JUN 2020 ● VOL 2

# CRYPTO REVIEW

GOSS INSTITUTE OF RESEARCH

COLLEGE OF BUSINESS
CITY UNIVERSITY OF HONG KONG

B2 FINTECH SCHOOL

## EDITOR-IN-CHIEF COLUMN
Mathematical Certainty in an Uncertain World
*Zhong Zhang*

## INDUSTRIAL INSIGHT
Exploring Bitcoin Blockchain
*Wai-ip Lam, Wai-man Yao, Kam-mau Kuo,*

## DIGITAL ASSETS AND DIGITAL FINANCE
**(PART I)**
*Yao Qian*

## CORRESPONDENCE COLUMN
Emergency Step of Cutting Interest Rate Taken by FED, Another Bull for Bitcoin?
*BitOffer Institute*

## INVITATION TO THE 2020 VIRTUAL CRYPTO FORUM
The Role of Cryptocurrency – Blockchain in the Post-Pandemic World
*CITYU CB & SDSC, GOSS, B2, Crypto Review*

GOSS Institute of Research

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

B2 FinTech Business School

# CRYPTO REVIEW

## CONTENTS


A MESSAGE FROM THE EDITOR-IN-CHIEF

EDITOR-IN-CHIEF COLUMN

01 Mathematical Certainty in an Uncertain World
***Zhong Zhang***

COVER ARTICLE

03 Digital Assets and Digital Finance (Part I)
***Yao Qian***

INDUSTRIAL INSIGHTS

08 Exploring Bitcoin Blockchain
***Wai-ip Lam, Wai-man Yao, Kam-mau Kuo,***

CORRESPONDENCE COLUMN

14 Emergency Step of Cutting Interest Rate Taken by FED, Another Bull for Bitcoin?
***BitOffer Institute***

16 INVITATION TO THE 2020 VIRTUAL CRYPTO FORUM:
The Role of Cryptocurrency – Blockchain in the Post-Pandemic World
***CITYU CB & SDSC, GOSS, B2, Crypto Review.***

# A MESSAGE FROM THE EDITOR-IN-CHIEF:

After a long hiatus, our second issue is now online in a very different world. So different that a year ago it would be considered a dystopian sci-fi movie script by any sane person.

This pandemic changed our view on globalization from every angle: the cross-border movement of people, product, capital, and information; the effectiveness of post-cold war institution and US dollar as its reserve currency; the explosion of "fake news" and the scarcity of truth; the struggle between individual liberty and governments' interest in mass surveillance. A post-pandemic new world must address all these issues to a certain degree. And cryptocurrency, as apolitical money and decentralized ledger, has a role in every single one of them.

The articles in this issue cover digital assets, market analysis for post-halving Bitcoin, the implication of consensus in Bitcoin's scarcity, and a deep analysis of Bitcoin's blockchain data.

We hope you find these articles informative. Stay safe!

**Dr. Zhong Zhang**
*Editor-in-Chief*

# MATHEMATICAL CERTAINTY IN AN UNCERTAIN WORLD

***Zhong Zhang,***
*Editor-in-Chief*

The world has entered a period of extreme uncertainty that has not been seen in at least a generation.

Global economy is idling with pandemic; central banks are printing like money supply matters no more; political risk is flashing here and there; common people are struggling through increasing hardship day after day.

One must hope there are some factors in the economy that are stable like π, a mathematical constant absolutely independent to human actions.

There is one: The total supply of Bitcoin will never be more than 21 million, and this consensus rule is realized by the "halving" mechanism we have just experienced for the third time on May 11, 2020.

Unlike π, which is based on the geometry of our universe, Bitcoin's 21 million supply was picked by human and enforced by a decentralized mechanism incentivized by the economic value of Bitcoin itself. In my opinion this achievement is mathematically beautiful, it is a modern wonder.

Before Bitcoin, we have never reached global consensus on anything created by ourselves: not in art, not in history, and never in economics and politics. The only subjects we can universally agree upon are mathematical and physical facts, like π and the gravitational constant, that are determined in the universe before our existence and are out of our control. Supply of Bitcoin is the first "man-made" mathematical certainty.

Counterintuitively, Bitcoin achieved this not by centralizing a dominating power, but by forming a decentralized network of voluntary peer-to-peer agreements: no one is forced to accept the 21 million total supply, anyone can copy-paste and create her own version of "Bitcoin" with a different total supply setting. But whenever a new peer agrees with this 21 million setting and joins the network, Bitcoin's certainty becomes more mathematical and less man-made.

From this certainty of supply, scarcity and economic value emerge. The value of Bitcoin attracted people from all walks of life, all corners of the world, to reinforce the ecosystem. They are uncertain about when the pandemic will end, about who will be the next president, about how much more money will central banks "print", or about how much more tax they must pay? But they do know Bitcoin provides certainty in monetary supply and uncensored global transaction, not because it is "backed" by a superpower, but because it has grown out of control of its creators. ■

Zhong Zhang

Dr. Zhang is currently a Senior Economist at Bates White Economic Consulting, a litigation consulting firm based in Washington, DC. He is an expert in the economic mechanism design, cryptocurrency and especially the blockchain technical features of Bitcoin's ecosystem.

Before he joined Bates Whites, he was an Assistant Professor of Finance at College of Business at City University of Hong Kong. He joined CityU in 2014 after receiving his Ph.D. from Kelley School of Business at Indiana University. His dissertation is about measuring informed trading in limit order markets. Before doctoral study, Dr. Zhang obtained his M.A. in Economics from Indiana University, and B.S. in Mathematics from Zhejiang University.

Dr. Zhang specializes in Financial Market Microstructure, Investment, and Derivatives. His current research focuses on informed trading, market liquidity, leverage, and their impact on security pricing and investment decisions.

Dr. Zhang has taught Algorithmic Trading and Option Pricing at CityU, and serves as faculty advisor of CityU's award winning delegation to Rotman International Trading Competition.

Disclaimer: Dr. Zhong Zhang's involvement in "Crypto Review" and all activities associated with "Crypto Review" are solely his own and do not reflect the views or opinions of Bates White or its clients. The opinions expressed represent only those of the author, and do not represent the views or opinions of Bates White, LLC or of other Bates White employees or affiliates.

# DIGITAL ASSETS AND DIGITAL FINANCE (PART I)

***Yao Qian,***
*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 first half of the speech given by Prof. Qian YAO at The 5th Global Blockchain Summit, 2019. It is translated and published under the authorization of Prof. Qian YAO. The second half of the speech will be published in next issue - Crypto Review Vol.3.*

The topic of my speech today is "Digital Assets and Digital Finance". Personally, I think digital assets and digital currencies are the two most important aspects of digital economy. The development of digital assets not only effectively expand the application scenarios of digital currencies, but will also lay as an important foundation for the issuance of digital currencies in the future. The coordinated development of the two is the fundamental driving force for the development of digital economy.

If digital economy is described as the body, then digital finance is the blood and digital assets are the core. Characterized by the digitalization of assets, the newly innovated digital finance is a brand new system, which may reconstruct the mode of operation and service, and even the entire ecology of traditional finance.

It seems that the image of "Internet Finance" is not that attractive now. The new image of fintech is defined by "Internet +", "AI +", "Mobile +", etc., with the new concepts including direct banking, online banking, open banking, intelligent investment advisory, etc. However, if overseeing these innovative financial businesses, it could be noticed that they are still within the boundary of traditional financial businesses. The design idea of "Internet +" products usually focus on expansion of channel to obtain long-tail customers, enhancement of data analysis capabilities to carry out precise marketing plans, customization of service to be compliant with specific industrial policies and supervision, etc. However, all these are on "technical" levels, far from the height of "Tao".

What is digital finance or what is its actual innovative attribute for new finance? I believe that digital assets are the core proposition of digital finance. Only when digital assets become active capital can digital finance be active. Therefore, digital finance is backed by the digitization of assets. Through digitization, the attributes of assets will be diversified- they can be securities or currencies, spot or futures at the same time ... In traditional financial business, these attributes are the "amulets" that describe and organize assets and process them into capital that assure the circulation. In the new finance world where assets are digitalized, the boundaries are blurred.

The reason is that the digitization of assets has opened up the "Conception and Governor vessels" of the financial market. All forms of assets that process to digital became divisible capital with liquidity. They can be standardized, empowered and activated without relying on traditional external forces. Taking off labels of currencies, securities, futures and so on, digital assets can circulate more flexibly and independently. Recently, the U.S. Securities and Exchange Commission (SEC) have approved several projects, including project BlockStack, which shows that financing activities can still be carried out without the

participation of traditional financial intermediaries, and that the digitization of assets can lower the financing costs, widen the coverage and increase efficiency. This breaks new ground for the financial system. Financial innovation with digitalization of assets as the core may be an important development direction of digital finance.

**I. Assets with Multi-attributes, Integrated Innovation**

There is a famous saying in economics, "Money is a veil". Applying this saying, we can say that any financial instrument such as currencies, securities, etc. is a veil over the underlying assets. Taking securities as an example, it is a purposefully created symbol for enabling the circulation of underlying assets.

Stocks are the securitization of shareholders' ownership; bonds are the securitization of claims; E-gold is the securitization of physical gold and mortgage-backed securities (MBS) are the securitization of bank credit. The significance of securities is to create liquidity for assets, but digitization of assets may cause a significance change in such. After digitization, assets naturally have liquidity, so there is no need of the veil of securities, nor the so-called securities attribute identification, nor the corresponding regulatory system.

There are many reasons for ICO being so controversial. In addition to being used as a fraud tool, ICO has a different procedure and system from traditional stocks in terms of issuance, circulation and trading. The traditional concepts and models of securities, based on the traditional financial systems and regulatory rules show ambiguity in governing and regulating ICO.

Facing new and unconventional model of digital assets, regulatory authorities in various countries either deny its emergence or, like the SEC, tries to put the veil of securities back on it. In a public statement of November 2018, the SEC mentioned an interesting name, called "Digital Asset Security". In a sense, "Security" seems redundant. The SEC adding "Security" after "Digital Asset" is to express its policy position.

The difference between digital assets and traditional securities can be illustrated with a simple example. The traditional electronic bills are defined as digital assets by many people, but actually they are not. Basically, traditional electronic bills are just a digital form of paper bills. They should be called as securities instead of digital assets. It is because traditional electronic bills record only part of the information that makes them as a circulation tool. They do not record the underlying information related to the trading background such as contracts, logistics, invoices, taxation, factoring, etc. The real digital assets should be original, containing all information, and be displayed and transferred in digital form. Only digitalized order contracts, logistics documents, invoices, factoring contracts and other assets can be called the real digital assets.

These digital assets are like securities, which can be circulated and traded, but they are difficult to be categorized by traditional securities standards. Similar to digital currencies obscuring M0, M1, M2 and other monetary levels, digital assets obscure the attributes of securities. In other words, their attribute connotations become more abundant. They can be recorded in the interbank market as a tradable product, and also be registered in the stock market as a tradable securities, and even be used as a payment tool on the basis of clarified legal relationships. These new attributes of digital assets are vague and diverse, which exactly makes digital assets special — they can be used as securities, or as quasi-currencies. Various attributes are deeply integrated and benefit innovation.

**II. Digitalization of Assets, Driven by Technology**

The digitalization of assets is inseparable from the use of financial technology. The winner of the Turing Award, the father of Pascal, Nicklaus Wirth once proposed a famous formula, "Algorithms + Data Structures = Programs". This formula profoundly reveals the essence of

programs. Extended to a wider range of business application, the formula can be well revised to "Algorithms + Data = Financial Technology". Those frequently mentioned terms such as regulatory technology, big data credit reporting, intelligent investment advisory, digital currencies, etc., are indeed the embodiment of "algorithm + data" with different focuses after the technological singularity is broke by computing power. Therefore, some people admire algorithms to a point that believe building algorithms to imitate and eventually surpass and replace humans is the most important capability in the 21st century. For them, the future belongs to algorithms and their creators.

Digitalizing assets is an exemplary application of algorithms and integration of data. Its fundamental requirement is to ensure the credibility of native data by technical means. The circulation of digital assets also requires various technical backups to ensure its safety, efficiency, collaboration, and control.

The traditional financial business, revolving around the accounts of commercial banks, will be upgraded to Public-Private Key Cryptography System in the era of digital finance. This is a significant change in the history of finance because this brand-new system is created outside the traditional financial system and supported by a set of complex trusted technologies and cryptographic schemes. The mint, circulation, and validation of digital assets will all rely on the new technology of value exchange. The digital form of assets can be either a string of binary encrypted information, or a centralized or distributed ledger, or quantum information stored as qubits in the future. In terms of value transfer, either the "Token model" or the "Account model" can be adopted, and various models can have mutual conversions.

When it comes to the significance of blockchain technology, after decades of development, Internet has initially completed its phased mission - connecting people and information. Nowadays even scenarios with high-consumption yet low-utility such as personal live streaming can be fully supported, indicating the great power of the Internet. However, digital data can be easily deleted, modified and copied. It is very difficult to guarantee efficient, safe and orderly flow of valuable data on the Internet with existing internet security technologies. Therefore, the exchange of value on the Internet still depends on the traditional financial network. In addition, because of data property rights, data is still bound by countries or institutions, forming data islands and constraining its synergy potential.

As a trust machine, blockchain technology has created a new paradigm connecting various parties involved in financial services, breaking data islands, improving data security, reducing transaction costs and enhancing risk control capabilities. Blockchain technology carries so many expectations and has attracted great attention from capital and industry.

All kinds of beautiful words have concealed the dilemma that blockchain technology has few major applications except Bitcoin and Ethereum. In such situation, researchers and technicians should calm down and carefully analyze and improve the deficiencies of blockchain technology, such as how to meet the demands of high-concurrency scenarios, how to interact with other non-blockchain systems, how to solve the data privacy problems, how to combine smart contracts with prevailing regulations, how to design governance mechanisms and set standards suitable for blockchain technology, etc.

China is a world power of Internet, as well as of data. Nevertheless, the power of data is usually referred to its quantity than quality. The big challenges for China in finance technology are the improvement of data quality, the transformation of data resources into valuable assets, the generation of credit score to serve the real economy and the encouragement of the economic development.

This is exactly the significance of asset digitization.

In The Mystery of Capital, Hernando de Soto once described, " It is the formal property system that provides the process, the forms and the rules that fix assets in condition that allows us to realize them as active capital … this formal property system begins to process assets into capital by describing and organizing the most economically and socially useful aspects about assets, preserving this information in a recording system- as insertions in a written ledger or a blip on a computer disk – and then embodying them in a title. " [1]

Blockchain as a trustworthy technology is recognized and endorsed by multiple parties. It is the prototype of a new generation of financial infrastructure. It can enhance credit for the underlying entities who have not been covered by existing financial institutions, promote mutual cooperation and reduce transaction costs. These benefits may largely help small and medium-sized enterprises (SMEs) and other marginalized groups who were once difficult to access loan resources. This technology is of great significance to the country's economic development and financial supervision. (Translated by Tracy Yin) ■

**REFERENCES**

1. Hernando De Soto. 2001. *The Mystery of Capital: Why Capitalism Triumphs in the West and Fails Everywhere Else.* London: Black Swan, 44.

**Yao Qian**

Dr. YAO Qian 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.

# EXPLORING BITCOIN BLOCKCHAIN

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

## INTRODUCTION

Bitcoin blockchain is the most well-known and commonly used blockchain. Hundreds of thousands of bitcoin transactions are confirmed everyday. The blockchain contains valuable data depicting financial activities. Processing of Bitcoin blockchain data has become a hot topic in various research areas.core may be an important development direction of digital finance.

### Sources of Bitcoin Blockchain Data

There are online blockchain browsers that allow users to search and navigate Bitcoin blockchain. You can search for the detail information of a block, a transaction or an address. You can navigate to the transaction that spent certain output of a particular transaction. You can also navigate to the transaction that paid to or spent from a particular address. Online blockchain browsers provide comprehensive information about Bitcoin blockchain. However, these web services may not be suitable for intensive use because of access rate limit.

By running a Bitcoin Core full node, you are maintaining your own local copy of the blockchain. The price is to spare a few hundred GB of disk space. But that should not be a problem because hard disks with several TB are very common today.

Bitcoin Core supports HTTP JSON-RPC protocol, in which the *getblock* command allows you to search for a block given a hash, and the *getrawtransaction* command allows you to search for a transaction given an id. To make *getrawtransaction* work properly, you need to turn on the *txindex* option of Bitcoin Core. These two commands are all you can use to retrieve information of arbitrary blocks or transactions. Unlike online blockchain browsers, there is no easy way to find out which transaction has spent the output of a previous transaction. Intuitively, you can scan through the blockchain and look for a transaction with an input matching the output of a previous transaction. But you will see that this is impractical in coming sections. The proper way is to build database indices that meet your query needs.

### Data Amount of Bitcoin Blockchain

By the end of 2019, there are roughly 610 thousand blocks in the active chain of Bitcoin blockchain. In this section, you will see how much data the first 610,000 blocks contain. A brief summary of the 610,000$^{th}$ block is given below.

Height: 609,999
Block hash:
000000000000000000005d5d8ee9235d74f3844
5289f3420de6250eeffcff028f
Size: 1,249,754 bytes
Transaction count: 2,779
Time: UTC 2019-12-27 11:52:43
Total input count: 5,915
Total output count: 6,599

Generally, each block carries one to thousands of transactions, and the number of inputs and the number of outputs of a transaction vary a lot. Therefore, block count is not a good indication of data amount of the blockchain. Our measurement includes transaction count, transaction size, input count and output count.

In these 610,000 blocks, there is a total of around 488 million transactions, which contain more than 1 billion inputs and also more than 1 billion outputs in total. These transactions altogether (excluding block headers) take up more than 255 GB in space.

| Block count | Total transaction count | Total transaction size (byte) | Total input count | Total output count |
|---|---|---|---|---|
| 610,000 | 487,648,601 | 255,451,501,444 | 1,195,530,351 | 1,298,786,181 |

*Table 1: Data amount of the first 610,000 blocks of the Bitcoin active chain*

Figure 1 plots data amount in four measurements against block count for the first 610,000 blocks. A closer look at the early stage is shown in figure 2. The data amount remained quite low for the beginning 100,000 blocks and started to grow faster afterwards. There was a rapid increase in growth rate at around the 180,000th block. In between the 300,000th and 400,000th block, the growth rate showed a significant increasing trend.

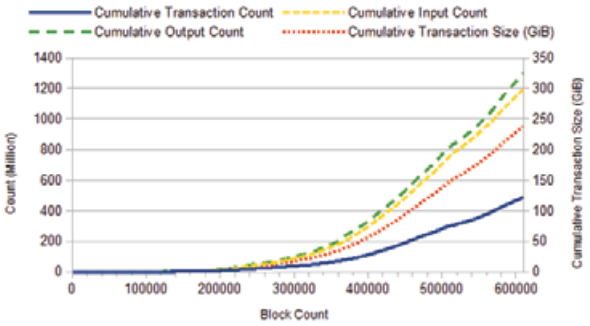



*Figure 1: Data amount against block count for the first 610,000 blocks*

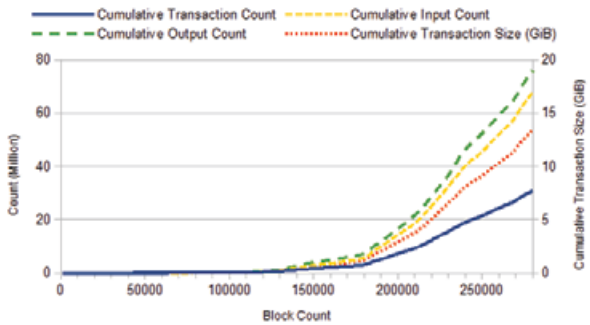



*Figure 2: Data amount against block count for the first 280,000 blocks*

Blocks created and confirmed nowadays carry far more information than blocks of early years did. According to the distribution presented in table 2, the first half of the 610,000 blocks accounts for less than 10 percent of total amount of the data. And the beginning one third of all blocks, that is, around 200,000 blocks, accounts for merely over 1 percent of total amount. That means you have to pay 10 to 100 times as much effort to process all data created so far in contrast to a few years ago. In next section, we will examine how long it takes to perform a basic but important operation with the blockchain data—fetching data from Bitcoin Core.

| Percentage of total data amount | Block height at which cumulative data amount reaches the given percentage of total amount in terms of: | | | | |
|---|---|---|---|---|---|
| | *block count* | *transaction count* | *transaction size* | *input count* | *output count* |
| 1% | 6,099 | 188,626 | 193,886 | 194,493 | 192,581 |
| 5% | 30,499 | 259,922 | 271,268 | 270,953 | 268,610 |
| 10% | 60,999 | 325,069 | 328,057 | 326,180 | 323,662 |
| 20% | 121,999 | 388,231 | 385,562 | 381,912 | 377,243 |
| 30% | 182,999 | 423,205 | 421,009 | 417,303 | 414,988 |
| 40% | 243,999 | 452,308 | 451,769 | 448,591 | 447,296 |
| 50% | 304,999 | 478,964 | 478,770 | 475,863 | 475,157 |
| 60% | 365,999 | 504,297 | 505,000 | 502,409 | 501,660 |
| 70% | 426,999 | 541,263 | 535,530 | 531,623 | 535,979 |
| 80% | 487,999 | 566,207 | 562,916 | 560,664 | 564,260 |
| 90% | 548,999 | 587,187 | 585,161 | 584,482 | 585,763 |
| 100% | 609,999 | 609,999 | 609,999 | 609,999 | 609,999 |

*Table 2: Cumulative distribution of data amount in the first 610,000 blocks of the Bitcoin active chain*

## Fetching Data from Bitcoin Core

To find out how fast Bitcoin Core can respond to intensive block and transaction data retrieval requests, we have written programs in two of the most popular programming languages, namely, Java and Python [1][2], for execution time measurement. The system we used was a virtual machine with 2 3GHz CPU cores and 4 GiB RAM, running 64-bit Linux with kernel version 4.19.0. The runtime environments were JDK 8 and Python 3.7.

Third party JSON-RPC client libraries were used in our programs. We have chosen those recommended by the Bitcoin wiki [3] as of this writing. For Java, we used *bitcoin-rpc-client* 1.0.0 [4]. The client handle was created like this:

```
import java.util.Map;
import
wf.bitcoin.javabitcoindrpcclient.BitcoinJSONRPCClient;
...
BitcoinJSONRPCClient rpc = new BitcoinJSONRPCClient(...);
```

For Python, we used python-bitcoinrpc 1.0 [5], and created the client handle like this:

```
from bitcoinrpc.authproxy import AuthServiceProxy
...
rpc = AuthServiceProxy(...)
```

The first RPC command that we have examined is getblock. It takes a block hash as a parameter, followed by an optional verbosity parameter. With verbosity of 2, detail information about the block and each included transactions will be returned. Two tests were carried out with Java and Python, respectively. In Java, this RPC is accomplished with the statement:

```
Map block = (Map)rpc.query("getblock", hash, 2);
```

And the Python statement for this is:

```
block = rpc.getblock(hash, 2)
```

Both Java and Python programs made a getblock call for every block in the active chain sequentially starting from height 0, and measured the elapsed time it took to run the corresponding statements.

The other RPC command examined is getrawtransaction. It takes a transaction id, known as txid, as a parameter, followed by an optional verbose flag. With verbose of true, decoded information about the transaction will be returned. Optionally, there is the third parameter, which specifies a block hash, indicating which block the transaction is in. When this parameter is missing, Bitcoin Core will need to consult the transaction index to locate the block. Since we would like to find out the time needed to retrieve arbitrary transactions, we did not make use of the block hash parameter. Again, we had two tests in Java and Python, respectively. In Java, this RPC is accomplished with the statement:

```
Map tx= (Map) rpc.query("getrawtransaction",txid,true);
```

And the Python statement for this is:

```
tx = rpc.getrawtransaction(txid, True)
```

Both Java and Python programs made a getrawtransaction call for every transaction in the active chain, including the coinbase, block by block sequentially starting from block height 0, and measured the elapsed time it took to run the corresponding statements. In processing each block, an additional getblock command with verbosity of 1 was issued in order to acquire the list of txid's, but it did not count towards the execution time.

The version of Bitcoin Core used in our tests was 0.18.1. The data folder was on a physical Linux partition, rather than a virtual storage, residing on a traditional hard disk. During the tests, it was configured in such a way that there would not be any peer connection. In between successive test runs, Bitcoin Core was restarted and system cache was cleared with the following command so that variations in execution time due to disk caching effect were eliminated.

```
sync; echo 3 > /proc/sys/vm/drop_caches
```

Some tests took really long and were forced to terminate after running for some 20 hours. The test results are shown in figure 3, with the plot of cumulative transaction size as a reference. Among the four tested methods, Python getblock was the most efficient, and the differences in execution time between it and the others are remarkable. As far as the first 180,000 blocks were concerned, programs using getrawtransaction ran slower than programs using getblock did, probably because they made more RPC invocations. For the getrawtransaction tests, the results with Java and Python were very close, with the Java program taking marginally longer time.

The result of Java getblock was surprisingly disappointing. Its efficiency dropped drastically at around the 180,000th block, which is also the point where a sudden increase in data amount happened. It seems that big JSON messages returned by Bitcoin Core have put a lot of stress on the Java JSON parser. The test could only finish around 19,000 blocks in 20 hours. As this only accounts for about 1 percent of total amount of the data, the test run is supposed to take a few months to complete, while the Python counterpart completed in just 19 hours.

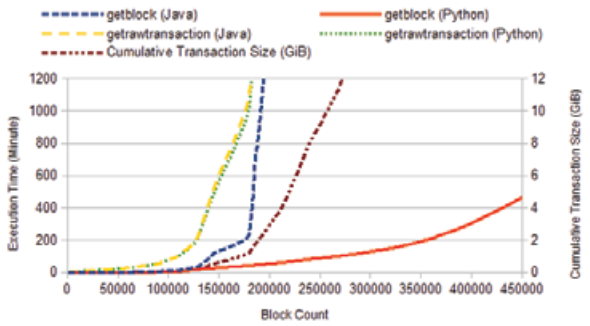



*Figure 3: Cumulative execution time against block count for the first 450,000 blocks*

**Trimming JSON Results from RPC Responses**

Although Java with the recommended JSON-RPC client library has an efficiency problem in handling the verbose result of the getblock command, Java still has its strength in other aspects. Many developers rely heavily on Java to accomplish their jobs. In the result of the getblock command, there is all sort of information including transaction amounts, sources and destinations of funds, and a lot of data for verification purpose. Most of the time, developers having a need to scan Bitcoin blockchain data are interested in the flow of assets rather than proving the correctness of transactions. Therefore, only a small part of the result is meaningful to them.

We suggest a way to get rid of all unnecessary information from HTTP JSON-RPC results, so that applications can save some execution time in processing those JSON results. As Python is found to be very efficient in handling big JSON data object, we implemented a simple HTTP reverse proxy server using Python that could sit between the Bitcoin Core RPC server and the developer's client application, trimming JSON responses. On receiving a request from a client application, the proxy server forwards it to the actual Bitcoin Core server, collects the result from Bitcoin Core and delivers the result, either intact or altered, back to the application.

A Python code template of a simple HTTP reverse proxy server can be found in the appendix. It listens to TCP port 8000 for incoming requests, and it is so simple that it does not include any exception handling. We demonstrate its use by inserting code for trimming the JSON result of the getblock command. Supposing we are only interested in information concerning the flow of assets, we will not need data fields like hex of tx, sequence, scriptSig and txinwitness of vin, hex and asm of scriptPubKey. These fields occupy quite a large portion of the result and can be trimmed. We inserted the following code segment into the proxy server code template.

```
j = json.loads(data)
r = j["result"]
if isinstance(r, dict) and "tx" in r:
  for tx in r["tx"]:
    if isinstance(tx, dict):
      del tx["hex"]
      for vin in tx["vin"]:
         del vin["sequence"]
         if "scriptSig" in vin: del vin["scriptSig"]
         if "txinwitness" in vin: del vin["txinwitness"]
      for vout in tx["vout"]:
         pk = vout["scriptPubKey"]
         del pk["hex"], pk["asm"]
         # BTC->Satoshi
         vout["value"] = int(vout["value"] * 100000000.0)
data = json.dumps(j, separators=(',', ':')).encode()
```

This code segment also plays a trick by converting the *value* of *vout* from a decimal BTC amount to an integral Satoshi amount. You can learn this from the last but one line of the code segment. We started the proxy server in the same host of Bitcoin Core, modified the Java *getblock* testing program by changing the server port number to 8000, which is the service port number of the proxy server, and performed tests with it. We ran the original testing program without proxy and the modified testing program with proxy to fetch the block of height 609999. While the original program took around 9 minutes 35 seconds to finish, the modified one with proxy took only around 1 minute 5 seconds. The saving in execution time is quite remarkable in this case.

**Conclusion**

Since the data amount of Bitcoin blockchain is huge, and continues to grow rapidly, doing intensive processing with the data has become a big challenge. Our tests show that by using RPC with Python, it can take you the greater part of a day to go through all data in the blockchain created by the end of 2019. However, these tests are merely simple tasks. In most serious works, you will probably need to perform a lot

of computation of the data, such as graph exploration, and read from and write to your own data store frequently. The choosing of good programming tools and making efficient use of them are crucial to your data processing works.

In dealing with big results of HTTP JSON-RPC such as those produced by the *getblock* command of Bitcoin Core, particularly with less efficient tools, we implemented a simple reverse proxy server that was able to trim the results for faster processing. By filtering out the selected unnecessary information from JSON responses, a major reduction in processing time can be achieved. ■

**REFERENCES**

1.Ben Putano. A Look At 5 of the Most Popular Programming Languages of 2019. August 30, 2019. https://stackify.com/popular-pro-gramming-languages-2018/.

2.Aman Goel. 10 Best Programming Languages to Learn in 2020 (for Job & Future). February 29, 2020. https://hackr.io/blog/best-programming-languages-to-learn-2020-jobs-future.

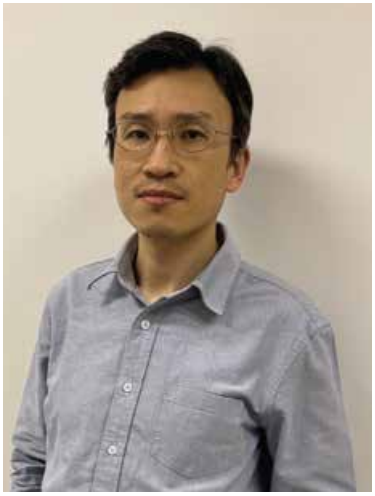
3.API reference (JSON-RPC). Bitcoin Wiki. https://en.bitcoin.it/wiki/API_reference_(JSON-RPC).

4.https://github.com/Polve/bitcoin-rpc-client.

5.https://github.com/jgarzik/python-bitcoinrpc.

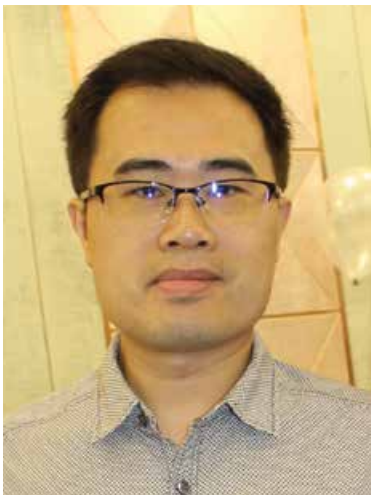
## Appendix: Python Code Template of a Simple HTTP Reverse Proxy Server

```
from http.server import HTTPServer, BaseHTTPRequestHandler
from http.client import HTTPConnection
import json    # for handling json response

class RequestHandler(BaseHTTPRequestHandler):
  def do_POST(self):
    data = self.rfile.read(int(self.headers["Content-Length"]))
    conn = HTTPConnection("127.0.0.1", 8332) # actual server
    conn.request("POST", "/", data, {
                "Authorization": self.headers["Authorization"],
                "Content-Type": self.headers["Content-Type"]})
    response = conn.getresponse()
    data = response.read()

    # Add code here to manipulate response data

    self.send_response(200)
    self.send_header("Content-Type", response.getheader("Content-Type"))
    self.send_header("Content-Length", len(data))
    self.end_headers()
    self.wfile.write(data)

httpd = HTTPServer(("", 8000), RequestHandler)# proxy port number
httpd.serve_forever()
```



**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.

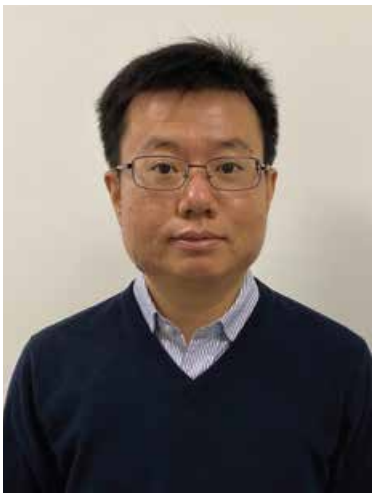


**Kam-mau Kuo**
**Senior Systems Analyst**
**Hieroglyph Digital Technology Limited**

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.

# EMERGENCY STEP OF CUTTING INTEREST RATE TAKEN BY FED, ANOTHER BULL FOR BITCOIN?

*BitOffer Institute*

***Editor's Words:***

*This article is selected from correspondences sent by BitOffer Institute. The Institute analyzes the US Fed's rate cut on March 3, 2020, and anticipates the impacts of this decision. Written before the halving of Bitcoin on May 11, the article also offers views on investing in Bitcoin regarding the current economic environment.*

The Federal Reserve on Tuesday took the emergency step of cutting the benchmark U.S. interest rate by half a percentage point, an attempt to limit the economic and financial fallout from the coronavirus. Since the financial crisis in 2008, the reduction of this time was the largest, which was considered as the bailout to the market. Even though, America Stock Market did not buy it. After the news released, the Dow Jones Index dropped by nearly 800 points (3%). In the short term, the decline of the America Stock Market has decreased by more than 10%.

Powell held a news conference following the central bank's decision. He said the Fed "saw a risk to the economy and chose to act."

"The magnitude and persistence of the overall effect on the U.S. economy remain highly uncertain and the situation remains a fluid one," he said, "Against this background, the committee judged that the risks to the U.S. outlook have changed materially. In response, we have eased the stance of monetary policy to provide some more support to the economy."

With the global outbreak of COVID-19, the fear of investors caused the capitals to be called back from the market, which pushed the market to face the shocking situation, especially for the stock market of Europe and the United States. As the stock market has been through the worst month since the last financial crisis, what kind of investments are investors able to follow while the stocks and golds performed unexpectedly? BitOffer Institute believes that the interest cut this time is the proof of that how severe the problem is. Comparing to the last emergency interest reduction happened on Oct 8th, 2008 because of the economic recession caused by the Collapse of Lehman Brothers, the rate cut this time obviously indicates Fed's serious attempt to the current situation. However, investors still need to be cautious about the impacts of the decision.

First, COVID-19 has brought unexpected challenges and risks to the global economy, leading to the turbulence in the financial market. In addition, it does significant impacts on the global industry chain and the operation of the supply chain, which also does harm to the economy of the United States. However, the interest cut was helpless to the problems of the supply chain.

Besides, the recent US Treasury yields have created the lowest level in the past 100 years. If the Fed continues cutting the interest, it would drop down the US Treasury yields further. Once it happens, the central banks of other countries and the institutions would start selling US Treasury. Including but not limited to the America Stock Market, when investors are worried about the economy of the United States, the capitals will choose to act in the way of "Cash Out" and seek other investments such as gold and Bitcoin to hedge the risk.

**Views on Investing in Bitcoin**

Despite the hedging feature of Bitcoin, the COVID-19 and its unmeasurable impacts witnessed the Bitcoin price plunging by $5,000 within 2 weeks in March. As it dropped from $9,000 to $3,800, it created the worst daily decline in 7 years. While the market liquidated almost all the longs positions, it triggered a chain reaction that the market had panic emotions surrounded, and the Bitcoin price was frustrated.

The decline indicates that the market is full of risks. Under such circumstance, the market usually liquidates the longs and shorts at the same time while one leverages the trading. The risk of futures trading thus can be extremely high. Similarly, if one trades standard contracts, whether he or she opens positions or not, the value of account would decline as the token price dropped.

In this way, we sees Bitcoin Options Trading as an investment with lower risk and profitable return. Bitcoin Options is a prediction of the price volatility of Bitcoins in the future. Essentially, it operates like the spot trading, but it allows the investors to buy call or put: Call when the investors expect the market to be bullish, Put when the investors expect the market to be bearish. Its profit formula is the same as that of the spot trading: Within the Options contract period, the investors would earn the price spread if the investors choose the correct direction.

The most significant feature of the options trading is that it has an inherent 2,000 times leverage, but it does not have any risk of being forced into liquidation. The investors who trade Bitcoin Options do not have to pay attention to the market all the time. With the feature above, the mentality will be hard to be influenced, so that it will be much easier to make correct choices and strategies.

Meanwhile, for long-term investors, we would consider investment in Bitcoin ETF. If one buys Bitcoins on the spot trading market and holds it, when the bitcoin price rises to $30,000, the owner would earn a 3-times payoff. However, if one buys Bitcoin ETF, the highest payoff would be able to reach 17 times due to its automatic positions adjustment mechanism and its compound calculation, which means that its ROI would be much higher than that of Bitcoins on the spot trading market.

Moreover, the 3rd halving of Bitcoins is expected to happen in May. On the occasion, the block reward of Bitcoin Mining will be reduced from 12.5 to 6.25. The scarcity will directly lift up the value of Bitcoin in the long term. We have reasons to believe that the upcoming halving of Bitcoins will be the catalyst to push the Bull market to come out. ■

# Invitation to the 2020 Virtual Crypto Forum: The Role of Cryptocurrency – Blockchain in the Post-Pandemic World

The 2020 Virtual Crypto Forum on 16th June 2020, organized by the **College of Business and School of Data Science at City University of Hong Kong (CITYU CB & SDSC), GOSS Institute of Research (GOSS), B2 FinTech School (B2)** and ***Crypto Review***.

The unprecedented outbreak of COVID-19 has drastically changed people's life styles across the globe. Facing the increasing demand for digital economy, the ideology neutral blockchain is seen as the bridge between different nations and an emerging global marketplace.

Responding to the global discussion of cryptocurrency and blockchain and to create a positive and inclusive voice in this era of instability and intolerance, the 2020 Virtual Crypto Forum brings together scholars in academia and senior experts from industry. The interdisciplinary discussion will take a focused look at the development and application of currency and blockchain integration, their social and economic significances in the post-pandemic world.

This is the First Joint Crypto Forum, also the fourth biennial GOSS Forum. The forum will be organized as a webinar to connect global speakers and audience. It will be conducted in English and Putonghua with simultaneous interpretation. Participation is open to the public.

Time: Jun 16, 2020 (Tuesday)
Morning Session: 09:00 - 12:30
Afternoon Session : 14:30 - 18:20
Medium: English / Putonghua (with simultaneous interpretation)

Forum Agenda:
English version ~ https://cryptoreview.hk/2020cryptoforum-agenda/
Chinese version~ https://cryptoreview.hk/2020cryptoforum-agenda-chinese/

*Remarks:
1. Confirmation (with Zoom ID & Password) will be sent by EMBA Office (emba@cityu.edu.hk) upon successful registration.
2. 300 Quotas (on first-come-first-serve basis, will be in waiting list if exceeded the quota). For "No shows" 10 minutes after the start of session, the quota will be given to participants in waiting list.

Learn More About Crypto Forum: https://www.cryptoreview.hk
For any enquiry, please email to: info@cryptoreview.hk

College of Business 香港城市大學 City University of Hong Kong | The new EMBA | School of Data Science 香港城市大學 City University of Hong Kong | GOSS Institute of Research | CRYPTO REVIEW

# 2020 Virtual Forum
# The Role of Cryptocurrency - Blockchain in the Post-Pandemic World

June 16, 2020 | Hong Kong Time Zone | Via Zoom Webinar

**Welcoming address by**

**Prof. Way KUO**
President and University Distinguished Professor,
City University of Hong Kong

## Morning Session
**09:00-12:30**

* Speakers are in alphabetical order by last name

**Chair:**
**Prof. S Joe QIN** (Organizer)
Dean of School of Data Science,
Director of Hong Kong Institute for Data Science,
Chair Professor of School of Data Science,
City University of Hong Kong

**Prof. Steven KOU**
Questrom Professor in Management and Professor of Finance,
Questrom School of Business,
Boston University

**Dr. Lawrence MA**
President of Hong Kong Blockchain Society

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

**Prof. Harald UHLIG**
The Bruce Allen and Barbara Ritzenthaler Professor,
Economics and the College,
University of Chicago

**Prof. Jerome YEN**
Head of Centre for Innovation and Entrepreneurship
Distinguished Professor of Department of Computer and Information Science of Faculty of Science and Technology, University of Macau

**Dr. Zhong ZHANG** (Organizer)
Editor-in-Chief
*Crypto Review*

**Prof. J. Leon ZHAO**
Chair Professor of Department of Information Systems at College of Business,
City University of Hong Kong

## Afternoon Session
**14:30-18:20**

**Chair:**
**Dr. Michael WONG** (Organizer)
EMBA Programme Director and Associate Professor of Finance,
City University of Hong Kong

**Mr. BAO DanRu**
Independent Director of China Construction Bank Pension Management Co., Ltd.
Former Deputy Director of the Shanghai Human Resources and Social Security Bureau

**Prof. Emil CHAN**
Chairman
Fintech Committee of Smart City Consortium

**Mr. DU Ping**
Chairman
ShuJu Bay Area Big Data Research Institute

**Mr. Frank KAO**
Product Manager
BitoEX, Taiwan

**Prof. Jason LAU**
Chief Information Security Officer (CISO)
Crypto.com

**Ms. Marie-Line RICARD**
Associate Partner of Sia Partners

**Dr. XIAO Feng**
Vice Chairman and Executive Director
China WangXiang Holdings

**Dr. Alex YANG**
CEO of V. SYSTEMS

## Details and Registration

https://cityu.zoom.us/meeting/register/tJMvc-uprTsuHNXYxY9Tfj_sHB0yi07vgbEN

Organizers:

**Prof. Houmin YAN**
Dean
College of Business
City University of Hong Kong

**Prof. QJ GAO**
President
GOSS Institute of Research Ltd

**Mr. Dadu LEE**
President
B2 Fintech School

GOSS INSTITUTE OF RESEARCH LIMITED

Penthouse 24C, Tai Yau Building,
181 Johnston Road, Wanchai,
Hong Kong

Tel : +852-28015500
Fax : +852-28017700
Website : www.goss.com.hk www.cryptoreview.hk

CITY UNIVERSITY OF HONG KONG
COLLEGE OF BUSINESS

12-200 Lau Ming Wai,
Academic Building (LAU),
City University of Hong Kong,
Kowloon Tong, Hong Kong

Tel : +852-34428989
Fax : +852-34420151
Website : www.cb.cityu.edu.hk

B2 FINTECH SCHOOL

Shanghai Main Campus:
Suite 603, Floor 6,
Jin Ying Tower A,
Han Xiao Road,
Shanghai

Tel : +86-21-68779982
Website : www.b2fintech.com