

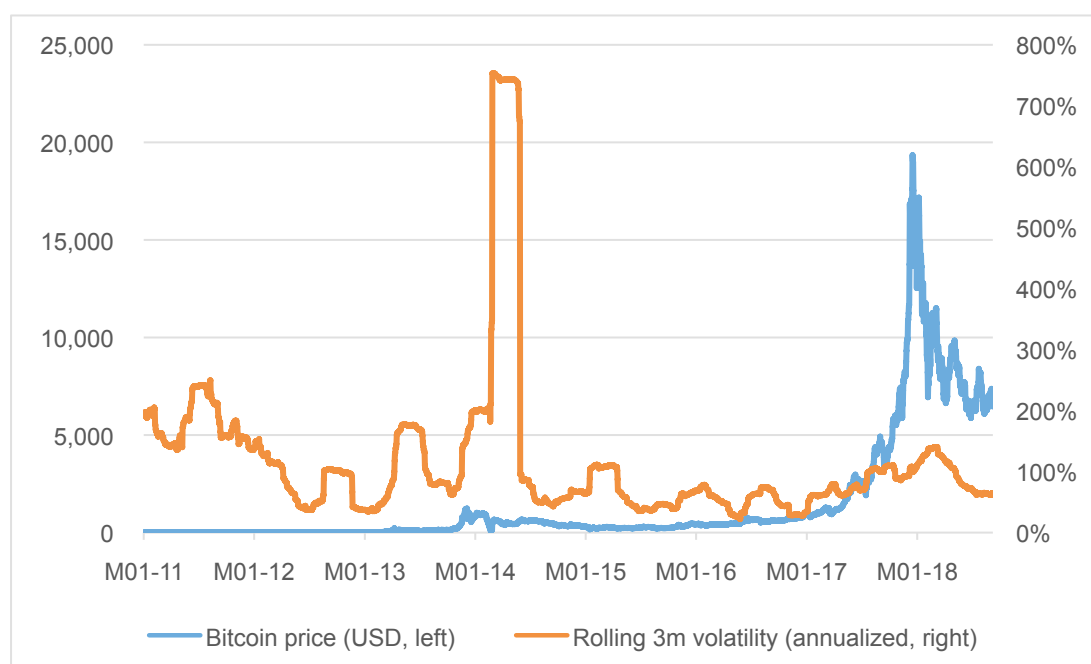
Bubbles and Opportunities: An Economic Analysis of Cryptocurrencies and Blockchain Technology

Chuanwei “David” Zou

Since 2017, speculation in cryptocurrencies has swept the world, and innovation in blockchain technology has been very active. Markets are flooded with specious ideas about cryptocurrencies and blockchain. In order to clarify popular misunderstandings, make financial innovations beneficial to society, and introduce necessary regulations, it is necessary to study cryptocurrencies and blockchain technology from an economic perspective.

I. Pricing of Cryptocurrencies

Figure 1 shows Bitcoin price and its volatility between January 1, 2011 and September 7, 2018. During that period, Bitcoin’s annualized return is 266% and its annualized volatility is 171%. Overall speaking, cryptocurrencies represented by Bitcoin have become the first asset bubble in a global scale, and many irrational behaviors of individuals and groups can be observed.



Data source: Yahoo Finance and calculations by the author.

Figure 1: Bitcoin price and volatility.

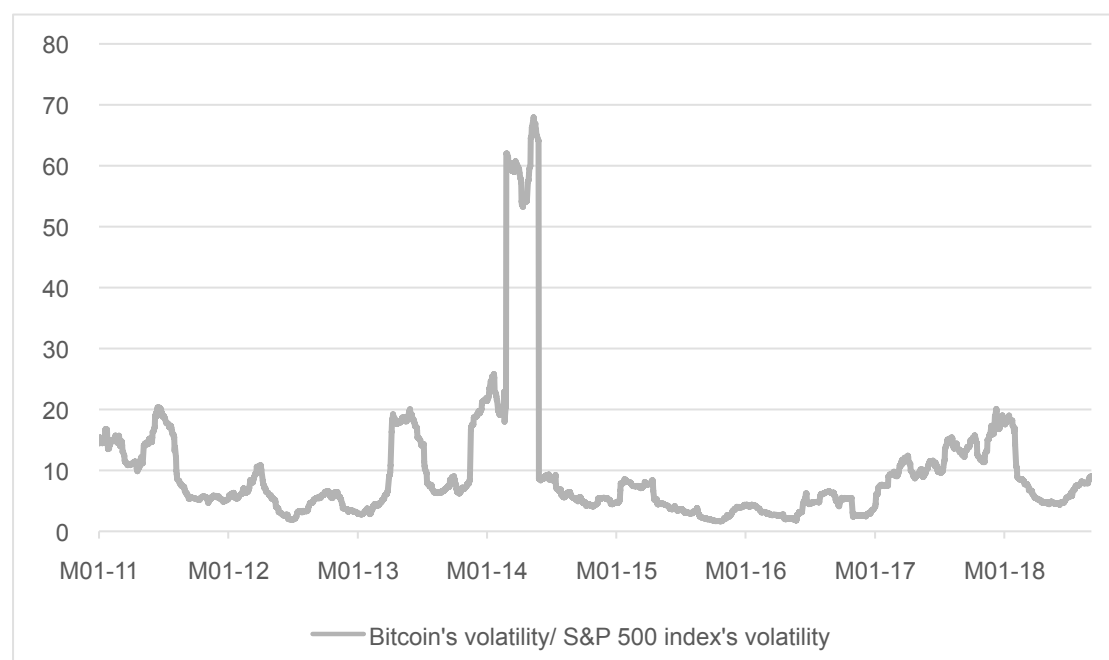
There are two popular misunderstandings about Bitcoin price. The first viewpoint is that the demand from the underground economy has pushed up Bitcoin price. There are certain reasonable elements in this viewpoint. Bitcoin has the characteristics of anonymity and decentralization, and

exists in an electronic form, which makes it suitable for the underground economy. However, there are no reliable data regarding the volume of Bitcoins used in underground economic activities. Lots of evidence indicate that due to the rising trend of Bitcoin price, a significant portion of Bitcoin is hoarded by speculators. Hoarding, of course, is a common phenomenon in speculation activities and helps to boost asset prices by reducing effective supply.

The second viewpoint is that the cost of Bitcoin "mining" supports Bitcoin price. As the "mining" cost increases, Bitcoin price will rise too. However, this viewpoint is hard to hold. At any given time, the supply of Bitcoin is determined by a prespecified algorithm and has nothing to do with how much computation power (measured by hashrate or the number of Hash operations per second) is engaged in "mining". If the price of Bitcoin goes up, hashrate will be higher, but the supply of Bitcoin will not increase correspondently, and the price of Bitcoin will not be held back. As more computation power competes for a given number of new Bitcoins, the cost of "mining" (measured by the number of Hash operations required to produce a new Bitcoin) rises. Similarly, if the price of Bitcoin falls, the "mining" hashrate will be lower, but the supply of Bitcoin will not be reduced, and the price of Bitcoin will not be pushed up. Under this scenario, less computation power competes for a given number of new Bitcoins, which reduces the "mining" cost.

II. Can Bitcoin futures stabilize Bitcoin price?

Bitcoin's volatility is too high for it to be an effective medium of exchange, nor is it economically feasible to develop Bitcoin-denominated financial transactions. Figure 2 shows the ratio of Bitcoin's volatility to that of the S&P 500 index since 2011. It is also very cheap to trade the S&P 500 index funds. Therefore, the S&P 500 index funds are a better medium of exchange than Bitcoin.



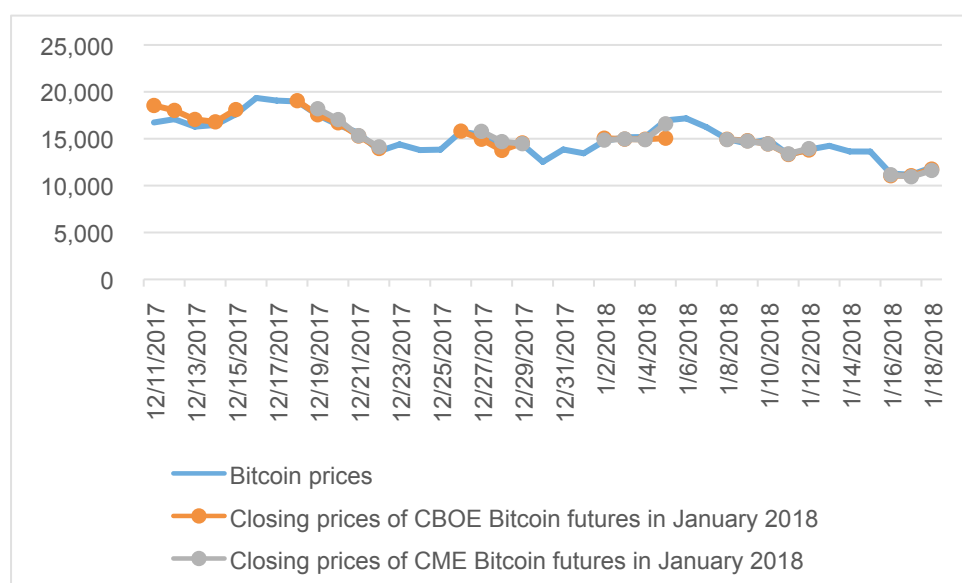
Data source: Yahoo Finance and calculations by the author.

Figure 2: Comparison of volatilities of Bitcoin and the S&P 500 index

Price stability is a necessary condition for Bitcoin to become an effective medium of exchange.

One proposal is Bitcoin futures. On December 10 and 18, 2017, CBOE Global Markets and CME Group respectively introduced Bitcoin futures. In addition to price discovery and risk management functions, Bitcoin futures facilitate the participation of institutional investors in the Bitcoin market, which was a key driver of the sharp rise in Bitcoin prices between October and mid-December, 2017. In addition, it is straightforward to develop Bitcoin ETFs based on Bitcoin futures, which allows retail investors to acquire exposure to Bitcoin through mainstream stock exchanges rather than cryptocurrency exchanges or wallets.

The Bitcoin futures of CBOE and CME play a certain role in price discovery and risk management (figure 3), but Bitcoin's volatility does not decrease significantly (figure 1 and figure 2). In fact, seeing from the general situation in commodity futures and financial futures markets, futures trading does not necessarily lower the volatility of underlying assets.



Data sources: CNBC, Yahoo Finance.

Figure 3: Bitcoin futures of CBOE and CME¹ (in USD).

The transaction volume of Bitcoin futures is not large. This suggests that Bitcoin futures only carry out very limited risk-hedging functions, and that institutional investors' interest in Bitcoin futures remains small.

III. Feasibility of stable tokens

Some practitioners are experimenting with stable tokens. There are two representative methods. The first category, represented by Tether, claims to issue a USDT token pegged 1:1 to USD and with a reserve rate of 100%. This amounts to a currency board regime. However, it is not clear whether Tether has sufficient reserves. If investors find that stable tokens such as Tether do not have sufficient reserves, a run on the currency peg will occur immediately. Indeed, Tether has become a source of systemic risk for cryptocurrency market.

The second category, represented by Basecoin, is still in the state of development, claiming that it will mimic the open market operations of central banks. In order to stabilize Basecoin's prices in

¹ Bitcoins are traded every day but Bitcoin futures of CBOE and CME are traded only on working days.

USD, it fine-tunes the Basecoin supply by issuing and repaying bonds denominated in Basecoin.

I think the success of the second category is very difficult. The "impossibility triangle" is a proper statement for this kind of stable tokens. Stable tokens can only achieve at most two of the three objectives, namely, fixed exchange rate against fiat money, free convertibility, and independent monetary policy. Stable tokens currently under experiment adhere to the first two objectives, which means abandoning the independence of monetary policy. Furthermore, these stable tokens try to implement monetary policy operations through algorithms, which is equivalent to giving up discretion in monetary policy. From the perspective of human history, it is the first time that a fixed exchange rate has been pursued solely through algorithms.

IV. Proliferation of blockchain forks

Theoretically, anyone can create a blockchain fork with the back of computation power. There is usually a limit on the amount of fork coins. A portion of them are "pre-mined" by the founder, another portion of them are given to the holder of original coins, and the rest of them are reserved for the communities of fork coins. In the secondary market, fork coins are traded independently of original coins.

The economic relationship between fork coins and original coins is quite complex. In many blockchain forks, holders of original coins receive fork coins for free (airdrop), the amount of which is proportional to the amount of original coins they hold. This makes blockchain forks look like stock splits or dividends. However, it is not technically necessary to give fork coins to the holder of original coins. The aim of airdrop is to win the support of the holders of original coins for fork coins, or to develop communities of fork coin based on communities of original coins. Therefore, it is not the inherent right of the original coin holders to get the fork coins for free. In this way, blockchain forks are equivalent to the replacement of different versions of currencies, with new currencies already in circulation but old currencies still in use. This actually leads to an extra supply of coins and weakens the binding power of the upper limits of original coins. If blockchain forks occur without constraints, oversupply of coins will cause inflationary effects.

There is a competitive relationship between original coins and fork coins, which is close to the situation of private currency competition envisaged by F.A. Hayek. The cryptocurrencies that win the competition will have the following characteristics: (1) Its transaction cost is low and its transaction efficiency is high. (2) Its wallets, trading venues and other infrastructure are very safe. (3) Its price is relatively stable so as to better undertake monetary functions such as medium of exchange and storage of value. Because of the inherent network effects of money, only a few cryptocurrencies can win.

V. Token economy

The token economy represents a category of promising blockchain application projects. In these projects, there are transactions with real needs, but these transactions were previously constrained by incentives, transaction costs, or payment tools. By introducing tokens, these projects not only solve the problem of fundraising, but also ease the constraints of incentive mechanism, transaction costs, and payment tools. Successful projects in this area remain to be seen. I think many token economies can be built through the following three steps.

(I) Exchange economy core

A token economy generally has an exchange economy core, around which other activities are built. The exchange economy is a basic concept in economics. It exists because different people have different endowments and because of the division of labor. It abstracts the production and consumption processes from economic activities and focuses instead on the scenario where the product has been produced and is held by different people, and the problem is just how to exchange the product among different people. E-commerce, sharing economy, browsers, web portals and search engines all have the characteristics of exchange economy.

(II) Tokenization

The meaning of tokenization is to replace the exchange medium in the Internet exchange economy with a certain token. At this step, we can assume that the token is issued and managed by a central entity.

There are two cases of tokenization. First, when the exchange medium is fiat money or a virtual currency, because of the existence of price mechanism, it is very straightforward to replace the exchange medium with the token. E-commerce and the sharing economy belong to this case. Second, when the exchange medium does not have any monetary characteristics, because there is no price mechanism, tokenization also means the introduction of price mechanism. Browsers, web portals, search engines, etc., belong to this case. The price mechanism can effectively aggregate market information, improve the efficiency of resource allocation, and maximize social welfare.

(III) Blockchain overlay

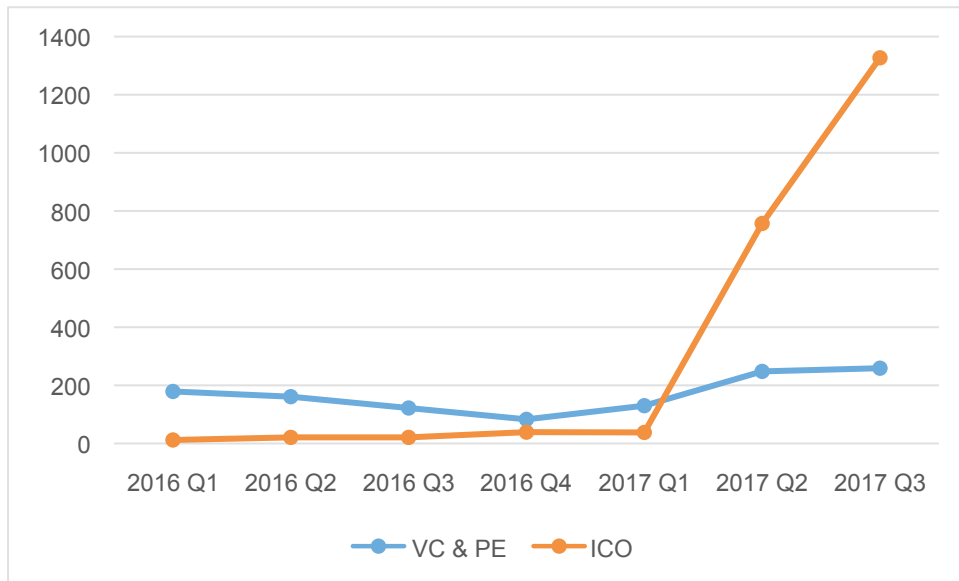
Blockchain overlay means: (1) The tokens issued and managed by the central entity in the second step are replaced with decentralized tokens generated within blockchain; (2) Through the distributed ledger of blockchain, the efficiency of division of labor in exchange economy can be improved. Also, the problem of asset registration and transaction records are solved; (3) A compatible incentive system is designed for the participants in token economy (including not only exchange participants but also entities providing ancillary services for exchanges) so as to encourage them to jointly maintain the sustainability of the token economy.

Blockchain overlay shows the triple attributes of blockchain in economics: a decentralized payment system, a distributed ledger, and an incentive mechanism. These attributes enable blockchain to support economic activities in a decentralized and self-organized environment. However, in the process of applying blockchain to achieve these goals, there are very complex problems regarding transaction costs and the governance structure.

At present, a highly controversial issue is that, although a token economy project has not yet been successful, the tokens issued by the project may be hyped up to a very high price through ICO (initial coin offering) and cryptocurrency exchanges.

VI. The unsolved problems of ICO

Blockchain projects generally have two financing channels: equity financing and ICO. ICO is chaotic and risky all around the world, which is reflected in the following three aspects.



Source: CB Insights.

Figure 4: Amount of global blockchain project financing (in million USD).

First, the economic functions and intrinsic value of the tokens given to investors by ICO are often ambiguous. Generally speaking, tokens have three possible characteristics: (1) Medium of exchange; (2) Certificate of equity, and ICO with the issuance of such tokens is close to equity crowdfunding; (3) Certificate for goods or service, and ICO with the issuance of such tokens is similar to crowdfunding for product development. Many tokens combine multiple characteristics and it is difficult to value them. Nevertheless, many tokens become hyped even before their intrinsic value is fully revealed or discussed.

Second, speculation in tokens occurs after ICO. Unlike crowdfunding, after many ICOs happen, tokens can be traded in the secondary market, especially in cryptocurrency exchanges. In theory, if the token is a certificate of equity, goods, or services, its valuation should be "anchored" to some fundamental factors. But in reality, many token prices are hyped up to the levels far above the fundamentals. Some tokens began to speculate even before ICO (i.e. the so-called pre-sales or pre-ICO stage). It is difficult for ICO to ensure the suitability of investors. ICO projects usually are in early stages with high risks. Theoretically, ICO should be limited to qualified investors with adequate abilities to identify and take risks, and it must also limit the exposure of a single investor. However, some ICO projects are actually open to the public through cryptocurrency exchanges.

Third, ICO distorts the incentive mechanism for blockchain start-up teams. The secondary market of tokens provides the start-up teams an easy way to "cash out" even when the blockchain venture projects may still stay in the white paper stage. In contrast, in the venture capital industry, the time from start-ups getting investment from venture capital firms to IPO is much longer. The fast "cash out" mechanism of ICO will distort the incentive mechanism of the blockchain start-up teams. Besides, token holders are often in a vague position in the governance structure of blockchain projects, and lack effective measures to align the interest of the start-up teams with theirs.

Finally, in the field of cryptocurrencies, ICO has formed a positive feedback loop between "central currencies," such as Bitcoin and Ether, and other tokens. ICO generally collects Bitcoin

and Ether, which will increase the demand for Bitcoin and Ether and push up their prices. And the prices of Bitcoin and Ether serve as the valuation benchmark for the tokens issued by ICO. In this way, a mutually reinforcing feedback mechanism has been formed between Bitcoin, Ether, and other tokens. This is a key driver behind the spectacular rise in the cryptocurrency market in 2017. However, if the prices of Bitcoin and Ether enter a downward path, this positive feedback mechanism will also cause the prices of other tokens to fall faster.

VII. Central bank digital currency

First, when it comes to its economic function, central bank digital currency (CBDC) is a replacement for cash. CBDC is issued directly by the central bank to the public and consists of the liability of the central bank. It is a form of fiat money and can pay interest to its holders. By contrast, the interest rate of cash is always 0.

Second, in terms of technical means, CBDC is not necessarily based on blockchain. The robustness and security of distributed ledgers are the primary considerations for the adoption blockchain. But a public blockchain (with free entry and exit of nodes) represented by the Bitcoin blockchain and its proof-of-work consensus mechanism will lead to a waste of social resources, mainly in computation power and electricity consumption. Thus, CBDC tends to take the form of a consortium blockchain, and the distributed ledgers are maintained by the central bank and certain preauthorized institutions.

Third, in terms of monetary policy, CBDC will become a new monetary policy instrument. Particularly, CBDC can pay negative interest, thus helping the central bank to break through the zero-lower bound of nominal interest rates and magnifying monetary policy stimulus during economic crises. In contrast, when cash is still in circulation, negative nominal interest rates are impossible because people will withdraw their bank deposits and change them into cash.

Fourth, when it comes to financial stability, CBDC will have a major impact on the payment and settlement system. Payment and settlement will not necessarily go through commercial banks and can be carried out directly on the balance sheet of the central bank. Therefore, CBDC helps to get rid of the special position of commercial banks in the payment and settlement system and the accompanying "too big to fail" problem. But this could also cause instability in bank deposits, as people may withdraw bank deposits and change them into CBDC.

VIII. Regulation of Cryptocurrencies

Speculation in cryptocurrencies directs limited social resources into unproductive areas. Once the speculative bubble bursts, it will have a negative impact on wealth distribution. Speculation is also accompanied by frauds, scams, and illegal conduct. Therefore, there is no doubt that regulation of cryptocurrencies should be strengthened. In addition, cryptocurrencies move across borders, and the speculation is global. Therefore, global regulatory coordination should be strengthened.

(I) Regulation of the production and issuance of cryptocurrencies

Cryptocurrency production consumes lots of electricity, especially for cryptocurrencies with proof-of-work consensus mechanisms. According to Digiconomist, the annual electricity consumption by the Bitcoin blockchain is equivalent to that of Peru and is still growing rapidly. Considering the pollution caused by thermal power generation, the Bitcoin blockchain is actually

causing serious environmental problems.

(II) Regulation of the circulation and transaction of cryptocurrencies

Cryptocurrency exchanges are widely distributed around the world. Exchanges provide liquidity for cryptocurrencies. Once a cryptocurrency is listed on an exchange, its price usually rises significantly. Essentially this shows the effect of the liquidity premium. Cryptocurrency exchanges have fueled speculation and have also taken on high risks themselves.

First, similar to ICO, cryptocurrency exchanges have few proper checks on account holders, and many exchanges allow anonymous accounts.

Second, leverage-based speculation exists. Some cryptocurrency exchanges offer leverage to investors, which amplifies the price fluctuations in cryptocurrencies. But if the cryptocurrency market enters a system-wide and large decline, high leverage will amplify the downward trend.

Third, there are problems of market manipulation. Many cryptocurrencies are held in a concentrated way, and the cryptocurrency exchanges do not have the same information disclosure requirements as the stock exchanges, making market manipulation possible. A typical manipulation strategy is the so-called "pump and dump," where a number of large cryptocurrency holders conspire to push up prices and attract retail investors, then suddenly sell their holdings. Retail investors without "roof escape" suffer losses.

Fourth, some cryptocurrency exchanges have opened the door to fraudulent ICO projects, actually colluding with them to deceive retail investors.

Fifth, incidents such as the cryptocurrency exchanges being attacked by hackers, leading to theft of customers' assets and even bankrupting exchanges, have occurred many times.

Finally, cryptocurrencies, because of their anonymity, are associated with illegal transactions or activities in the underground economy. The former "Silk Road" website is a typical example. Cryptocurrencies help ISIS to get access to funding. Cryptocurrencies are also used to circumvent capital controls.

To handle the above problems, regulators all around the world should implement the following measures: (1) The requirements of "Know Your Customer" (KYC), anti-money laundering and anti-terrorism financing, especially for cryptocurrency wallet providers and exchanges; (2) Tax on cryptocurrency transactions; (3) Requirements for investor suitability; (4) Combating frauds and market manipulation; (5) The exchange between cryptocurrencies and fiat currencies, which is the area where regulators should and are best able to strengthen regulation.

IX. China's Role in the Cryptocurrency Market

China has a large presence in the cryptocurrency market. The three largest Bitcoin mining hardware companies—Bitmain, Canaan Creative, and Ebang—are all in China. By some estimations, Chinese mining pools control more than 70% of the computational power of the Bitcoin network. Three of the largest cryptocurrency exchanges in the world, namely Binance, OKEx, and Huobi, are run by Chinese. However, since 2013, Chinese government has become more and more negative towards cryptocurrencies. In 2013, Chinese government warned domestic financial institutions against the risk of Bitcoin. From late 2016 to early 2017, the Chinese

government investigated major cryptocurrency exchanges, especially regarding their roles in money laundering and capital outflow. In September 2017, the Chinese government banned ICO and centralized cryptocurrency trading. Many cryptocurrency exchanges moved abroad but still offered trading services to domestic investors. In January 2018, the Chinese government blocked online access to overseas cryptocurrency exchanges. Since August 2018, the Chinese government has clamped down online platforms promoting ICO projects and cryptocurrencies trading. It has also introduced more restrictions on over-the-counter cryptocurrency trading.

It is worth noting that Chinese government is very positive on the potential of blockchain technology. For example, China's central bank, the People's Bank of China, has a dedicated team for CBDC. This team has conducted extensive research and experiments on the application of blockchain technology in the financial sector. However, due to the restrictions of China's securities law, ICO and cryptocurrency exchanges won't be legal in China for the foreseeable future. In China, only certain categories of financial instruments are considered securities. Security tokens aren't covered by the securities law. Therefore, fundraising via token issuance is considered to be illegal and subject to severe punishment. As a consequence, cryptocurrency exchanges facilitating trading in those tokens are illegal, too. Those situations will not change without revising the securities law. By comparison, the Chinese government is neutral towards mining pools as long as they purchase electricity in a legal way and pay due tax. Mining hardware companies are considered to be high-tech companies. Chinese government encourage them to apply their chip design skills to areas more relevant to the real economy such as artificial intelligence.

About the author

Dr. Chuanwei "David" Zou is the Chief Economist of Bitmain since 2018. From 2015 to 2018, he was a founding partner of Nanhu Financial Corporation. From 2006 to 2015, he held various posts in China Investment Corporation (CIC), China's sovereign wealth fund. Dr. Zou holds a B.S. in statistics and a M.A. in economics from Peking University, a Ph.D. in Economics from Tsinghua University, and a Mid-Career MPA from Harvard University. In 2015, he won the Sun Yefang Prize for Financial Innovation, China's top prize for economists.