The Future of Decentralized Digital Currencies and its Potential Impact on the Transaction Process in the Canadian Market

Matthew Muriithi from University of Toronto

& Limei Chen from University of Toronto

under supervision of Wayne S. Cheng

Date: December 5th, 2021

Table of Content

Executive summary

After doing research on the original topic, “the future of Digital Currencies and its potential impact on doing business in the future”, we found it too wide to provide comprehensive details. Hence, with deliberate consideration, we narrowed down the scope to decentralized digital currencies and we decided to focus on its impact on the transaction process in the Canadian market.

This paper discusses the future of decentralized digital currencies and its potential impact on the transaction process in the Canadian market from three perspectives: banks, consumers (and vendors), and cash-in-transit which refers to the underlying middle state that exists between banks and consumers (as well as the technologies that underpin this state). As our goal is focused on the transaction process, it is fitting to analyze the impact of cryptocurrencies on the key players in such process, which is consumers (& vendors) and banks, and the underlying technology that facilitates such a transaction process. For each implication, the benefits and risks are analyzed with potential solutions.

Decentralized digital currencies are both a threat and an opportunity to banks, with the potential value of providing services involving cryptocurrencies outweighing the risks (where the risks may be mitigated to an extent). Such currencies also provide great value to consumers, with the risks of switching from traditional central bank issues fiat currency eclipsed by the value that decentralized digital currency offers. Through their existence on a blockchain, a decentralized ledger that itself carries its own risks and benefits, and all the players in the transaction process in the Canadian market stand to realize the terrific value by including cryptocurrencies in the transaction process.

In conclusion, we believe that it is an inevitable trend that decentralized digital currencies will be adopted in more places. By implementing potential solutions to its risks, all parties involved in the transaction process will be able to benefit from it.

In the end, we also include a comparison table to better present the differences between decentralized digital currency and traditional fiat currencies.

Introduction

What are digital currencies? Digital currencies refer to currencies that exist in an electronic format with no physical form, although they are virtual, they share the same properties as that of physical currencies (albeit in an electronic format). Centralized forms include the issuance of currency and virtual currency (e.g., in game currency) by the central bank, although one may argue that decentralized digital currencies are potentially the most exciting in terms of their use-cases and disruptions.

Decentralized digital currencies are also known as cryptocurrency. They are decentralized as they are an application of blockchain technology. A blockchain is a decentralized distributed database that is secured with cryptographic protocols. It utilizes a ledger that tracks transactions, storing a full copy of the ledger among computers that agree to be part of the

network. Transactions that happen in the same timeframe are grouped together into *blocks,* with each block referencing the previous block (i.e., transactions that happened earlier), forming a chain of transactions (hence, the name *blockchain*). Any computer can join the network, and computers on the network are referred to as nodes. The blockchain uses the computers on the network to secure the network through consensus mechanisms, with the most common one being *proof-of-work*. Consensus mechanisms are the method by which computers on the blockchain agree on a single state of the network, and consensus must be reached after each transaction by at least 51% of computers on the network. Reaching consensus through a given consensus mechanism is known as *mining*, and computers that mine receive rewards as an incentive.

Cryptocurrency was invented by Satoshi Nakamoto (whose real identity is still unknown) with his creation of the first cryptocurrency Bitcoin. In 2009, Bitcoin became public to all Internet users (Marr, 2017). Nowadays, there are more than 10,000 types of cryptocurrencies in the world, and some popular cryptocurrencies besides Bitcoin are Ether (often known by its underlying blockchain Ethereum), Dogecoin and Litecoin.

Zooming into Canada, Canada is the first country which approves exchange-traded fund tracking Bitcoin, and the Purpose Bitcoin ETF (ticker BTCC) started trading in Toronto in 2021 (Potter, 2021). Though cryptocurrency is not the legal tender in Canada, some retailers have started to accept Bitcoin as a way of payment. With more prevalent use of decentralized digital currencies, we would like to discuss its impact on the transaction process from the perspective of banks, consumers (and vendors), and cash-in-transit which refers to the underlying middle state that exists between banks and consumers.

Implication on banks

- **Benefits**

Cryptocurrencies and their underlying blockchain allow for transfers of large sums to occur at a faster rate than traditional bank transfers, especially for international transfers. In *Figure 1*, we see the transaction time of remittance and fees of different methods, based on data on transactions from the United States to other countries in 2017 (World Bank). Remittance refers to the transfer of money abroad. For figure 1, a sample of 1800 payments was taken, and was compared to how long it would have taken for those same payments to be done using various cryptocurrencies and their underlying blockchain. Western Union, a common method of sending money abroad, has a transaction time of 3-5 days on average. Bitcoin, currently the top ranked cryptocurrency by market cap, takes an average of 1.3 hours. Ether, the second ranked cryptocurrency by market cap, takes an average of 6 minutes. Banks can utilize cryptocurrencies and the underlying blockchain technologies to provide a service of fast international transfers to their consumers.

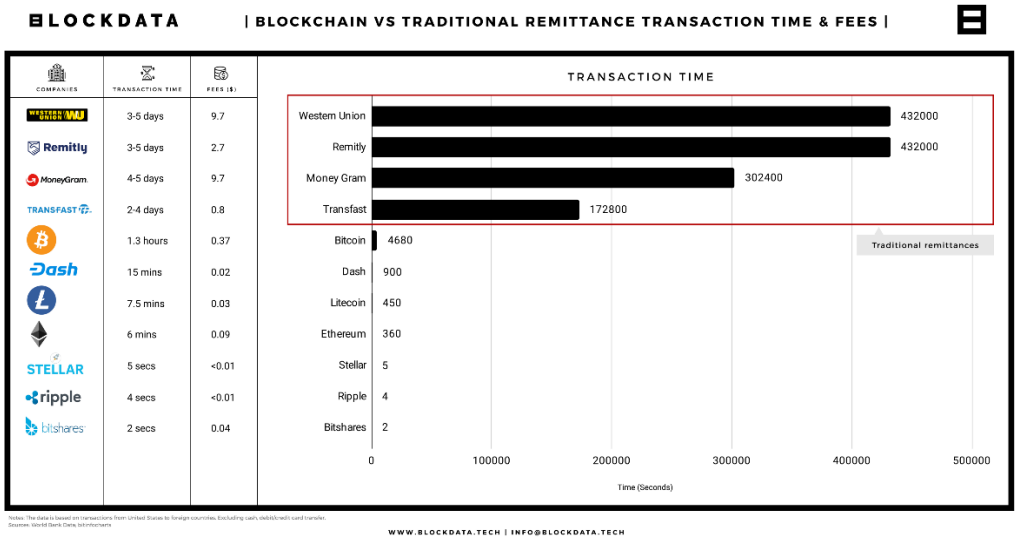

Figure 1: Transaction time of remittance for different transaction methods

As cryptocurrencies lie on decentralized platforms, there is less reconciliation and errors made. There is always a clear immutable trail.

Clearing and settlement systems allow banks to do payments with other banks safely and securely. Clearing and settlement systems are also required in all payment transactions that banks are involved in. Clearing refers to the act of updating accounts between two parties for the transaction that will take place, and happens before money has been exchanged (e.g., the settlement). Settlement refers to the actual transfer of monetary value (in this case, fiat currency) from one account to another.

The Automated Clearing Settlement System (ACSS) manages the payment system in Canada, and it is the mechanism by which all retail payments must be cleared (Bank of Canada, n.d.). Settlements happen overnight, which means that even though money is being credited and debited on a customers account, no real monetary value is exchanged until settlement happens. However, by making use of the underlying blockchain technology, cryptocurrency transactions make it possible for both the clearing and the settlement happen at the same time. The cost of banks' independent crediting and debiting accounts, which have to reconcile with each other, is eliminated, and funds are transferred in from a couple of seconds to a couple of minutes. Banks also pay interests on these payments, and cryptocurrency could let banks avoid the interest payments.

- **Risks**

Supporting and providing a platform for digital currencies may expose banks to more risk. Banks in Canada are compelled by law to abide by Canadian sanctions, which include UN resolutions and often are aligned with the resolutions of key allies around the world, such as the United States. This means that banks would have to deny transactions that involve

sanctioned parties, or freeze the assets of clients that have been sanctioned. If banks were to provide services involving cryptocurrencies, they would be much more limited. Wallet addresses are pseudonymous, meaning that banks facilitating the sending of cryptocurrency to some public addresses may violate individual sanctions if the owner of that address is sanctioned. Although banks may track public transactions of the given destination address on the blockchain to infer the identity, any individual may have a virtually unlimited number of addresses. This is especially problematic if there is no transaction history for an address that the bank is sending cryptocurrency to, as there is no method to infer the identity of the owner, providing true anonymity.

For numerous banking services, banks may lose out on fees that they typically receive. The value proposition of banks lies in their ability to be a trusted middleman in financial transactions. Cryptocurrencies and their underlying blockchain technologies are decentralized. By having a public ledger, they essentially take out the middleman. The utility provided by digital currencies can decrease the value proposition of a traditional bank, or rather require a bank to radically transform what services they offer. For example, the fees that are involved in transferring money using cryptocurrencies are mining fees, which is also called gas fees, and it depends on network congestion. In contrast, bank transfers usually involved higher fees.

- **Potential solutions**

Although decentralized digital currency, also known as cryptocurrency, challenges banks and their role as centralized institutions in payment systems, banks should leverage their position to combine the value proposition they offer as a centralized institution with the value that comes from the decentralized nature of cryptocurrency.

As centralized institutions, banks are trusted by their customers. Banks that hold deposits in cryptocurrencies with the underlying blockchain technology is using a proof-of-stake consensus mechanism. This can stake a portion of the depositors' cryptocurrency and keep for themselves the gas fees that they earn.

Furthermore, the security of the blockchain would improve with the addition of large institutional players like banks. Banks may have the resources to add computational power to the blockchains of cryptocurrency they hold, which follow a proof-of-work consensus model. This will allow them to reap gas fees while securing the underlying blockchain.

Banks can simply mandate that the public addresses of people receiving cryptocurrency must be tied to an identity, and that identity (along with the association with the public address) must be verified by a central authority. This takes away the pseudonymity that cryptocurrency provides by tying wallet addresses to the identity of bank clients and recipients of funds. This allows the bank to do due diligence to the same capacity as with currency that central banks issue.

Lastly, banks can mandate that clients must provide the bank with both the private and public key of their wallets. This effectively gives full control of the funds to the bank to the same degree as that the fiat currency issued by central banks.

Implication on consumers (and vendors)

- **Benefits**

The more and more prevalent use of cryptocurrencies will benefit the consumers and vendors with higher privacy, convenience, lower transaction fees, and better security with confirmations in the transaction process.

Blockchain transactions are censorship resistant, which means that no one or authority could censor the transaction. This significantly protects the sender's and receiver's identities and details of the transaction.

Compared to traditional banking, cryptocurrency transactions are much faster as the crypto payment is made by simply transferring the cryptocurrency from one wallet to another. This gives advantages to cryptocurrency especially in large transactions. Its decentralized nature may also make cryptocurrency transactions more convenient to consumers, as no banks or financial authorities are involved in the process, which makes the transactions more flexible.

The low and almost no transaction fees also give cryptocurrency an advantage over traditional transaction methods, such as using credit cards. Credit Card fees is usually about 0.5% to 5%, and there is an additional 20 to 30 cent flat fees for each payment. As the cryptocurrency fees are based on the amount of data sent, it usually imposes exceptionally low cost (Blystone, 2020).

When two users or entities are transacting with a digital currency, confirmations (which happen on the underlying blockchain) help indicate how secure that transaction is. A confirmation is the number times a subsequent block (i.e., transaction) has occurred after your transaction. The more 'confirmations' there are, the more secure and stable your transaction is (Ethos, n.d.). Why is this secure? Because bad transactions can be rejected or reversed by the network when one node tries to add it, and confirmations are the proof that the network has accepted the transaction as being trusted and verifiable. With more blocks added after yours, an attacker has to decrypt all subsequent blocks after the block containing your transaction, which is cryptographically infeasible. As more blocks keep getting added, it is significantly costly to decrypt all blocks in terms of processing power.

- **Risks**

However, certain risks also arise when consumers use cryptocurrency transactions. The main risks that people are concerned about include inability to cancel the transaction, less regulation in the cryptocurrency market, and cyber hacking.

Like a double-edged sword, the fact that blockchain transactions are generally irreversible may cause potential risks to consumers in the transaction process as well. Imaging that you have purchased a product from a seller online. You paid the seller and seller said he has shipped the product to you. However, you found that you are not able to contact the seller anymore. You

realized that this is a fraud, but you could not cancel or reverse the payment which is in cryptocurrency.

Cryptocurrency is only in its rapid development in this century, and compared to traditional banking with a long history, the cryptocurrency market is much less regulated. Thus, the users may not be able to use the complaint-handling procedure like compared with using debit and credit cards (Government of Canada, n.d.). Basically, the users are less protected in the cryptocurrency market from regulations.

With immense use of technology, cryptocurrency transactions are prone to cyber hacking, and this imposes certain risks to consumers. Cybercriminals may attack the cryptocurrency trading platforms and once the attack succeeds, they can then steal funds from the users. Some famous cyber attacking events on cryptocurrency trading platforms includes the "vampire attack" on UniSwap in 2020 and the hacking attack on CoinDash's ICO (initial coin offering) in 2017.

- **Potential solutions**

To enforce regulations in the digital currency market, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) has made a notice on the assessment of obligations for reporting entities. As part of the obligations, the reporting entities are required to report large virtual currency transactions if they receive an amount of virtual currency equivalent to $10,000 or more in a single transaction (FINTRAC, 2021). As of June 1, 2020, FINTRAC also required foreign cryptocurrency exchanges to register first so that they could conduct business with Canadian clients (Segev LLP, 2019).

Moreover, the cryptocurrency trading platforms can also adopt better safety systems, such as firewall, and hire experienced IT team to response quickly to issues that arise. As technology is always changing, the trading platform needs to update its safety system constantly in order to better protect its users from cybersecurity attacks.

Implication on cash-in-transit

- **Benefits**

Cash-in-transit refers to the underlying middle state that exists between banks and consumers, which is also the physical transfer of banknotes and coins. It happens every day to ensure sufficient money is transferred from place to place, such as between ATMs and banks, to fulfill depositors' needs. With decentralized digital currencies, the time and cost of cash-in-transit will be greatly reduced with higher level of security.

Transferring cash or items with value is usually costly because the authority needs to hire not only administrative staff but also security guards, in addition to purchasing or renting transportation tools. By using decentralized digital currencies, no physical transfer of money is needed and therefore, it saves the time and cost of cash-in-transit.

- **Risks**

For digital currencies following a proof-of-work consensus mechanism (e.g., 3 largest currencies by market cap: Bitcoin, Ether on Ethereum 1.0, Litecoin), the functionality of the digital currency is dependent on the state of the network being such that no one node on the network (or collaborating group of nodes collectively known as a *mining pool*) controls more than 50% of the computing power. Such an occurrence would allow them to prevent, reverse, and 'double spend' during the period when they control most of the computing power. However, they would not be able to delete any transactions that occurred before they controlled most of the computing power on the network.

- **Potential solutions**

One remedy to the consensus mechanism is to switch to a newer consensus mechanism that does not have the same pitfalls as proof-of-work (as Ethereum is doing), or for a currency that uses a preferable consensus mechanism to be used. Proof-of-stake is a newer consensus mechanism that depends on the number of coins a miner has rather than computing power. A miner is able to 'stake' some of the digital currency they hold that can be used to verify transactions and add blocks to the network (i.e., mine), with the amount one makes for verifying transactions dependent on the amount one stakes. Such a method is many times more energy efficient than proof-of-work.

Conclusion

According to a recent article, the banking industry is trying to embrace cryptocurrencies, and making profits from it. For example, JPMorgan started its digital currency, JPM Coin, in 2019 (Flitter, 2021). As more and more people adopt decentralized digital currencies as a way of payment and investment, it is an inevitable trend that decentralized digital currencies will have an impact on our daily life in the future. Though there are still many uncertainties in promoting decentralized digital currencies, the risks of decentralized currencies could be mitigated with the help of appropriate solutions, and people will be able to benefit from an improved transaction process with it.

Appendix: Decentralized Digital Currency vs. Fiat Currency

	Decentralized Digital Currency	Fiat Currency
Transaction Fee	Low, almost none	About 0.5% to 5%
Transaction Time	Low	1-5 business days for international wire
Security	High	Subject to conditions
Issuance	Through mining	Through government
Value	Derived from blockchain	Determined by the central bank
Exchange	No intermediary is required	Centralized intermediaries are required except for cash exchanges

(Cryptopedia Staff, 2021)

References

Bank of Canada. (n.d.). Canada's Major Payment Systems. Retrieved on December 3, 2021 from

https://www.bankofcanada.ca/core-functions/financial-system/canadas-major-payments-systems/#acss

Blockdata. (2019, March 3). Blockchain is disrupting the $700 billion remittance industry. Retrieved on December 3, 2021 from

https://medium.com/@blockdata_tech/blockchain-is-disrupting-the-700-billion-remittance-industry-b79a01a95a10

Blystone, D. (2020, June 21). Bitcoin vs. Credit Card Transactions: What's the Difference? Investopedia. Retrieved on November 23, 2021 from

https://www.investopedia.com/articles/forex/042215/bitcoin-transactions-vs-credit-card-transactions.asp

Cryptopedia Staff. (2021, March 14). Fiat Money vs. Cryptocurrency. Retrieved on November 30, 2021 from

https://www.gemini.com/cryptopedia/fiat-vs-crypto-digital-currencies

Ethereum. (2021, November 22). Ethereum Whitepaper. Retrieved on November 12, 2021 from

https://ethereum.org/en/whitepaper/

Ethos. (n.d.). What are Blockchain Confirmations? Retrieved on November 29, 2021 from

https://www.ethos.io/what-are-blockchain-confirmations/

FINTRAC. (2021, September). Reporting large virtual currency transactions to FINTRAC. Retrieved on November 29, 2021 from

https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/lvctr/lvctr-eng

Flitter, E. (2021, November 1). Banks Tried to Kill Crypto and Failed. Now They're Embracing It (Slowly). The New York Times. Retrieved on November 23, 2021 from

https://www.nytimes.com/2021/11/01/business/banks-crypto-bitcoin.html

Government of Canada. (n.d.). Digital Currency. Retrieved on November 12, 2021 from

https://www.canada.ca/en/financial-consumer-agency/services/payment/digital-currency.html

IBM. (n.d.). What is blockchain security. Retrieved on November 22, 2021 from

https://www.ibm.com/topics/blockchain-security

Marr, B. (2017, December 6). A Short History Of Bitcoin And Crypto Currency Everyone Should Read. Forbes. Retrieved on November 12, 2021 from

https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/?sh=4fab382c3f27

Nakamoto, S. (n.d.). Bitcoin Whitepaper. Retrieved on November 12, 2021 from

https://bitcoin.org/bitcoin.pdf

Potter, S. (2021, February 18). First Bitcoin ETF in North America is launching in Canada today. Financial Post. Retrieved on November 12, 2021 from

https://financialpost.com/investing/first-bitcoin-etf-in-north-america-is-launching-in-canada

Rosic, A. (2021, November 25). What is Cryptocurrency? Blockgeeks. Retrieved on November 29, 2021 from

https://blockgeeks.com/guides/what-is-cryptocurrency/#What_is_cryptocurrency_mining

Segev LLP. (2019, August 16). Changes to Canadian Cryptocurrency Regulations. Retrieved on November 12, 2021 from

https://segev.ca/changes-to-canadian-cryptocurrency-regulations/

Switchere. (2021, August 19). How Long Does ETH Take to Send in 2021. Retrieved on November 29, 2021 from

https://blog.switchere.com/how-long-does-eth-take-to-send-in-2021/

Voshmgir, S. (2020). Token Economy. Shermin Voshmgir. Retrieved on November 27, 2021.