

Cryptocurrencies: New Rules for a New Technology?

Research note

Guillaume Beaumier and Kevin Kalomeni*

Université Laval, Canada

May 29, 2018

Abstract

In a time of macroeconomic uncertainty, the recent upswing in cryptocurrencies' prices has raised many eyebrows. While its supporters see it as the way forward, many established economists and heads of financial institutions warn us of falling for an economic mirage. As the dust settled and Bitcoin is no longer on the front page of every newspapers, one question remains: what do cryptocurrencies mean for our modern financial system? Behind the speculative practices already common in stock markets, one can effectively wonder if cryptocurrencies are not posing a real challenge to the traditional actors of our financial system, such as banks, international organizations and states. The technical characteristics of the Blockchain technology behind the rise of cryptocurrencies effectively open avenues inconceivable in a world of fiat money. Minimally, cryptocurrencies offer new ways to store and transfer value. By doing so, they may limit the effectiveness of some tools employed by financial regulators and reinforce the power of private actors. In this context, this research note will reflect on the potential consequences of cryptocurrencies and their meaning for regulators around the world. After reviewing what's really new with the technology behind cryptocurrencies, we discuss how regulators have responded to the threats and opportunities it may pose. This allows us to point out some trends in the regulation of the growing digital economy.

*Both authors contributed equally to this paper.

1 Introduction

In financial circles, 2017 will go down as the year of cryptocurrencies. The dramatic upswing in their prices made them simply impossible to ignore anymore. In a matter of a few months they went from being only known by a small group of financial and technological enthusiasts to being on everyone's lips. This quick rise to prominence however did not only attract praise from political and economic observers. As cryptocurrencies now appear to be here to stay, it is important to question what do they actually mean for our modern financial system? In what way will they impact our economies and what does that mean for traditional actors like banks and states?

In this research note, we shed light on these questions by first reviewing the impact of the technology underlying cryptocurrencies. With all the buzz surrounding cryptocurrencies, there is many partial information going around. This unfortunately led to many wrong assertions being made in public debates. In order to establish a constructive reflection about the threats and opportunities posed by cryptocurrencies, we thoroughly review how the Blockchain technology works and how exactly can it affect our current financial system. Having done that, we discuss how regulators in different jurisdictions have responded to the rise of cryptocurrencies. This second part allows us to point out different trends that will probably be followed in the future.

2 Cryptocurrencies: in Tech we trust

Beyond all the hype and headlines, cryptocurrencies, or crypto-assets¹, mainly derive their value from their use of the Blockchain technology. To understand how the latter works, it is essential to go back to the first crypto ever created: Bitcoin.

¹The recent expansion of the cryptocurrencies market has seen the development of many diverse business models and concepts that do not pretend to act as currencies. The term "crypto-assets" was hence coined as an overarching term that includes both types of cryptos that aim to function as a currency (e.g. Bitcoin) and cryptos that do not. To avoid any confusion, the rest of this paper will simply talk about cryptos.

2.1 Bitcoin and the origins of Blockchain technology

The invention of Bitcoin, and concomitantly of the Blockchain technology, is broadly credited to the individual or group of developers behind the alias of Satoshi Nakamoto. While it is important to recognize that parts of the technological components are actually the achievement of the work of many academics in the 1980's and 1990's (Narayanan and Clark 2017: 38), the publication of the Bitcoin White Paper really laid down the ground for the development of the first electronic payment system without any central administration.

At its heart, Bitcoin is a decentralized open ledger which aims to remove the need of “trusted third parties to process electronic payments” (Nakamoto 2008: 1). The main objective driving Bitcoin, and most cryptos, is precisely to allow the safe transfer of information without any intermediate. For Bitcoin users, financial transactions are simply a form of information transfer, which do not need to be approved by a bank or any other central actor. As described in the White Paper, Bitcoin is a “chain of digital signatures” secured by cryptographic technology (Nakamoto 2008: 2).

To really understand how the technology behind Bitcoin can replace trusted third parties, it is crucial to look at one of its key components: Blockchain. Interestingly, the term Blockchain was actually never used and thus never defined in the paper of Satoshi Nakamoto. Blockchain can nevertheless be simply understood as “a database that contains all the transactions ever executed in the Bitcoin network” (Atzori 2015: 2). This record of all transactions is done through “linked timestamping”. The latter is a concept developed by computer-scientists, which means: recording a document at a given time in an open ledger that is observable by all. This is achieved by creating an evidence (or events causation) of this record without revealing its content (Bayer, Haber and Stornetta 1993).

In such a system, the security is derived from the impossibility to modify the information recorded on a Blockchain. For Bitcoin, this means that all transactions are irreversible. Once a transaction is recorded into the Blockchain, it is effectively almost impossible to reverse it. While this may be scary for everyday consumers, it is an essential feature for the system to work properly. It prevents the infinite duplication of digital coins and, concomitantly, the possibility for someone to double-

spend its money². While banks ensure that this does not happen in the current financial system, the open ledger and timestamping of the Blockchain technology do it in the world of cryptos. Despite its importance, Blockchain is however not enough to create value for cryptos. Two other features need to be mentioned to understand why cryptos can really have a disruptive impact for the economy: decentralization and proof of work.

One of the key element of Bitcoin is the decentralized nature of the open ledger that record all transactions in the network. All transactions recorded in the Blockchain are open for scrutiny by all participants. Instead of having a central authority, which owns the physical and virtual nodes of the network and creates private channels of communication for processing transaction, everything is open in Bitcoin (Pilkington 2015: 13). The channels for processing transactions are visible as well as the code behind them. As such, anyone in the network can check the validity of any transactions. Cryptographic functions are again employed to guarantee the inviolability of the system.

To describe shortly how the cryptographic technology works, transactions are being recorded along time, one after the other, following a linear pattern and in blocks of data all protected by a hash. A hash is a cryptographic algorithm impossible to revert. The blocks are moreover structured following a merkle tree as depicted in figure 1.

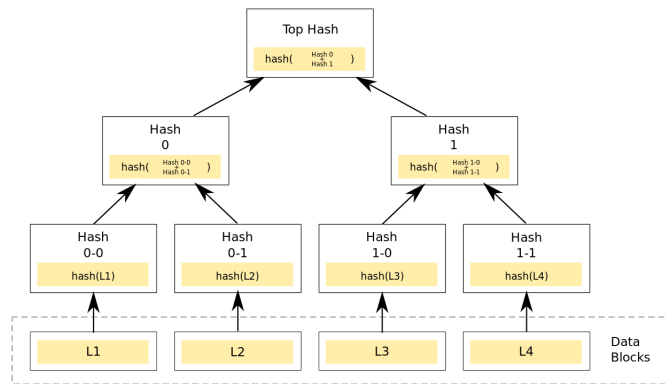


Figure 1: Example of Merkle Tree (illustrated by David Göthberg)³

²The “double-payment issue” was actually one of the main problem that Satoshi Nakamoto was trying to solve in its White Paper.

³Image retrieved from Wikipedia on May 24th, 2015: https://en.wikipedia.org/wiki/Merkle_tree.

In short, this merkle structure signifies that each parents blocks are divided in children blocks also containing their own hash. The hash of the parents are the digest of the children (Narayanan and Clark 2017: 39). This technically means that if you know the hash of the parent block of data, it is possible to obtain the information from all its children blocks. Moreover, any changes to the information in a previous block (transactions in the case of Bitcoin) would have to alter the entire tree. This makes changes particularly difficult and information easy to access even when only knowing the latest transaction. Lastly, it must be mentioned that a nonce, an arbitrary 32 bits' number, is added in each block and used to solve the mathematical puzzle behind the hash. This is illustrated by figure 1 below.

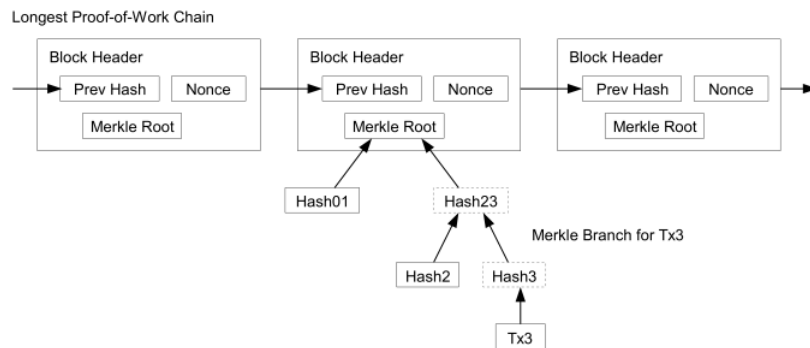


Figure 2: Longest Proof-of-Work Chain (Nakamoto 2008: 5)

Besides the innovative features of blockchain and the decentralized nature of Bitcoin, one important question remains: why should people invest in making this system work beyond the fact they could use it too? In effect, Bitcoin can only function if some people accept to spend their computing power to solve the mathematical puzzles allowing new transactions to be added to the blockchain. In other words, for Bitcoin to work, there must be people offering their computers to validate the transactions of others.

Proof of work (PoW) is the economic incentive behind it. It encourages certain participants of the Blockchain not transferring money to instead “mine blocks”⁴. By mining, they try to solve the mathematical puzzles behind the hash protecting the

⁴The expression of mining was adopted in reference to people who used to mine to find value in gold or other precious metals. In effect, miners are currently mainly paid by receiving new Bitcoin. It is however important to note that they are also receiving a transaction fee, which will remain their sole source of revenue after all bitcoins will have been emitted in 2140.

integrity of the Blockchain. In the event that they succeed and find the value corresponding to the cryptographic hash of a transaction block, they are rewarded with the token of the cryptocurrency they are mining for (e.g. Bitcoin). The system continues with the validation of the first block, followed by the mining of another block, which is the signal for the record acceptance of the first block in the Blockchain (Nakamoto 2008: 3).

The emphasis put on miners as validators and extractors of value runs however the risks that some of them turn “rogue” and attempt to hack the system by validating false transactions for their own benefits. To prevent this scenario, the system plan that for a block to be validated or reverted more than 50% of the central processing unit (CPU) power of the entire network is necessary to alter the code. The whole Proof-of-Work process will have also to be done to revert the older transactions (Nakamoto 2008: 3). This is not without a cost as the more time is spent in the mining process and block addition, the harder and more expensive it becomes to revert it. In the end, a full-scale attack of the honest chains would bear such a cost that it would remove all profits incentives to go “rogue”.

The structure of Bitcoin just described laid out all the premises at the foundation of our current understanding of Blockchain. That being said, since the publication of the Bitcoin White Paper by Satoshi Nakamoto, the industry has considerably evolved and several debates have emerged, such as on anonymity/pseudonymity and centralization/decentralization. The next section will review these at greater length before looking at the regulatory responses that rise of cryptos have attracted.

2.2 The Crypto Industry and its Debates

Contrary to common belief, Bitcoin is not anonymous. It is rather a pseudonym based system. Users’ identity is created by emitting a public key, composed of a list of numbers and letters which serve as an address to send or receive funds. However, as it is a decentralized system, all transactions under this key are open for scrutiny from everyone in the network. It is hence theoretically possible by recouping data to identify who is behind an address. It would obviously be impossible to know it for sure, but it is a possibility. These flaws in the Bitcoin system have led to the development of cryptos, such as DASH and Monero, which are specifically designed

to guarantee the anonymity of the users through various technological features of their respective Blockchains. This is notably done by splitting transactions.

Moreover, in most crypto projects, including Bitcoin and Ethereum, the programming code is chosen through a consensus protocol. This means that programmers can put forward new lines of code to improve a specific Blockchain, but they will not be able to force anyone to actually use it. This is an essential characteristic of the decentralization feature at the core of the agenda of most cryptos. It remains that certain nodes or individuals dispose of a larger influence than others such as Vitalik Buterin, co-founder of Ethereum. Some cryptos have also deliberately decided to adopt a centralized strategy in order to facilitate cooperation with existing financial institutions. An instance of this strategy is Ripple (XRP)⁵, which was specifically designed to facilitate payment within the preexisting payment structure to *de facto* compete with previous established player (e.g.: SWIFT).

Other challenges which have prevented the massive adoption of cryptos are the costs and time of transactions. As seen in Figure 3, the average transaction fee peaked in December 2017 as more and more people wanted to buy Bitcoin. Such shortages are however to be expected with the introduction of a new technology and the rush of attention that Bitcoin got in the space of a few months. Moreover, technological ongoing improvements such as the development of the Lightning Network⁶ by Bitcoin developers and sharding⁷ by Ethereum’s co-founder, Vitalik Buterin, have the potential to solve this issue in the long term and build the necessary infrastructure for accommodating large number of users. This simply reminds us that we are only still at the beginning of the history of cryptos.



Figure 3: Bitcoin Average Transaction Fee (USD), bitinfocharts.com

⁵For more information on Ripple, see: <https://ripple.com/insights/the-worlds-biggest-banks-lead-the-Blockchain-charge/>

⁶For more information about the lightning project, see: <https://lightning.network/>

⁷For more information about the sharding project, see: <https://medium.com/prismatic-labs/how-to-scale-ethereum-sharding-explained-ba2e283b7fce>

The energy consumption is also a recurrent criticism addressed to Bitcoin (Böhme et al. 2015: 214) and the crypto industry as a whole. With the rise of interest in crypto markets, this issue actually became so important that Bitcoin was often accused of becoming an issue for sustainable development and climate change. The high energy consumption rate is a consequence of the PoW consensus system, which required a large amount of computing power and hence electricity. While this issue remains prominent, propositions to switch from a PoW to a Proof-of-Stake system (PoS) may contribute to solve this challenge. The main difference from PoW is that in PoS the miner is not chosen by solving a mathematical puzzle but rather on the amount of wealth (number of token) he puts at stake. His incentives to do so is not derived from mining blocks but rather to collect transaction fees from validating transactions. In the event that he would turn “rogue” and start validating false transactions, he would be punished by the network by losing parts or the entirety of the stake that he put into the network. It is hence in its interest to remain loyal. This new system should significantly reduce the amount of electricity needed for the system to work. This change could also be quickly adopted, contrary to what some people think, as Vitalik Buterin, co-founder of Ethereum (ETH), for example already announced the roadmap of ETH toward partly switching to a PoS system⁸.

Interestingly, despite that crypto and sustainable development are often seen in opposition, they may actually play a complementary role in the near future. Contrary to most economic activities, crypto mining does not need to work during energetic rush time and look for places with cold temperature and the lowest electricity prices. An agreement can be found with providers of sustainable source of energy which often suffer from the limitation of batteries and the irregularity of their supply (i.e.: solar exposition and wind). As crypto do not have the same requirements than most energy consumers, such as factories, public utilities or households, a differentiated sequential supply of energy would not be problematic. This kind of synergies between the two sectors could enable the creation of decentralized industrial/energetic clusters, where supply of renewable energy would be financed by crypto companies. For the latter, this combination would guarantee their electric supply at low cost.

Beyond technical elements, it is necessary to look at the future impacts that crypto may have in political economy. Its implication is not benign as it clearly

⁸For more information see: <https://www.coindesk.com/ethereums-big-switch-the-new-roadmap-to-proof-of-stake/>

touches on certain key competences of states, especially in monetary policy. Among the vast majority of the crypto companies, the emission of token is limited. Only a certain amount of token can hence be created. For example, there will never be more than 21 millions Bitcoin on the market. This feature makes these assets fundamentally de-inflationary over time with a constant increasing demand curve. As the prices rise, no authority can decide to compensate it by creating suddenly more tokens. One of the long term consequences is that this class of assets can be particularly attractive for a large strand of actors as their values cannot be subject of devaluation policy from central banks.

The recent case of Iran is exemplary. More than 2,5 Billions USD were moved outside the country using crypto, following the USA denunciation of the nuclear disarmament treaty⁹. In the near future, central banks will not have the same leeway to proceed through re-structuration plans, such as during the Euro crisis in March 2013 with the levy imposed by the Troïka (EU, ECB, IMF) on deposits over 100'00 Euro in Cyprus Banks. Bank accounts' holders and investors could in the future resort to crypto as an insurance investment in case of a similar major crisis, as witnessed in 2008 and in Europe in 2011.

Furthermore, the role of banks for investment loans and initial public offering (IPO) will also be severely affected in the future. Instead of going through major financial institutions to raise capital by emitting stocks, technological companies will have the opportunity to go through initial coin offering (ICO)¹⁰. By issuing coins rather than stocks, voting power do not leave the company and IPOs banking fees are saved, rending the operation even more profitable. ICOs, when opened to the public, allowed a larger public to invest by buying coins, without required minimum amount due to the divisibility of a token. The smallest unit of a Bitcoin is for instance 1 Satoshi, which correspond to 0,00000001 BTC. An ICO well publicized can hence create a hike of the price and increase the use of the token, which will make the company even more profitable.

But, this all lead to another question: what are the uses of coins or tokens? The token will often, although not in all cases, be the mean through which the services

⁹For more information, see: <https://cointelegraph.com/news/iran-sanctions-citizens-use-crypto-to-move-25-bln-out-of-country>

¹⁰Far from being hypothetical, many companies have already started to do so in the last couple of years.

could be accessed. In fact, in order to purchase the technological service of a specific company, a consumer will have to use the related token to do so. While the coins' value are currently often derived from speculation in exchange platform, in the long run the prices will be linked to the use rate of a coin. This explains partly why certain coins run such a high pike of prices, as some investors are speculating that this specific coin will become a key component of the new crypto economy.

In terms of services provided, they ranged from assuring transparency in the supply chain, renting CPU power, to making certain current financial assets more liquid and tradable such as airlines miles or supermarkets fidelity points. This is also another reason why decentralization and transparency are so important for cryptos and Blockchains. This allows them to be interoperable. Without it, they would lose crucial share of the value created by these technologies. Noteworthy, the interoperability of cryptos could also empower consumers and increase their purchasing power. Indeed, consumers would be able to sell the service's token they do not need anymore, to buy the one that they currently want, all of that without any bottlenecks. Transparency play the role of safeguards in this system, assuring that everyone benefits similarly from the same service's access and token supply.

This closes our section on Bitcoin and the crypto industry. The next section will dive deeper into the global regulatory answers that emerged from the rise of this new sector and discuss its divergences and consequences for the global and domestic economic system.

3 Regulatory responses

The rise in popularity of cryptos obviously did not go unnoticed in governmental offices around the world. If 2017 was the year where cryptos prices burst, 2018 could well be the year of their regulation. In effect, multiple agencies around the world have started to look at how they can regulate crypto markets. As of now, regulatory responses have however been mixed. While some governments have adopted a positive stance towards cryptos, many have held that they represent a systemic threat to the global economy. In the rest of this paper, we discuss how different states have thus responded to the impact of cryptos on their monetary sovereignty and their financial markets.

3.1 Monetary sovereignty

One of the first concern for states arising from the development of cryptos was obviously related to their monetary sovereignty. In our modern economic system, states hold the exclusive power to print banknotes and mint coins. In practice, private banks play an important role in the creation of money, but states remain at the heart of this process. Cryptos, and chiefly Bitcoin, however reminded us this not need to be so.

As a side note, it is worth keeping in mind that cryptos are far from the first attempts to create non-governmentally backed currency. In recent years, there was notably a surge of interest in “local currencies”. The latter are developed in small-geographic area to foster local economic activities. The obvious difference with cryptos is that they can reach a much broader audience by using cryptography to solve the trust issue between its users. Bitcoin is a prime example in that respect as it is now traded all over the world.

It is precisely this capacity of cryptos to be used on a large scale, which pose a real threat to state’s monetary sovereignty. Unsurprisingly, many states thus reacted quite negatively to the idea that cryptos could be used as an alternative to their national currencies. Regulators in the US¹¹, the UK¹² and the EU¹³ notably clearly affirmed that cryptos were not legal tender and were nowhere near to be equivalent to their national currencies.

While regulators in most countries have followed the leadership of these three jurisdictions, some have adopted a different stance. Japan, for one, has adopted amendments to its Payment Services Act, which consider that some cryptos can be considered as methods of payment¹⁴. As indicated by Yuzo Kano, head of the Japan Blockchain Association, this does not mean that Bitcoin or other cryptos have

¹¹As early as 2013, the U.S. Federal government through one of its agencies maintained that cryptos were not real currencies (U.S. Federal Department of Treasury’s Financial Crime Enforcement Network 2013).

¹²This year, Mark Carney, Governor of the Bank of England, recalled that “only sterling is legal tender in the UK” (2018: 6).

¹³In response to the project of Estonia to create its own crypto, Mario Draghi emphasized that that the euro is the only currency of the Eurozone in a press conference (2017).

¹⁴An english summary of the amendments can be found on the following website: <https://www.dlapiper.com/en/japan/insights/publications/2017/12/japan-regulatory-update-on-virtual-currency-business/>

acquired the status of legal tender¹⁵. As such, no sellers are obliged to accept a payment in cryptos. Yet, the recognition of cryptos as a legal method of payment helped the adoption of payment in Bitcoins by many retailer stores in Japan.

Other countries went even further by starting to develop their own cryptos. As of now, Venezuela is the only one to have officially launched one (the Petro), but others like Russia¹⁶, China and Estonia have shown interest in doing the same. For Venezuela and Russia, their support for cryptos clearly follows their desire to undermine the hegemony of the US dollar. In the midst of an economic crisis, the launch of the Petro by Venezuela was notably a way to circumvent American sanctions and get an influx of foreign capital. More recently, in the midst of the American decision to review, and in the end exit, the nuclear deal, the Iranian government maintained that it was also looking into the possibility to develop its own crypto. With the threat of facing new economic sanctions hanging on over their head, this is a clear attempt to circumvent them as Venezuela tried to do. It remains to be seen how effective those state-backed cryptos will be in doing that in the long term, but it is interesting to note that they might limit the structural power that the US held with the domination of the US dollar since the end of the Second World War.

Meanwhile, in China, there is both an interest in the economic potential of cryptos and concerns over their possible impact on the current financial system. China particularly dislikes the idea of a currency not backed by a government as it can ease fraud, capital outflows, tax evasion and, perhaps most importantly, secrecy. As a result, China has banned the sell and purchase of cryptos on its territory. At the same time, they view quite positively the capacity of cryptos to ease the development of mobile payments and thus significantly reduce transaction costs. The People's Bank of China (PBOC) went as far as running tests to launch its own crypto. Chinese authorities have however indicated that the introduction of a Chinese's crypto will only be done when they will be sure that it would not entail excessive speculation. For now, stability and state control are thus the two main imperatives for the Chinese government.

¹⁵For his analysis of the most recent Japanese amendments to its Payment Services Act, see: <https://www.coindesk.com/japan-new-heart-bitcoin/>

¹⁶Reports indicate that Russia helped Venezuela to develop the Petro.

Estonia has finally been keen to complete its e-residency project with the development of a crypto ('Estcoin')¹⁷. In effect, the Estonian government strongly believes that the future of its economy depends on its ability to harness the power of digital technology. As a member of the Eurozone since 2011, Estonia was however sharply criticized by Mario Draghi, President of the European Central Bank, for trying to develop what he perceived as a rival currency to the Euro. Since then, the leader of the Estcoin project has held that the aim is not to develop an alternative currency to the Euro, but mainly to allow companies to raise funds digitally¹⁸. Yet, it is unclear what would happen if Estonia launched its crypto.

Apart from these reactions, the rise of cryptos however did not lead to major (if any) changes in the monetary policy of most states. This is mainly due the fact that cryptos still unsatisfactory fulfill the basic tasks of money. As Mark Carney recalled in its recent discussion on the future of money, money should generally serve as a store of value, a medium of exchange, and a unit of account (2018: 3). As of now, cryptos' volatility and lack of critical mass however impede them from doing any of these effectively. The development of new technology and procedures (e.g.: sharding or proof-of-stake) might well change this, but for now cryptos are actually more investment assets than real currencies. Concomitantly, it also explains why most states' regulatory responses were directed towards financial issues raised by cryptos as discussed in the next section.

3.2 Financial regulation

Despite their current limited capacity to act as currencies, cryptos have increasingly been perceived as legitimate assets. To be clear, many cryptos remain highly speculative and risky investments. The possibility of making significant profits and the future transformative potentials of the underlying technologies have however attracted the attention of several mainstream investors. This rise in importance of cryptos even led Deutsche Bank to list a Bitcoin crash as a significant threat for the global economy in 2018.

¹⁷For more information about the Estcoin, see: <https://medium.com/e-residency-blog/estonia-could-offer-estcoins-to-e-residents-a3a5a5d3c894>

¹⁸For his entire statement, see: <https://medium.com/e-residency-blog/were-planning-to-launch-estcoin-and-that-s-only-the-start-310aba7f3790>

As the capitalization of all cryptos still represents less than 1% of global GDP, it is hard to see them as posing a real threat to the stability of the financial system (Carney 2018: 9). Yet, it is inescapable that the decentralization and pseudonymity features of cryptos like Bitcoin make them great tools for money laundering and the financing of illegal activities. Additionally, cryptos pose serious questions of tax evasion and consumer protection. The mostly unregulated nature of crypto trading has notably eased the apparition of scams. Faced with all these issues, governments around the world have again diverged in their policy responses. The latter can however be summed up in three general approaches.

First, some states simply found the gains were not worth the risks. China is a leading example in that respect. As briefly mentioned in the last section, the Chinese government decided to ban crypto exchanges in 2017. As a result, China went from one of the most important crypto market in the world to one of the less in the space of a few months. It is very difficult to assess such changes as we cannot in practice know from where crypto traders come from, but we can still get a good idea by looking at which fiat money is used to buy cryptos. As shown in Figure 4, the share of cryptos bought in Yuan dramatically fell in the course of 2017.

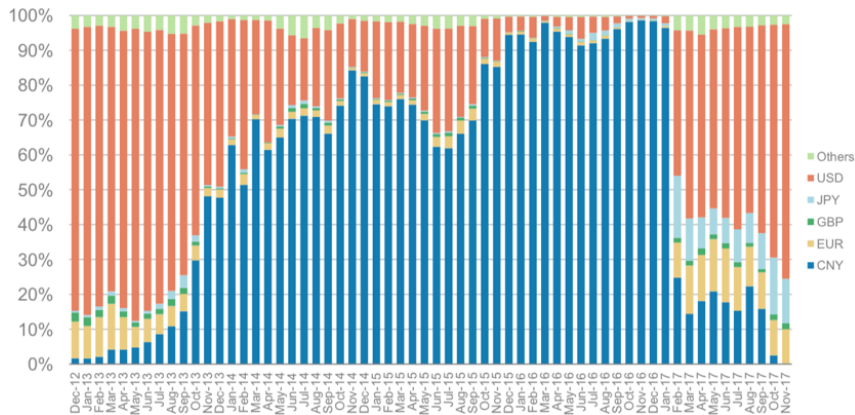


Figure 4: Bitcoin/fiat trade composition by currency (Morgan Stanley Research 2017)

This entire crackdown actually started when the PBOC opened an investigation to see if crypto exchanges had served to finance illegal activities. Again, it is clear that China dislikes the idea of a system which allows private actors to circumvent its rules. Instead of taking any risks, they thus decided to limit as much as possible cryptotrading. As of now, China has probably adopted the most severe attitude towards the financial risks posed by cryptos. Recently, India joined China in its

suppression of cryptos trading as its Reserve Bank prohibited any entities coming under its purview to offer any form of services to entities dealing cryptos. While it does not mean that crypto trading is banned, this puts a serious constraint on Indian crypto exchanges as they won't be able to use the service of any financial institution from India.

A second approach is not as prohibitive, but still try to limit the impact of cryptos by applying to them the current legal framework. It is probably best exemplified by the approach of the United States. Since China decided to crackdown on crypto trading, the United States have been one of the biggest crypto markets in the world as depicted in Figure 3. This high interest of investor in cryptos unsurprisingly attracted the attention of American regulators. Rather than developing new rules, federal agencies however tried to see how cryptos could work under the purview of the current system. This approach is partly due to the American view that governments should only play a minimal role in the economy and partly because American regulators are still unsure how to approach cryptos. In this context, the main question that American regulators have for now tried to answer was about the legal nature of cryptos.

Traditionally, financial products are divided in two main categories: commodities and securities. While definitions may vary in different jurisdictions, a commodity is generally understood as a good with an intrinsic value (i.e.: gold, silver, oil, wheat, foreign currency, etc.) and a security is a financial instrument showing ownership (i.e.: bond, share, etc.). The importance of the qualification of cryptos according to these two categories is that both are not regulated the same way. In the United States, exchanges selling commodities and securities notably do not have to register with the same federal agency and follow the same precautionary rules. Gains from commodity or security investments are also taxed differently.

While this approach of applying the current legal framework is not without interest, the problem is that it can be difficult to actually implement. The mixed nature of cryptos most notably make them quite hard to categorize. This appeared quite clearly in a recent Senate hearing of the Banking committee where both Chairman of the Security and Commodity Commission maintained that cryptos fell under their

jurisdiction¹⁹. This ambiguous situation creates an opportunity for crypto exchanges and new cryptos to simply not follow the rules of any system. As a matter of fact, in the above-mentioned senate hearing, the Chairman of the Security Commission indicated that no exchanges ever registered with them for the sale of cryptos.

A third approach adopted by some countries tries to fill this hole by developing new rules to govern the trade of cryptos. Canada, Japan, Switzerland and Malta have been leading the way in that respect. Interestingly, Canada was the first country to adopt official rules for cryptos when amending the Proceeds of Crime (Money Laundering) and Terrorist Financing Act in 2014. The amendments actually simply added that crypto exchanges were also obliged to follow this Act²⁰. This still has major implications as it forces both exchanges established in Canada or dealing with Canadian customers to register with the Financial Transactions and Reports Analysis Centre of Canada and implement an anti-money laundering program. Practically, this means that exchanges have to report suspicious or terrorist activities, report large transactions, verify the identity of its customers, keep digital records of their activities and perform risk assessments. Lacking from this new law is however a definition of crypto.

Japan adopted amendments to its settlement act to also regulate cryptos as mentioned in the last sub-section. Rather than focusing on the money laundering and financing of terrorism issues, the new legal provisions of the Japanese Law were focused on protecting crypto investors. In addition of being obliged to register with Japanese authorities, crypto exchanges must notably take measures to protect their customers' money and privacy. They must also take steps to ensure that no customers confound cryptos with 'real' currencies. This focus on customer protection clearly reflects the fact that Japan was the theater of the bankruptcy of one of the first and largest Bitcoin exchange, Mt. Gox, in 2014.

Switzerland is nowadays eyeing to become the "land of crypto". As such, Swiss regulators have been in the process to develop clear regulations to attract investors in cryptos since 2017. While Switzerland has yet to adopt a new law, its Financial

¹⁹For detailed information about the hearing, see: <https://www.banking.senate.gov/hearings/virtual-currencies-the-oversight-role-of-the-us-securities-and-exchange-commission-and-the-us-commodity-futures-trading-commission>

²⁰For full amendments to Bill C-31, see: <http://www.parl.ca/DocumentViewer/en/41-2/bill/C-31/third-reading/page-347#38>

Market Supervisory Authority (FINMA) published in February 2018 guidelines for the introduction of new cryptos on exchanges based on its territory. These guidelines give clear indication on how to categorize cryptos and to apply Swiss financial law accordingly. Promoters of new cryptos will notably have to provide the Swiss authorities with various information about their project, including their names, the name of their organization and their partners, the key dates and deadlines, the investors' rights and obligations, etc. As opposed to the approach United States, which also focus on applying the preexisting laws, investors currently have much more certainty in Switzerland.

More recently, Malta also joined the race to attract crypto investments by adopting friendly regulations. More precisely, it plans to adopt three laws aimed at providing legal certainty for crypto exchanges and crypto promoters. While the texts of the final laws have yet to be public, they already had an impact on the crypto ecosystem by leading major exchanges, such as Binance, to relocate their head office in Malta. This contrasts with the adoption of the Bitlicense regulation in 2015 by New York lawmakers²¹, which led exchanges to stop offering services in the state of New York altogether. For many new or small developers, this state regulation was seen as too burdensome and costly. As global regulators are trying to set limit on the development of cryptos, this example highlights the difficulty to do so in a fragmented regulatory system. This is especially the case for economic sectors, which can quickly delocalize their activities, such as digital financial services. The important digital aspect of crypto exchanges should however not blind us to the fact that these companies might not always move as easily as they want. More precisely, the bigger an exchange will be, the more it will have a physical presence (computer, servers, employees, offices, etc.) which will limit its capacity to move easily.

To sum up, we found that three different approaches were adopted by states globally. Some, like China, simply preferred to impede any trading in cryptos from occurring at the moment. Others, like the US, tried to apply their current legal framework to this new phenomenon²². Finally, a few went further and adapted their laws to limit the risks posed by cryptos. While different, all these new regulations

²¹Even though the U.S. Federal government has yet to adopt a law, New York lawmakers quickly did so as New York status as one of the main financial hub led it to similarly be one of the first crypto hub.

²²As indicated, this federal approach however did not stop state like New York to do adopt new regulations.

have one important element in common. They all focus on intermediary actors, and mainly crypto exchanges. We can obviously expect that this trend will go on in the years to come. In an increasingly decentralized and digital world, it is effectively safe to assume that states will focus their regulatory reactions on actors who act as intermediaries between different systems (financial or others). This actually mirrors the tendency of states to hold liable Internet service providers, which act as important intermediaries between the Internet and the material world. At the same time, the digitization of financial services certainly makes them more difficult to regulate as private companies can threaten regulators to leave unfriendly regulatory space. Global rules are obviously one way to solve this issue, but it is definitely unrealistic to think that such rules could be adopted anytime soon. Competition and diverging interests appear to be simply too strong for a broad consensus to emerge.

4 Conclusion

Throughout this research note, we attempted to present an accurate picture of the crypto industry, from its technological origins to the most recent regulatory responses of states. As seen, the birth of Bitcoin was a founding moment of new industry. It set the stage for the development of all the cryptos which appeared in the last couple of years. At the same time, the Bitcoin White Paper did not solve all the issues. The technology behind cryptos still has to be improved to allow its adoption by a critical mass of consumers. Some features, such as the necessary degree of centralization or decentralization of cryptos, are also still heavily debated. As the technology will evolve and resolve its issues, it is clear that cryptos will have an increasingly disruptive impact on the global economy. This fact actually starts to be well understood in the capitals around the world. Regulatory activities on crypto are rising everywhere, motivated by both the monetary and financial implications that this new technology could have in our global economic governance.

While, it is still early to distinguish pure short-term speculation from sound investment, the near future will certainly be very informative on the relations between technological innovations and our economic systems. Indeed, it will be of great interest to see if the regulatory and policy capacities of states will be increasingly constrained by these technologies that certainly challenge their sovereignty. There clearly remains the possibility that they successfully adapt their framework to accommodate these

new economic players, but they could also significantly lose influence. Similarly, it will be fascinating to see how established private actors, such as banks, will react to the arrival of these new challengers. Will market structure evolve or will the oligopolistic patterns typical of the technological industry repeat itself? All these questions are crucial for crypto as well as for other technologies. This is why any study on these subjects must combine not only good technical knowledge but also sound understanding of social actors and institutions. In the end, technology is nothing without humans.

5 Bibliography

- Atzori, Marcella. 2015. “Blockchain Technology and Decentralized Governance: Is the State Still Necessary?” *SSRN Electronic Journal* pp. 1–37.
- Bayer, Dave, Stuart Haber and W. Scott Stornetta. 1993. Improving the Efficiency and Reliability of Digital Time-Stamping. In *Sequences II: method in Communication, Security and Computer Science*. pp. 329–334.
- Böhme, Rainer, Nicolas Christin, Benjamin Edelman and Tyler Moore. 2015. “Bitcoin: Economics, Technology, and Governance.” *Source: The Journal of Economic Perspectives Journal of Economic Perspectives—Volume 29(2—Spring):213–238*.
- Carney, Mark. 2018. “The Future of Money.”. Inaugural Speech at the Scottish Economics Conference.
URL: <https://www.bankofengland.co.uk/-/media/boe/files/speech/2018/the-future-of-money-speech-by-mark-carney.pdf>
- Draghi, Mario. 2017. “Press Conference on the Eurosystem.”.
URL: <https://www.ecb.europa.eu/press/pressconf/2017/html/ecb.is170907.en.html>
- Morgan Stanley Research. 2017. “Bitcoin Decrypted: A Brief Teach-in and Implications.”.
URL: <https://fa.morganstanley.com/robert.emple/mediahandler/media/113362/BitCoin\%20Blockchain\%20MS\%20paper.pdf>
- Nakamoto, Satoshi. 2008. “Bitcoin: A Peer-to-Peer Electronic Cash System.”.
- Narayanan, Arvind and Jeremy Clark. 2017. “Bitcoin’s Academic Pedigree.” *Communications of the Acm* 60(12):36–45.
- Pilkington, Marc. 2015. Blockchain Technology: Principles and Applications. In *Research Handbook on Digital Transformations*, ed. Xavier Olleros and Majlinda Zhegu. Edward elg ed. pp. 1–39.
- U.S. Federal Department of Treasury’s Financial Crime Enforcement Network. 2013. “Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies.”.
URL: <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>