CRYPTO REVIEW

SPECIAL COLUMN

Three Bitcoin Valuation Methods

– A Literature Review

Robin Xie

COVER ARTICLE

KEY PERSPECTIVES TO UNDERSTAND DEFI

Chuanwei David Zou

INDUSTRIAL INSIGHT

Digital Assets and Digital Finance (Part II)

Qian Yao

Blockchain Solution for Loyalty Programs

Wai-ip Lam, Wai-man Yao, Kam-mau Kuo

GOSS
Institute of Research

CityU College of Business
香港城市大學
City University of Hong Kong

B2
B2 FinTech
中企信學院

CRYPTO REVIEW

CONTENTS

A MESSAGE FROM THE EDITORS:

The increasing price volatility of cryptocurrency markets recently has aroused heated discussions both inside and outside the crypto community, drawing scathing criticism especially from many who have doubts about cryptocurrency. All those who are concerned about digital currencies are now looking for an answer to this wave of violent market fluctuations: What is the main cause of the shock? Is it a human factor or a normal reaction of the market? Perhaps currently any evaluation system would find it difficult to provide a satisfactory answer. Whether the new object has vitality can always be proved by the conflict between traditional and non-traditional forces.

It only took less than six months for the Bitcoin price to rise from around USD30,000 to over USD60,000. Previously, it took nearly two years for its price to increase from USD10,000 to USD30,000. One can only presume that there were many speculative factors behind the recent boost. One of these factors could be the strong speculative demand in the market, causing the trading volume of derivatives to exceed the spot trading volume. In April of this year, amidst the sudden rise in the enthusiasm for cryptocurrency, the annualized average value of the premium between the Bitcoin futures market and the spot price rose to 50%. This meant that investors could lock in huge profits through simple convergent transactions.

The particularity of Bitcoin, as a unique digital currency (the market used to call it virtual currency), lies in its emergence and development, as opposed to fiat currency. It has certain attributes of fiat money, but the mechanism, especially the logic of these two, is totally different.

The core behind Bitcoin is "decentralization" and "consensus", which are the embodiment of natural rights. As a result, the rights and interests of currency holders can be fully respected. In this sense, Bitcoin followers must be people with firmbeliefs. The value of Bitcoin therefore will fluctuate in response to changes in market conditions, but it will never return to zero.

Meanwhile, based on the continuous development and innovation of cryptocurrency and blockchain technology, application scenarios are constantly being renewed, colliding with business models in traditional industries from time to time. For example, the idea of "decentralization" has led to the rapid development and practical application of DeFi technology. Similarly, the emergence of non-fungible tokens (NFTs) has also exemplified the vitality of the idea of cryptocurrency and its internal logic.

Around this theme, in our latest issue, we are presenting four articles, all focusing on the development of cryptocurrency and blockchain, but with different perspectives.

- Dr. Chuanwei David Zou, Chief Economist of Wanxiang Blockchain, will introduce some key perspectives to understand DeFi.

- Dr. Qian Yao, the Head of Technology Supervision Bureau of the China Securities Regulatory, will continue his discussions on digital assets and digital finance.

- Robin Xie, from iSunOne will provide a review of three Bitcoin valuation methods.

- Lam, Yao and Kuo from Hierodigit, will explore blockchain solutions for loyalty programs.

We hope that these insights will provide our readers with an innovative angle observing and understanding trends of this controversial cryptocurrency market. Additionally, these insights may help readers to judge for themselves the application prospects of the rapidly developing cryptographic digital technology based on blockchain technology.

Cryptor Review Editorial Board

KEY PERSPECTIVES TO UNDERSTAND DEFI

Chuanwei David Zou,
Chief Economist of Wanxiang Blockchain

How will the DeFi ecosystem evolve? What logic will the evolution follow? In addition to the skill of writing smart contracts, what other tools should DeFi developers master? This article answers these questions from eight key perspectives:

1. Financial functions;
2. Discrete-time finance;
3. Trustless environment;
4. Oracles and information;
5. Liquidity;
6. Arbitrage;
7. Incentives;
8. Risks and interconnections.

1. Financial Functions
Some researchers refer to mainstream financial institutions to understand DeFi, for example, what should be the form of banks, securities firms, and insurance companies in the DeFi field.

This analogy is actually not precise enough, because DeFi is built according to financial function modules. This involves the relationship between financial institutions and financial functions.

Financial development has two main lines that are entwined and rising like double-stranded DNA. One is financial function and the other is financial institution. Zvi Bodie and Robert Merton put forward six basic financial functions. They believe that financial functions are more stable than financial institutions, and the form of financial institutions depends on the financial functions they perform. Their insights also apply to DeFi (Table 1).

DeFi projects have very good assemblability. Multiple DeFi projects can be assembled together to achieve complex and diverse financial functions, which can be close to mainstream banks, securities firms, and insurance companies.

Financial function	DeFi field
Payment and settlement	Stablecoins
Resource integration and equity segmentation	Staking and liquidity tokens
Resource transfer across time and space	DEX (including automatic market makeror AMM) and DeFi lending
Risk management	DeFi insurance and derivatives
Information provider	Oracles
Incentive solution	Token governance

Table 1: DeFi and financial function modules

2. Discrete-time Finance

Mainstream finance is continuous-time finance, and the unit of time is generally hours, days, weeks, months, quarters, and years. DeFi is discrete-time finance, and the unit of time is the update frequency of the public blockchain - block time.

Discrete time and TPS limitations have a comprehensive and profound impact on DeFi. First, the amount of DeFi activities is naturally restricted by the physical properties of the public blockchain. Second, the efficiency of information synchronization and arbitrage are affected on and off the blockchain. Third, the efficiency of price discovery and risk clearance are also affected.

Continuous-time finance is easier to analyze because it can use mathematical tools such as calculus. The analysis method of discrete-time finance is:
Discrete-time finance = approximation of continuous-time finance + the influence of public blockchain TPS and latency

In discrete-time finance, the time value of money still applies. Although block time is a random variable, the interest theory of mainstream finance can still be introduced into DeFi. Basic concepts and tools such as present value, future value, discount factor, simple interest, compound interest and non-arbitrage pricing are applicable to DeFi.

3. Trustless Environment

No matter what role DeFi participants assume, they are essentially addresses in the public blockchain. The public blockchain offers a trustless environment. Addresses are essentially anonymous, identity-less and reputation-less.

The trustless environment is the foundation of DeFi's openness and permissionlessness. But in a trustless environment, enforcement of addresses' obligations in financial contracts relies on over-collateralization and staking, rather than their creditworthiness. How to understand over-collateralization and staking?

First, over-collateralization and staking are important channels for public blockchains to capture value from DeFi. Without this mechanism, value interaction between the public blockchain and DeFi may be ineffective.

Second, over-collateralization locks in liquidity, which is equivalent to converting the credit risk of addresses into the liquidity risk of the collateral. In DeFi and mainstream finance, risks do not disappear, they just change a form.

Third, because of over-collateralization, the risk pricing efficiency of DeFi lending is very low. The DeFi lending rate does not include a risk premium for the borrower and has nothing to do with the creditworthiness of the borrower. Fourth, in MakerDAO, over-collateralization guarantees that Dai (essentially CDP liabilities) from different Collateralized Debt Positions (CDPs) have the same intrinsic value. No matter who initiates the CDP, and no matter what kind of collateral the CDP adopts, as long as the over-collateralization rules are followed, Dai is equivalent to each other.

Fifth, staking is a commitment mechanism for stakeholders. This has been fully reflected in the PoS consensus algorithm to solve the Nothing-at-stake problem.

Financial activities are inseparable from trust. Trust can reduce the uncertainty about the future and is essential for reducing the transaction costs of financial activities. This is true for both mainstream finance and DeFi. Blockchain is trustless, essentially transforming trust in people and institutions into trust in algorithms and smart contracts.

4. Oracles and Information

There are two consensus mechanisms regarding blockchain. The first is consensus algorithms such as PoW and PoS, which form a consensus on token status and token transactions. The second is Oracle, which form a consensus on the off-chain information and read the information into the blockchain. Oracle is the basis for information synchronization and arbitrage on and off the

chain. Whichever consensus mechanism applies, it means entropy reduction (that is, elimination of chaos), and energy input is required. The goal of Oracle design is to minimize the ratio of error to cost.

There are many design schemes for Oracle, but they can be roughly divided into two types. The first type of Oracle is based on reputation and voting, represented by ChainLink. The second type of Oracle is based on trading and arbitrage, and the arbitrage mechanism allows Oracle quotations to converge to the market price.

From the perspective of communication engineering, no matter what form it takes, DeFi Oracle sample the continuous off-chain signals at discrete points in time, and then read the discrete signals into the public blockchain (Figure 1).
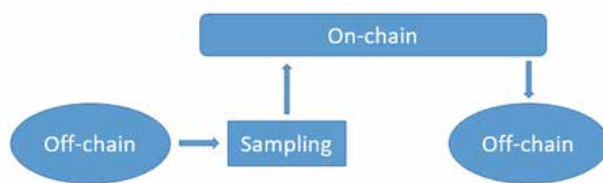

Figure 1: Sampling process of Oracle

5. Liquidity
Liquidity reflects the possibility of selling assets at a reasonable price within a reasonable time. Obviously, the liquidity of transactions on the blockchain is restricted by its TPS. Liquidity is the product of interaction between buyers and sellers. The higher the confidence of both parties, the greater the liquidity. For most commodities, rising demand will stimulate supply by pushing up prices. However, because liquidity is related to the confidence of buyers and sellers, the supply may be the least when it is most needed.

For investors, liquidity is a commitment mechanism that provides confidence about whether a transaction can be completed and at what price. There are two main types of

commitment mechanisms. The first type is reputation-based commitments, such as market makers in the limit order book. The second type is algorithm-based commitments, such as automatic market makers. Under the same conditions, products that can provide better liquidity are more attractive to DeFi investors.

Liquidity has agglomeration effect. For multiple liquidity pools, their combined liquidity will exceed the sum of their respective liquidity. This is the same as the risk diversification effect, which is the basic law of finance - the risk of the a portfolio is less than the sum of its components.

6. Arbitrage
There are many driving factors for financial development, such as regulation and technology, but the fundamental driving force is arbitrage. When any financial market or

product is first launched, because the pricing mechanism is not sound, there will always be arbitrage opportunities and will attract arbitrageurs. Driven by arbitrageurs, the pricing mechanism will be corrected, and the financial market and products will gradually be improved. With such a cycle, financial development can continue to move forward.

Arbitrage converges prices, but it takes time and cost. For any Oracle based on trading and arbitrage, once the Oracle's quotation deviates from the market price, it means an arbitrage opportunity, but the arbitrageur needs to pay a cost to execute the arbitrage strategy. Therefore, arbitrageurs will carefully weigh the arbitrage benefits and costs, and will execute the arbitrage strategy only when the Oracle quotation deviates from the market price by a large enough extent. The execution of the arbitrage strategy will correct the deviation of the Oracle quotation from the market price until the arbitrage strategy is no longer economically attractive. The higher the arbitrage efficiency, the smaller the Oracle quotation deviation.

Arbitrage is derived from the basic needs of human nature and is a universally applicable mechanism design. Arbitrage only requires people to be rational, to seek advantages and avoid disadvantages, and to maximize their own interests, without knowing whether they are good or bad. In the decentralized environment of DeFi, the incentive and coordination role of arbitrage is more important. For example, MakerDAO collateral liquidation is based on arbitrage design.

7. Incentives

Incentive mechanism design should make DeFi an infinite game, instead of a finite game. Community self-organization and self-upgrading are the keys to the evolution of DeFi. Community members should be able to get their own benefits from DeFi. In other words, in the design of DeFi incentive mechanism, one cannot expect a certain type of participant to always subsidizing others. This problem is common in the blockchain field. For example, if the block reward is not considered, or the block reward drops to a very low level, can the transaction fees received by PoW miners make up for the mining cost? For another example, can the user's payment for an Oracle to make up for the cost of the Oracle?

The above issues all involve the provision and financing of public goods in a decentralized environment. To solve these problems, we must refer to the economic theory of public goods.

8. Risks and Interconnections

The core of DeFi is making profits via taking risks, which mainly includes market risk, liquidity risk, technical risk and credit risk. Market risk comes from fluctuations in the price of crypto assets. In DeFi, the widespread application of over-collateralization and staking converts the credit risk of addresses into the liquidity risk of the collateral. The technical risks of DeFi are much more prominent than those of mainstream finance, which may come from loopholes in smart contracts or from the limitations of public blockchain TPS. Risks can

be transferred, shared, hedged, converted and diversified, but they will never disappear.

DeFi projects are interconnected and combined through channels such as information, funds, and risks, which helps to develop the DeFi ecosystem in a bottom-up approach, but lacks an overall plan and accumulates risks. In particular, the more basic projects in the DeFi ecosystem, although they have "moat", the more likely they are to introduce a single point of failure risk.

Many researchers sort out the DeFi ecosystem according to different business types, but it is even more necessary to draw an overall "risk map" for the DeFi ecosystem. In the future, before the DeFi project goes live, in addition to smart contract audits, financial risk audits should also be done. ■

Dr. Chuanwei David Zou

Chief Economist of Wanxiang Blockchain

Previously, Dr. Zou held various positions in China Investment Corporation (CIC) and Nanhu Finance Corporation from 2006 to 2015. Dr. Zou received Ph.D. in Economics from Tsinghua University, Mid-Career MPA from Harvard University, M.A. in economics and B.S. in Statistics from Peking University. In 2015, Dr. Zou was a winner of the 1st Sun Yefang Prize for Financial Innovation (China's top prize for economists) and the 5th China Soft Science Prize for his research on fintech. In 2013, 2014 and 2017, his books were selected into the lists of "financial books of the year" by China Business Network. In 2019, Dr. Zou was nominated as one of the "top 10 institutional economists of the year" by China Business Network.

DIGITAL ASSETS AND DIGITAL FINANCE (PART II)

Qian Yao,
Head of the Technology Supervision Bureau of
*the China Securities Regulatory Commission,*
Former Head of China's Central Bank Digital Currency Initiative

* This paper is the second half of the speech given by Dr. Qian Yao at The 5th Global Blockchain Summit, 2019. It is translated and published under the authorization of Dr. Qian Yao. The first half of the speech was published in Crypto Review Vol.2.

III. Self-financing, Inclusive and Sharing

The production and circulation of digital assets are very different from the existing financial system. The deeper meaning of asset digitization is that data is native, penetrable and traceable, and that data can be self-validated and third-party validated, thus deriving the concept of self-financing. There are three typical characteristics of self-financing: first, users control their digital identities independently; secondly, users control their digital assets independently and take the responsibility of transactions as well; thirdly, users make point-to-point transactions among themselves, being independent of third-party intermediaries. Digital finance can be both self-disciplined and imposed-disciplined. Although digital finance is a fintech system built on the full disclosure of the underlying information, it provides high degree of personal privacy protection. Users produce data, create digital assets and add various elements to the innovative digital financial services. Take asset securitization as an example. SMEs in China have been suffering from financing difficulties for a long time. This problem has attracted much attention. In the process of financing, SMEs face the problems such as complex counterparties, scattered information sources, complicated information of the underlying assets and disclosure difficulties, all preventing SMEs from using asset securitization as an effective financing
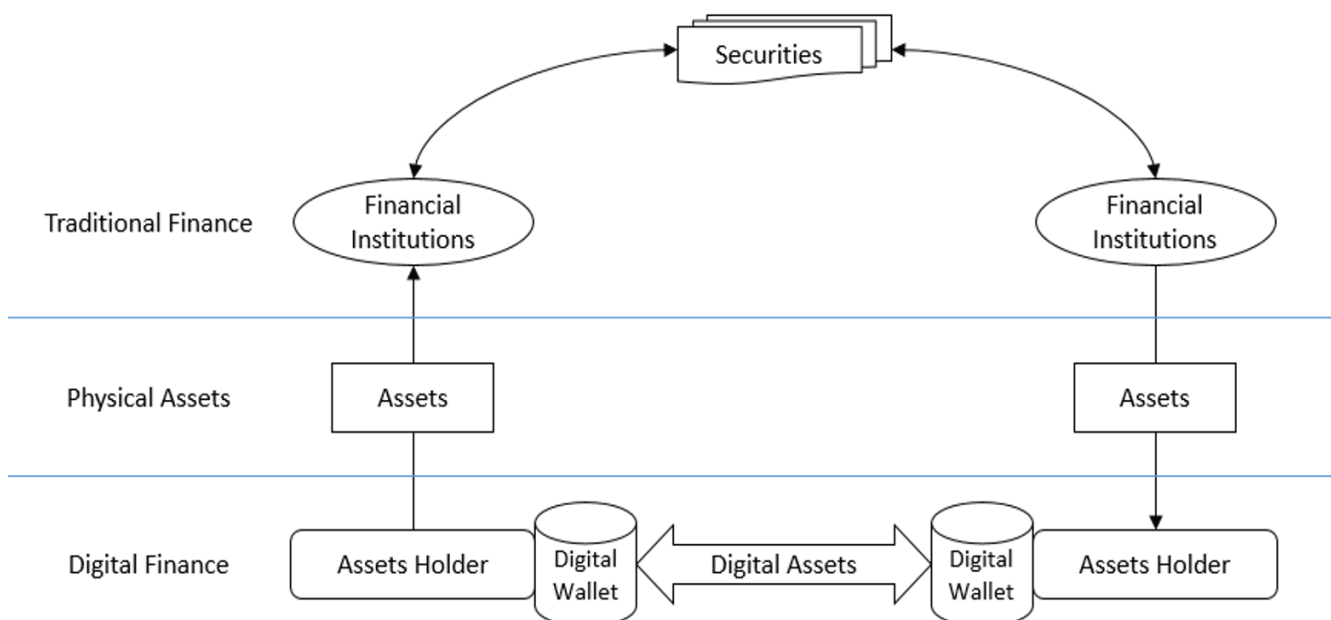
tool. How can SMEs get equal access to information and obtain independent financing capabilities? An effective solution is by distributed ledger technology and distributed file systems. By synchronizing all the native information of the underlying assets on the chain, using public-private cryptography key to realize the ownership and the transfer of assets, getting access through information operation providers and continuously disclosing the underlying transaction information. Digital assets are thus created.

Digitalization of Assets makes traditional assets fungible with a high degree of liquidity autonomy, which greatly improves the efficiency and authenticity of supply chain financial businesses. It also establishes a dynamic, complete, true and credible information disclosure mechanism for investors. This fundamentally solves the multi-layered information penetration problem of SMEs. SMEs can have a say in financing and carry out independent financing activities, without relying on enterprise credit scoring. On the other hand, financial institutions can obtain SMEs' underlying assets information directly from trusted distributed ledger technology, instead of relying on enterprise credit scoring.

This is the practical value and meaning of digitization of assets and self-financing model, which solves the financing problem of the disadvantaged groups in traditional finance systems. Financing system better serves the enterprises becoming more inclusive and sharing. With the support of modern technology, the new financing system is more secure than traditional financing. In regulatory aspects, it is also more convenient and efficient. Self-financing fills the gaps in existing financial services flexibly.

IV. Financial Integration, Free and Open

The development of digital finance will blur the boundary between on-site and off-site market. In a sense, one of the main reasons leading to the market stratification of on-site and off-site in the present is the lack of technology credibility. Traditional technology cannot solve the trust problem of financial transactions. Hence, many transactions need to be carried out in the organized on-site market. Economies of scale is certainly another reason. The legal guarantees recognized by the state solve the credibility problem. With the development of modern digital finance technology such as blockchain, technology has become a supplementary means of legal credit enhancement. With the empowerment of trust technology, data and value, physical and logical parts, can be integrated as digital assets. Data is value and value is data, therefore the circulation of data is the circulation of value. With the trust technology, any assets can be digitized, circulated and activated, without relying completely on the traditional legal credit enhancement. As a result, there is no more boundary between on-site and off-site markets.

Digital finance may reconstruct the financial operation methods, service models and even the entire ecosystem. It is concise and efficient, free and open, transcending the boundaries of nations, time and space. It respects the autonomy and wills of market participants. Driven by technology, it does not need to rely on traditional financial intermediaries to make assets circulate and what is more, it retains the complete native information.

Large amounts of non-standard assets, such as warehouse receipts, intellectual property rights, contracts, etc., will regenerate financial "vitality", circulate with low cost and high efficiency, and create significant economic value. What is more revolutionary is that digitization of assets will start a revolution in retail finance. Just as the emergence of Internet incubating retail giants like Ali, the awakening of retail financial market will make more profound changes in financial world.

V. New Form of Currency, with Independent Control

Digital assets call for digital currencies. The private and the public sectors are working hard on it.

Virtual currencies are correcting the

fundamental defect of the lack of backing assets. From Bitcoin (lack of backing assets) to various stable coins (backed by fiat currency or tied to an algorithm), to the recent JPM Coin and Facebook Libra, the compliance and value volatility problem of virtual currencies are expected to be solved. It seems that the value of virtual currencies is backed by the central bank currency, but in fact, it is the process of "de-virtualizing".

Therefore, the concepts of cryptocurrencies and virtual currencies need to be reviewed. Cryptocurrencies are no longer necessarily virtual currencies. It is of great significance to distinguish between cryptocurrencies and virtual currencies.

Cryptocurrencies may have already become a real currency, but at the currency level, it is not necessarily M0, it may be a higher level of currency than bank deposits, say Mn. Compared with M0, the digitization of higher-level currencies such as M1, M2 ... and Mn, gives more room for imagination.

The central bank has always been considered unsuitable for the role as a digital currency supplier. In addition to the concern of narrowing banking system, the main concern is that the central bank will face great service pressure and costs when issuing digital currency to C (to retail clients, that is, the public). This is one of the major difficulties faced by countries in the developing of fiat digital currencies. Currently, digital currency trials conducted by various central banks worldwide are all still in the application scenario to B (to institutions), such as the project Jasper of the Bank of Canada, the project Ubin of the Singapore Monetary Authority, and the project Stella of the European Central Bank and the Central Bank of Japan.

According to the views of IMF economists Tobias Adrian, Tommaso Mancini-Griffoli and others, for Alipay and WeChat Pay, after depositing 100% provisions to the central bank, clients' transactions is backed by the central bank liabilities. It essentially makes Alipay and WeChat Pay played the role as central bank digital currency. If this is the case, then China has long been the world's first big country to realize the digitalization of fiat currency. Of course, this is only the version 1.0. It should be noted that the 100% reserve assets proposed by Facebook's Libra white paper and the 100% provisions people usually referred to are not the same concept. The former puts the reserve assets in a third-party custodian, while the latter deposits all the funds in the central bank.

Technically, the 100% provisions mode means that the full life cycle of digital currency, issuance, circulation, recovery, and destruction must be attached to the traditional account system, especially the cross-institution central bank digital currency circulation. The central bank has to update the digital currency account system, and also has to deal with clearing and settlement between corresponding provisions accounts. This not only increases the pressure and complexity of the central bank's central system, but also makes it difficult to achieve the "account loosely coupled" requirement. Under such condition, it is hard to develop self-financing innovation. Also, the potential of cross-border payments would greatly shrink. In comparison, the Central Bank Crypto-Currencies (CBCC) allows customers to manage their own currency, instead of entrusting the currency to a third party. It also goes pass Swift and breaks a new ground for cross-border payment business. It seems to be the hottest focus at present.

Mark Carney, Governor of the Bank of England, believes that Libra-like digital currencies will be a better choice for global reserve currencies. My understanding is that digital currency is not just the digitization of fiat currency, as digital assets are not just as simple as the digitization of assets. The future digital currency needs to make up the shortcomings of the existing currency system, surpass the US dollar, and upgrade to a new level.

VI. Regulatory Technology in Response to New Ideas
The various characteristics of digital assets mentioned above, diverse in attributes,

integrated and innovative, technology-driven, free and open, have brought new propositions and challenges to financial regulation. The traditional regulatory system that monitors and manages financial institutions and their accounts by license mechanism needs to be reexamined.

First, the license management for institutional access should be transformed into the authority management for user access.

In the self-financing mode, users must pass the identity authentication and verification of relevant certification authorities. The business process must be isolated from the identity authentication. Identity and content privacy protection is achieved by cryptographic primitives and solutions. However, the regulatory department has the right to carry out penetrating supervision. On this basis, regulatory authorities of various countries collect their residents' digital identities and demarcate digital jurisdictions accordingly. Within their own digital jurisdictions, regulatory authorities should set up various types of business participation permissions based on KYC, AML / ATF and other financial regulatory policies for their residents.

Financial operations and transactions between residents and non-residents from different jurisdictions are regulated by regulatory authorities in accordance with their respective capital account and cross-border financial regulatory opening up policies. Such design could not only ensure the free and open self-financing business, but also comply with regulatory requirements of different countries. Take Calibra, Facebook's regulated financial subsidiary, as an example. Its first product is the Libra digital wallet. Facebook connects social users' identity information with Libra users' blockchain addresses through the Calibra wallet. In the self-financing mode, the wallet replaces the licensed financial institutions and becomes the object of supervision. The supervision strategy can be implemented according to the specific requirements of the jurisdiction, meeting both the requirements of user privacy

protection and regulatory compliance.
Secondly, smart contracts should be verified and become part of business approval.

In the self-financing mode, traditional financial services will be logically encoded into smart contracts that are transparent, trustworthy, automatically executed, and enforced. Smart contracts carry various financial services and even one smart contract represents one format of financial business state. In a sense, controlling smart contracts means controlling the future self-financing business. On the basis of safe and efficient user identity authentication and authority management, smart contracts must be verified by relevant departments before going on chain. The program should be judged whether it can run in accordance with the regulatory policy expectations. When necessary, the authorities can prevent non-compliant smart contracts going on chain, or stop residents' authority to execute such smart contracts. Meanwhile, the authorities can set up regulatory intervention mechanisms to suspend or terminate execution.

In addition, setting parameters of smart contracts is also a regulatory means, just like using indicators such as statutory reserve ratio and capital adequacy ratio to prevent and manage banking risks. The regulatory authorities can control the business scale and risk exposure for self-financing business by adjusting or intervening parameters of smart contracts. It is a trend to adopt regulatory technology to respond to finance technology. The regulatory authorities of various countries have mixed concerns in view of new digital assets. On the one hand, the authorities appreciate the innovative significance, but on the other hand, they are worried about the uncontrollability. In essence, under the means of digital technology, digital assets can not only be controlled, but also be supervised in a more precise manner. In other words, the authorities should concern more about controlling too tight instead of worrying about the uncontrollability of the future.

Digital finance, characterized by the digitization

of assets, will follow the new development concepts of "innovation, coordination, green, openness, and sharing". Through the innovative application of modern science and technology, it is possible to revitalize existing assets at a higher level and activate edge assets in various fields, and deepen the structural reforms on the financial supply and promote the high-quality development of the real economy with prospering future. ■

Qian Yao

Dr. Qian Yao is the Head of the Technology Supervision Bureau of the China Securities Regulatory Commission, former Head of China's Central Bank Digital Currency Initiative, former Chief Executive Officer of China Securities Depository and Clearing Corporation Limited (CSDC). He is also serving as the Research Fellow at the Financial Research Centre of the Counselors' Office of the State Council of the People's Republic of China and the Secretary General of China Financial Standardization Technical Committee.

Before joining CSDC, he served consecutive positions as the Deputy Director General and Counsel of the Technology Department of the People's Bank of China (PBoC), Director General of Institute of Digital Money of PBoC, and Deputy Director General of PBoC Credit Reference Centre.

He has published around 150 papers and 7 books and holds more than 100 patents. He has been awarded provincial and ministerial first prizes for his outstanding contribution in promoting new technology development and application in the banking sector.

YAO Qian holds a Doctor of Engineering degree. He is a professorate senior engineer and a Ph.D. supervisor.

BLOCKCHAIN SOLUTION FOR LOYALTY PROGRAMS

Wai-ip Lam, Wai-man Yao, Kam-mau Kuo,
Hieroglyph Digital Technology Limited

Introduction

For a long time, companies have used loyalty programs as a marketing strategy to retain existing customers and encourage repeat purchases by offering points, discounts and coupons. However, traditional loyalty programs present challenges for both companies and customers. Many loyalty programs suffer high cost, low redemption rate and low customer satisfaction rate. Blockchain, as a distributed ledger technology (DLT) which based on a peer-to-peer (P2P) topology has the potential to revolutionize loyalty programs by eliminating some of the inefficiencies of traditional programs and provide better customer experience.

History of Loyalty Programs

Some believe that "premium marketing" in the late 18th century was one of the earliest loyalty programs. Since 1793, American retailers began to give customers copper tokens with purchases that could be collected and exchanged for items later [1]. This kind of rewards was very popular throughout the 19th century.

In the late 19th century, a less expensive medium, trading stamps were used to replace the copper token. The first trading stamps were introduced in 1891 at Schuster's Department Store, Wisconsin [2]. At the beginning, trading stamps were redeemed at the issuer's store. After that, there emerged third-party providers of trading stamps for various companies, such as Sperry and Hutchinson Company which was the first providers started in 1896, S&H Green Stamps which founded in 1897 and became popular from the 1930s to the 1980s. Merchants paid a third-party trading stamp company for the stamps and customers attached stamps to the booklet and took the booklet to a trading stamp company redemption center to exchange for items. By 1957, there were approximately 200 trading stamp companies in operation in the United State.

In the early 20th century, trading stamps still was the most popular method of rewards. Meanwhile, individual brands and retailers began to introduce their own ways of engaging customers, with "box tops" as one of the original brand specific programs [2]. Box tops were coupons that were printed directly onto product packages and could be redeemed for premiums later. Betty Crocker introduced their box top program in 1929, which lasted until 2006 and was one of the longest running loyalty programs.

In the late 1900s, modern loyalty programs started to sweep across the market. American Airlines launched their frequent flyer program in 1981, which is the first full-scale loyalty program of the modern era. Within a few years, many other travel industry companies launched similar programs.

Card-based loyalty programs gained popularity since the 1990s. In recent years, companies have introduced loyalty apps in replace of loyalty cards as part of their loyalty programs. These apps are downloaded onto a customer's mobile phone. With the rise of information technology, it is now possible for anyone to start a loyalty program app for their store or site.

Issues of Traditional Loyalty Programs

Loyalty programs help companies on growing and retaining existing customers through incentives. However, traditional loyalty programs present challenges for both companies and customers. First, companies are concerned with estimating liabilities related to loyalty programs which may be recorded on the company's financial statements [3]. The cost of operating a loyalty program may be high. According to a report from LoyaltyOne, more than 71% companies invests 2% - 4% of total revenues for loyalty and CRM to activate customers and leverage the data asset to create personalized offers and extensions [4].

Companies are also concerned with the personalization, which has long been considered as an important part of the customer experience. Only 22% of the customers are satisfied with the level of personalization at The Loyalty Report 2019 form Bond [5].

In addition, there are other shortcomings such as restrictions and rules on redemption, limited reward choices, expiration, losing track of accumulation of rewards points and complex registration process. Consumers also tend to wait longer than expected to earn enough points for their desired products. This results in customers leaving the program earlier than expected with poor customer experience and low customer satisfaction rate. According to Bond, only 37% of hotel loyalty members are satisfied with their programs. Meanwhile, airlines is slightly better at 42%, Credit Cards is at 46% and Movie is the highest at 50%. In this year's survey, 44% of members indicate they are very satisfied with the program, down from 47% in 2018 [5].

Benefits by Adopting Blockchain Loyalty

Blockchain, as a distributed ledger technology (DLT) which based on a peer-to-peer (P2P) topology has the potential to revolutionize loyalty programs by eliminating some of the inefficiencies of traditional programs and provide better customer experience.

First, transactions on a blockchain ledger are cryptographically secured, immutable and time-stamped, hence increasing transparency and making everything trackable. A blockchain token transaction cannot be revoked and is recorded publicly on the blockchain. The token is stored in a digital wallet and can be redeemed at any time. This is both a win for consumers, who no longer have to worry about their points being expired and a win for companies, who will gain greater customer loyalty by providing a better and more transparent shopping experience.

According to the KPMG survey, 82 percent of consumers are willing to use tokens as part of membership in an existing loyalty program, and 81 percent would trust the use of tokens more readily if they are already a part of a company's loyalty program [6]. Program enhancements driven by tokenization could further cement a brand's engagement with loyalty members.

Moreover, blockchain can decrease the cost of setting up and operating a loyalty program. For example, a blockchain-based partnership between two companies can be set up to enable exchanges of tokens by the customers with no centralized management. Smart contracts can be used to enforce contract terms, automate processes and reduce organizational costs.

Loyyal is one of the earliest developers of blockchain-based loyalty and rewards solutions. It started a pilot program with airline Emirates Group in 2018 [7]. Emirates has 120 partners earning or redeeming mileage points. Previously, it takes Emirates 30 to 60 days to reconcile the partner transactions and complete the redemption for fiat currency from the partners. Through the pilot program, Emirates were able to reduce that relationship cost by 80% by using smart contract. The blockchain based solutions provides real time visibility into partner transactions as well as increased operation efficiency.

Furthermore, blockchain enables a frictionless system and provides more flexibility in customizing tokens. Through a trustless,

decentralized technology solution, loyalty provider can build a loyalty system with their partners, deciding the rules of how the blockchain tokens can be used by customers. On the other hand, from a consumer's perspective, his or her ability to access and manage the token is practically frictionless. Singapore Airlines is a good example. In July of 2018, Singapore Airlines officially launched its blockchain-based loyalty program for frequent customers. Their frequent flyer program KrisFlyer is reinvented as KrisPay, a digital wallet developed in partnership with KPMG and Microsoft, allowing Singapore Airlines customers to turn travel miles into units of payment, which can be used with partner merchants in Singapore [8]. The press release announcing KrisPay describes it as "the world's first blockchain-based airline loyalty digital wallet." At launch, KrisPay was partnered with 18 merchants through categories ranging from beauty and food services to gas and retail.

In October 2020, Singapore Airlines announced the launch of its newest payment, lifestyle, and rewards app, Kris+, an extension of its existing blockchain wallet KrisPay [9]. Kris+ has more than 150 partners with over 650 outlets in Singapore to provide exclusive deals for the Airline's customers. Kris+ has updated its interface and user experience, now allowing personalized offers to its customers based on location and interest. Travelers can earn miles from everyday expenditure, or vice versa, miles can be used as a means of payment. The app also offers customers discounts on dining, entertainment, and retail.

A Blockchain-based Solution
Here we will briefly introduce a blockchain-based and data-driven solution for loyalty points programs, called Points Self-management and Service Platform (PSSP). PSSP aims to use blockchain technology to reduce the costs of setting up and operating a loyalty program for both large and small companies, improve the program execution efficiencies, customer experience and customer satisfactions.

PSSP is consisted of blockchain wallet, reward protocol, loyalty ecosystem and data analysis services. Through PSSP, companies create tokens that function as loyalty points and reward them to their customers. Each customer owns a PSSP digital wallet (blockchain wallet app) to accumulate tokens. Through the PSSP digital wallet, customers can flexibly manage their tokens by themselves, including redeeming rewards at any time, transferring token, making payment by using token in stores.

PSSP also offers the potential to connect different loyalty programs across brands, creating a consolidated loyalty network. Tokenization of loyalty points transforms points into digital assets, which can be exchanged among different loyalty programs.

Besides points program, PSSP also provides data analysis services. PSSP can capture and analyze customer data for segmentation and profiling, and deliver personalized offers to customers. In the longer run, companies can launch bundled offerings and joint campaigns based on the segments identified. Not only does this extend the reach to a larger customer base, it also helps cut down advertising and branding expenses, increase sales, and improve brand recall and customer stickiness.

Conclusion
The development of a loyalty program has been undergoing for several years. Besides the increasing number of its applications, the unsolved inefficiencies of current programs are still causing the lack of users' activity [10].

To conclude, we believe that the best option for loyalty marketing could be using the state-of-the-art technology to make the program efficient, fast, and secure in the long term. In this sense, using blockchain technology is highly encouraged for creating a network of partnerships where consumers can use and trade their tokens, where a business can also gain access to an ecosystem of potential customers. ■

REFERENCES

1. Loyalty marketing
https://en.wikipedia.org/wiki/Loyalty_marketing#History

2. Trading stamp
https://en.wikipedia.org/wiki/Trading_stamp

A History of Loyalty Programs, and How They Have Changed
https://blog.smile.io/a-history-of-loyalty-programs/

Improving Customer Retention And Loyalty Programs With Blockchain
Apr 29, 2020,07:00am EDT|1,819 views
https://www.forbes.com/sites/forbestechcouncil/2020/04/29/improving-customer-retention-and-loyalty-programs-with-blockchain/?sh=547fc30bb27f

3. An Inside Look at Loyalty Program Benchmarks for the Hospitality Industry
November 28, 2018
https://www.kyrosinsights.com/blog/2018/11/28/loyalty-program-benchmarks-hospitality

4. New Research Report: Global Customer Loyalty a $323B Endeavor
May 3, 2019
https://www.businesswire.com/news/home/20190503005033/en/New-Research-Report-Global-Customer-Loyalty-323B

5. The Loyalty Report 2019 from Bond
https://info.bondbrandloyalty.com/loyalty-report-2019

6. KPMG Study Finds Digital Tokens Are Transforming the Way Consumers Interact with Each Other and Businesses
September 25, 2019
https://home.kpmg/us/en/home/media/press-releases/2019/09/kpmg-study-finds-digital-tokens-are-transforming-the-way-consumers-interact-with-each-other-and-businesses.html

7.Bringing smart contracts to consumer loyalty rewards programs
By Leo Jakobson / September 18, 2019
https://modernconsensus.com/technology/bringing-smart-contracts-to-consumer-loyalty-rewards-programs/

8. KrisFlyer Launches Innovative Miles-Based Digital Wallet, KrisPay
24 July 2018
https://www.singaporeair.com/en_UK/sg/media-centre/press-release/article/?q=en_UK/2018/July-September/ne2518-180724

9.Singapore Airlines Customers Get Even More Options With All-New Kris+ App
13 October 2020
https://www.singaporeair.com/en_UK/sg/media-centre/press-release/article/?q=en_UK/2020/October-December/ne1620-201013

Singapore Airlines rolls out Kris+ lifestyle app in India
3 Feb 2021 by Business Traveller India
https://www.businesstraveller.com/business-travel/2021/02/03/singapore-airlines-rolls-out-kris-lifestyle-app-in-india/

Kris+
https://www.singaporeair.com/en_UK/sg/ppsclub-krisflyer/use-miles/krisplus/

10.Making blockchain real for customer loyalty rewards programs
https://www2.deloitte.com/us/en/pages/financial-services/articles/making-blockchain-real-customer-loyalty-rewards-programs.html
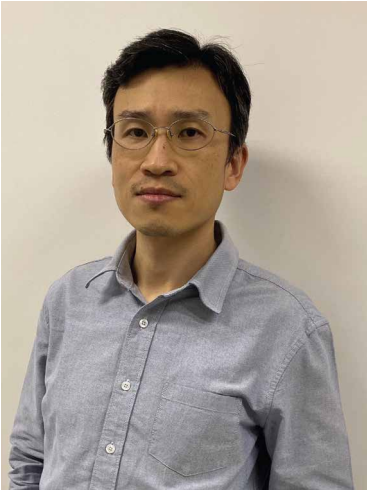
Wai-ip Lam
Senior Systems Architect
Hieroglyph Digital Technology Limited

Mr. Lam has over seventeen years of professional experience in Research & Development, and System Design. He was responsible for designing advanced modules in ERP systems, such as Distribution Resources Planning (DRP), Advanced Planning & Scheduling System (APS), Material Requirement Planning (MRP), Finite Scheduler etc. His expertise focuses on SCM and retail optimization. With his broad professional knowledge in these fields, he helped many clients design and review existing process flow and then customizes SCM software for client's long-term growth.
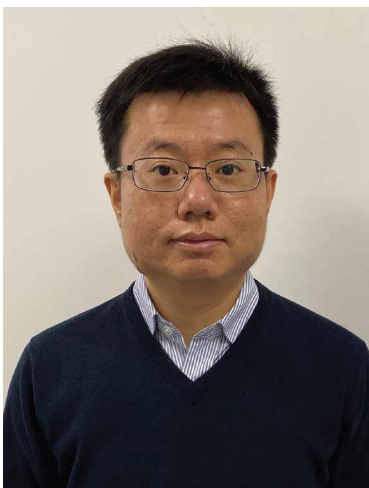

Kam-mau Kuo
Senior Systems Analyst
Hieroglyph Digital Technology Limited

Mr. Kuo has over fifteen years of professional experience in system design, software engineering and quality assurance.

He was responsible to design, implement and maintain the system framework. Besides, he interacted with customers, both onsite and offsite, gather requirements and data. He has helped Hong Kong listed companies and local enterprises to implement state-of-the-art enterprise software, such as e-Procurement System, ERP System, Supply Chain Management etc.

He contributed to technical team activities (design, modeling, prototyping, coding, testing, and documentation) in full-life cycle of products.

Wai-man Yao
Senior Systems Analyst
Hieroglyph Digital Technology Limited

Mr. Yao has over fifteen years of professional experience in project management, software engineering, software design, testing and quality assurance. He has been helping different Hong Kong listed companies and local enterprises to implement state-of-the-art enterprise solutions. He is familiar with Supply Chain Management System and e-Procurement System.

THREE BITCOIN VALUATION METHODS – A LITERATURE REVIEW

Robin Xie [i]
Chief Commercial Officer, iSunOne

"Bitcoin is dead" as pronounced 411 times by mainstream media.[ii] Why the disdain and disbelief? Perhaps it originates from bitcoin's famously hidden message on its genesis block, "chancellor on brink of second bailout for banks", when bitcoin was born as a decentralized peer-to-peer electronic cash system[iii] in Jan 2009 during the global financial crisis.[iv] Gradually, "what doesn't kill you, only makes you stronger". While central banks were busy printing fiat currencies out of thin air, bitcoin started its super bullish cycle since Oct 2020 with price quintuple in less than five months. In retrospect, "it is inevitable", as claimed by Elon Musk whose Tesla treasury buying up to 10% bitcoin with corporate cash[v], coinciding with mass institutional adoptions including PayPal[vi], Square[vii], Guggenheim[viii] , MassMutual[ix], NY Bank of Mellon[x], Fidelity[xi], JP Morgan Chase[xii], DBS Bank[xiii], BlackRock[xiv] etc. This article leads investors through the three bitcoin valuation methods utilized by "smart money".

"The bitcoin story is very easy; it is supply and demand. Bitcoin is digital gold , and it is better at being gold than gold." [xv] Bitcoin is a scarce digital asset that cannot be devalued like fiat currency, with a fixed supply of 21 million; ownership is preserved on a public, transparent, and decentralized ledger, as maintained by global network, advanced cryptography and market incentives.

The store of value theory states that a digital asset's value is a function of its ability to act as a store of monetary value for its investors and users. As an example of calculating the fair value of the price of bitcoin with store of value

Rank	Name	Symbol	Market Cap	Price	24h	7d	Price (30 days)
1	Gold	GOLD	$11.637 T	$1,832	0.90%	3.57%	
2	Apple	AAPL	$2.173 T	$130.21	0.53%	-0.95%	
3	Microsoft	MSFT	$1.901 T	$252.46	1.09%	0.11%	
4	Saudi Aramco	2222.SR	$1.901 T	$9.51	0.00%	0.71%	
5	Amazon	AMZN	$1.66 T	$3,291	-0.45%	-5.07%	
6	Alphabet (Google)	GOOG	$1.592 T	$2,398	0.73%	-0.47%	
7	Silver	SILVER	$1.507 T	$27.57	0.32%	6.06%	
8	Bitcoin	BTC	$1.071 T	$57,257	-3.04%	0.65%	
9	Facebook	FB	$904.73 B	$319.08	-0.29%	-1.85%	
10	Tencent	TCEHY	$752.08 B	$78.18	-0.23%	-1.86%	
11	Berkshire Hathaway	BRK-A	$664.98 B	$437,131	0.46%	5.97%	
12	Tesla	TSLA	$647.43 B	$672.08	1.29%	-5.27%	

(Figure 1: image courtesy of 8marketcap.com)

in mind, we could look at the price of gold and make the assumption that bitcoin could one day replace gold as the go-to store of value for investors. [xvi]

At a current gold price of around $1,832 per troy ounce, the total value of the world's gold bullion is around $11.6 trillion. Suppose bitcoin replaces gold as a popular store of value globally and its total network value rise to $11.6 trillion, knowing that the total supply of coins is capped at 21 million, the price of one BTC would end up being $552,380.

$11.6 trillion / 21 million BTC = $552,380 per one bitcoin (Figure 1)

Bitcoin's Price Dynamic: Stock to Flow Model
"As a thought experiment, imagine there was a base metal as scarce as gold, and one special, magical property: can be transported over a communications channel" - Satoshi Nakamoto[xvii]. Bitcoin is the first digital object with a fixed supply that cannot be copied, duplicated or forged, contributing to its unique mathematical value. The Bitcoin network has been generating uninterrupted blocks since day 1 - genesis block was generated on the 3rd, Jan, 2009 and the reward for mining it was 50 bitcoins. On every 210,000 generated blocks

there is an event called "halving" which cuts, in half, the reward value distributed to miners from that moment on. Since blocks are generated every 10 minutes, "halving events" take place every 35,000 hours: almost exactly every 4 years. Halving events continue to take place until the reward for miners reaches 0, as after the 33rd halving in year 2140. It will be the 21 millionths bitcoin to come into existence, after which point it will be impossible to create anymore, and after that bitcoin will become truly deflationary[xviii]. An anonymous hedge-fund manager in the name of "Plan B"[xix] applied Stock-to-Flow model to bitcoin price on a log scale, with an astonishing accuracy: (Figure 2)

The 'Stock-to-flow' is a number that shows how many years, at the current production rate, are required to achieve the current stock.

S2F ratio = Stock / Flow
While Stock = current reserve
Flow = current production

Bitcoin with a fixed supply on an immutable irreversible blockchain is associated with scarcity, the word linked with precious metal and monetary supply. Note for bitcoin as it halves every four years, the flow would decrease to 50% of its last value every four

(Figure 2: image courtesy of lookintobitcoin.com)

years, causing its S2F to double every four years, making it more scare in nature. The above figure is done with linear regression plotted on a log scale chart illuminating the mathematical relationship between past (dotted) and predicted (line) bitcoin price as a function of its S2F ratio, which increases every four year in the halving events due to the halving decrease in the production. For more in-depth analysis, readers are encouraged to pursue this article "modelling bitcoin with scarcity"[xx] written by Plan B.

Bitcoin as World Reserve Currency

"Upon when investors use bitcoin denomination, not US dollar denomination on the accounting balance sheet, Bitcoin become a reserve currency in the monetary system." – Nik Bhatia, "Layers money: from gold and dollars to bitcoin and central bank digital currencies"[xxi]. Quoting from this fascinating book, "Bitcoin is antifragile, because it thrives off global monetary disorder within the dollar pyramid and is resilient to the threats, slander, and legislation from dismissive bureaucratic entities. The plain truth about bitcoin is that nobody controls it. It has become the first-ever government-free, universally accessible digital currency …. The following figure elucidates a future in which BTC is the world reserve and only first-layer money:" (Figure 3)

In this version of future vision, all future money will eventually be digital tokens held in digital wallets. People will simultaneously hold an assortment of currencies: bitcoin for neutrality with no counter-party risk, central-bank-digital currency for daily consumption and paying taxes, and stablecoins for earning interest. If bitcoin as a reserve currency embodies a future world outstanding treasury bond which is estimated as 119 trillion[xxii], per bitcoin price will eventually come to:

$119 trillion / 21 million BTC = $5,666,666 per one bitcoin

Conclusion

In conclusion, the above three mathematical modeling predicts bitcoin price statically and dynamically as follows:

1. If Bitcoin could eventually replace gold, 1 BTC would reach 550,000 USD.

2. If Bitcoin could eventually become world reserve currency, 1 BTC would be worth more than 5 million USD.

3. Dynamically speaking, stock to flow model has accurately simulated bitcoin to reach 10,000 USD in 2017 and to exceed 50,000 USD around 2021, both occurring within one year of halving event. It predicted bitcoin to reach or exceed 1 million USD around 2026.

This is only a mathematical modeling-based prediction, and by no means should be regarded as financial advice. ◼
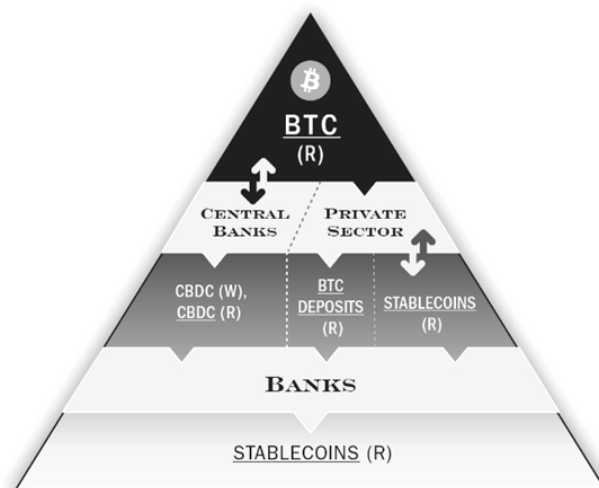
(Figure 3: image courtesy of layered money book)

REFERENCES

i.   Robin Xie is from iSunOne (https://www.isun.one), a cryptocurrency wallet whose clients earn daily interest on BTC, ETH, USDT, USDC.

ii. https://99bitcoins.com/bitcoin-obituaries/

iii. https://bitcoin.org/bitcoin.pdf

iv. https://cryptobriefing.com/bitcoin-birthday-satoshi-hidden-message-explained/

v. https://www.bloomberg.com/opinion/articles/2021-02-08/elon-musk-s-tesla-buying-bitcoin-is-inevitable-and-disconcerting

vi. https://www.wsj.com/articles/paypal-wantmore-customers-to-pay-using-crypto-assets-11620341510

vii. https://www.coindesk.com/square-bitcoin-cash-app-q1-2021-earnings

viii. https://www.coindesk.com/guggenheim-cio-says-bitcoin-could-eventually-climb-to-600000

ix. https://www.bloomberg.com/news/articles/2020-12-10/169-year-old-insurer-massmutual-invests-100-million-in-bitcoin

x. https://www.cnbc.com/2021/02/11/bny-mellon-to-offer-bitcoin-services-a-validation-of-crypto-from-a-key-bank-in-the-financial-system.html

xi. https://www.cnbc.com/2021/03/24/fidelity-to-launch-bitcoin-etf-as-investment-giant-builds-its-digital-asset-business-.html

xii. https://www.coindesk.com/jpmorgan-to-let-clients-invest-in-bitcoin-fund-for-first-time-sources

xiii. https://forkast.news/singapore-dbs-bank-crypto-exchange-digital-assets/

xiv. https://citywireselector.com/news/blackrock-opens-two-funds-to-bitcoin-investments/a1453179

xv. https://markets.businessinsider.com/currencies/news/bitcoin-price-legendary-investor-bill-miller-resilience-better-every-day-2020-11-1029776469

xvi. https://www.bitcoinmarketjournal.com/digital-asset-valuation/

xvii. https://satoshi.nakamotoinstitute.org/quotes/economics/?order=desc

xviii. https://stats.buybitcoinworldwide.com/stock-to-flow/

xix. https://100trillionusd.github.io/

xx. https://medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity-91fa0fc03e25

xxi. https://www.amazon.com/Layered-Money-Dollars-Bitcoin-Currencies/dp/1736110527

xxii. https://en.wikipedia.org/wiki/Bond_market#:~:text=As%20of%202021%2C%20the%20size,Financial%20Markets%20Association%20(SIFMA).

Robin Xie

Robin Xie is the chief commercial officer for iSunOne (https://www.isun.one) , a cryptocurrency asset management platform – "Save anytime. Send to anyone. 8.76% annual interest on USDT, USDC, paid out daily". Robin specializes in start-up success and turn-key solutions, with focus in decentralized finance (DeFi), cryptocurrency, blockchain, and strategic investing. Robin joined iSunOne in 2018, with an aim to build the future of finance and wealth management, as well as to provide financial freedom and autonomy to many unbanked populations. Prior to that, Robin has years of executive management experience in NYSE-listed public companies in subsea robotics and energy-related disciplines. She has a master's degree in engineering from Rice University, and a computer science bachelor's degree from University of Science & Technology of China. She is a proud alumna of Special Class for Gifted Young (class of 1998), admitted in the program at the age of thirteen.