONTAINED HEREIN ARE BASED ON FAIR AND REASONABLE ASSUMPTIONS, NONE OF HOORAY GROUP, ITS ASSOCIATES INCLUDING HOORAYSEC, AND THE COMPANY HAS INDEPENDENTLY VERIFIED ANY OF THE INFORMATION HEREIN. IF THE COMPANY SHOULD AT ANY TIME COMMENCE AN OFFERING OF SECURITIES, ANY DECISION TO INVEST IN ANY SUCH OFFER TO SUBSCRIBE FOR OR ACQUIRE SECURITIES OF THE COMPANY MUST BE BASED WHOLLY ON THE INFORMATION CONTAINED IN THE FINAL OFFERING MEMORANDUM ISSUED OR TO BE ISSUED BY THE COMPANY IN CONNECTION WITH ANY SUCH OFFER AND NOT ON THE CONTENTS HEREOF. THIS IS NOT AND SHALL NOT BE TREATED AS AN OFFER (OR SOLICITATION OF AN OFFER) TO BUY OR SELL THE SECURITIES/INSTRUMENTS MENTIONED. HOORAY GROUP DOES NOT REPRESENT THIS IS ACCURATE OR COMPLETE AND WE MAY NOT UPDATE THIS. ACCORDINGLY, NONE OF THE COMPANY, ANY UNDERWRITER OF SECURITIES OF THE COMPANY, OR ANY OF THEIR RESPECTIVE DIRECTORS, OFFICERS OR EMPLOYEES, SHALL IN ANY WAY BE RESPONSIBLE FOR THE CONTENTS HEREOF, OR SHALL BE LIABLE FOR ANY LOSS ARISING FROM USE OF THIS REPORT OR OTHERWISE ARISING IN CONNECTION THEREWITH. BY ACCEPTING THIS REPORT, THE RECIPIENT AGREES TO BE BOUND BY THE FOREGOING LIMITATIONS.

Contact

H. C. Kwan – Head of Research	kwan.hc@hooraysec.com.hk	(852) 2159 – 4506
Yanny Chu – Research Assistant	yanny.chu@hooraysec.com.hk	(852) 2159 – 4505
Research Department	research@hooraysec.com.hk	(852) 2159 – 4500

Hooray Securities Limited
1/F
Guangdong Investment Tower
148 Connaught Road Central
Sheung Wan, Hong Kong

Main：	(852) 2159 – 4500
Customer Services：	(852) 2159 – 4515
Dealing Hotline：	(852) 2159 – 4511
Facsimile ：	(852) 2110 – 4044