A Guide to Blockchain and Cryptocurrency

Since the initial release of a white paper by developer(s) under the pseudonym Satoshi Nakamoto, the concept of blockchain has greatly challenged the traditional method of "transaction". Over the past decade, the Blockchain technology has extended its application to a myriad of sectors, and one major application is cryptocurrency transactions. Although cryptocurrencies gained significant popularity among investors, the classification and legality of cryptocurrencies as an asset have yet to reach a global consensus. In midst of a global economic recession, the cryptocurrency industry also faces enormous challenges following the plunge of crypto prices. This report will serve as a handbook that offers an in-depth overview of the blockchain technology, recent activities in the Canadian market, and our view on the potential impact cryptocurrency can have on the capital markets.

Isaac Dong | Cameron Brown | Azmir Arfeen | David Kang | Emily Yang

14 September 2022

Table of Contents

History..... Page 3
Purpose..... Page 3
Types of Bitcoin..... Page 4
Wed3 Technology..... Page 5
Case Study – Filecoin..... Page 5
The Blockchain Technology..... Page 6
Overview..... Page 6
Mining..... Page 7
Benefits and Drawbacks..... Page 8
Regulations..... Page 8
Recent News..... Page 9
KPMG Investment in Metaverse..... Page 9
OSC Regulatory Actions..... Page 9
FTX Acquisitions..... Page 10
Blockchain Impact on the Capital Markets..... Page 11

Introduction to Cryptocurrency

Overview

A cryptocurrency is a digital or virtual currency that is secured by cryptography which can be mined or directly purchased from cryptocurrency exchanges. These are often represented on **decentralized networks** based on blockchain technology, a distributed ledger enforced by a diverse network of computers. A key defining feature of cryptocurrencies is the **absence of a central authority**, rendering them theoretically immune to government interference or manipulation.

While such currencies were initially intended to provide an alternative method of exchange, they are seldomly used for retail transactions as the volatility has rendered them **popular trading instruments.**

Tokens vs. Coins

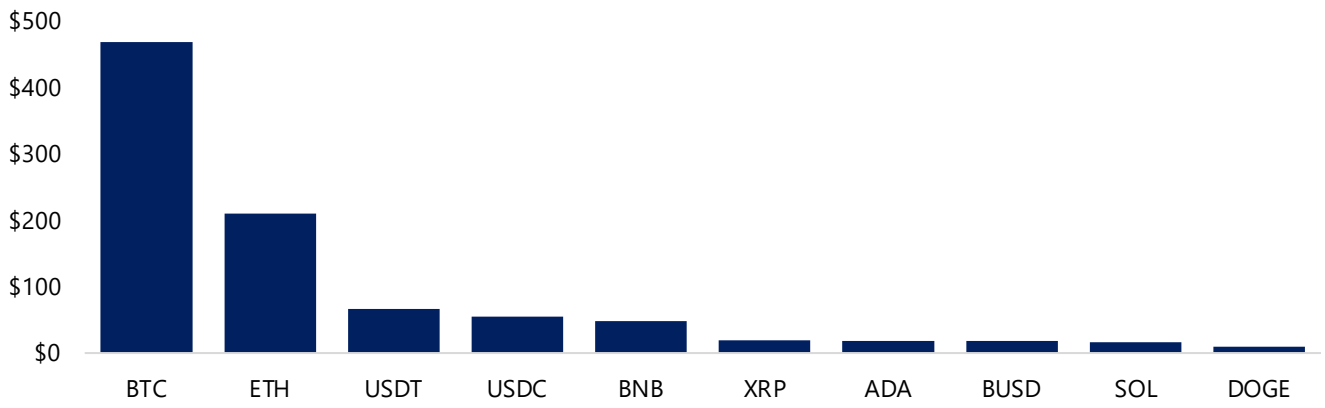
Cryptocurrency can be separated into coins and tokens. A digital **coin** is created on its own blockchain and are analogous to traditional money as they can be used to store value and as a means of exchange. Bitcoin represents the most popular digital coin in circulation.

Tokens on the other hand, are created on top of an existing blockchain and can have far more uses extending to gaming, non-fungible tokens (NFTs), and stablecoins. Crypto tokens are usually created through an initial coin offering (ICO) process which involves a crowdfunding exercise to fund projects. Ether represents the transactional token that facilitates operations on the Ethereum network as a form of payment for participants.

Cryptocurrency in Practical Application

Advantages	Disadvantages
• Cryptocurrencies eliminate intermediaries enabling anonymous, cheap and fast transfers • The blockchain network secures each transaction and prevents counterfeiting • Decentralized networks prevent interference and manipulation • Cryptocurrencies are offered in limited pre-set quantities which protect against inflation	• The anonymity offered has resulted in cryptocurrency being used for illegal activities • The lack of a central authority ensuring inherent value has resulted in extreme price volatility • Losing digital wallet keys can lead to users being unable to access their coins • Mining activities consume a significant amount of energy

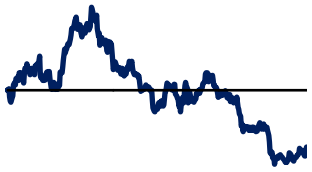
Cryptocurrency Market Cap Breakdown (in USD$B)



Sources: Investopedia, The Motley Fool, Statista

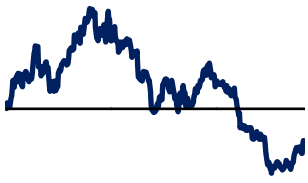
Bitcoin

Bitcoin is regarded as the first decentralized cryptocurrency using blockchain technology to facilitate payments and digital transactions. Bitcoin established the basic system of cryptography and consensus known as peer-to-peer (P2P) verification which laid the foundation of most forms of crypto today. Bitcoin's price is renowned for being highly volatile and has become the most popular crypto investment to date.



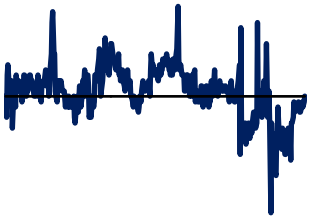
Ethereum

Ethereum enables global transactions through its native cryptocurrency, ether, which has unbounded supply. It was designed to expand the utility of cryptocurrencies by allowing developers to create their own applications. Ethereum utilizes smart contracts that carry out a various functions ranging from executing transactions to loaning funds once collateral is deposited into a digital wallet.



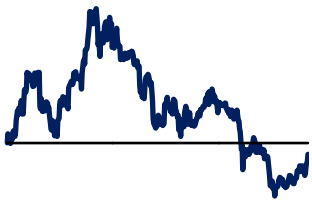
Tether

Tether is the largest stablecoin by market cap, a cryptocurrency that has its value tied to a fiat currency. Tether tracks the US dollar and combines the benefits of a cryptocurrency with the stability of a currency issued by a sovereign government which alleviates a major concern over volatility. It also issues a token tied to the price of gold known as tether gold, backing its value by gold bars instead of fiat currency.



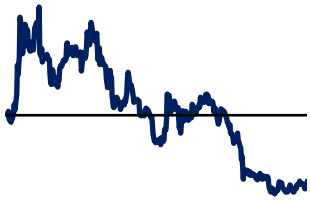
Binance Coin

Binance coin is the exchange token of the Binance cypto exchange. Investors in BNB are awarded discounts on trading fees on the exchange which has linked the token's value to the demand of Binance's services. This is similar to the prospect of buying shares in a company without any ownership interests. Binance coin was initially based on the Ethereum network but is now based on the Binance chain.



XRP

XRP Ripple is the native cryptocurrency of the XRP Ledger, an open-source blockchain designed to enable faster and cheaper payments. Ripple was intended to serve as a replacement for SWIFT for cross-border transactions. The XRP Ledger operates differently compared to most blockchains as it is somewhat centralized due to its consensus protocol that allows users to verify their transactions through unique node lists.



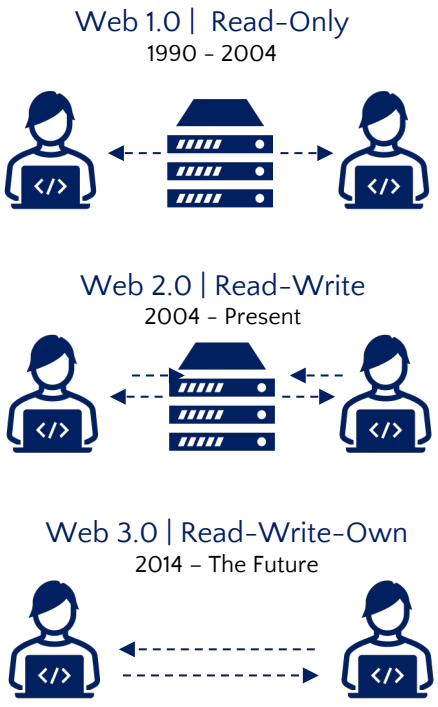
Sources: Coindesk, Forbes, Nasdaq, The Motley Fool

Web3

Web3 refers to the third generation of the internet. This idea was coined by Ethereum co-founder Gavin Wood following the its launch in 2014. The premise of Web3 stems from the belief that the current Web required too much trust as it relies on trusting a select few companies to act in the public's best interests. Web3 aims to **remove control from large corporations** through decentralization which allows it to be owned, built, and operated by the users themselves.

One of the central purposes of Web3 is **to return ownership** of one's data to the user to avoid companies leveraging their information. This would create unique possibilities, for example, it would allow artists to post their music on decentralized platforms instead of replying on companies like Spotify or Youtube that profit through serving as middlemen.

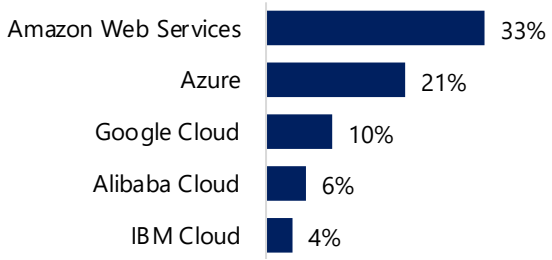
Web3 cryptos represent a new wave of cryptocurrencies that focus on carrying forward the decentralized vision of the internet. These **combine** blockchain technology with smart contracts to eliminate intermediaries for a variety of purposes.



Case Study: Filecoin

Filecoin (FIL) is a decentralized, peer-to-peer network for **file storage** that serves as a Web3 alternative for data storage products like Amazon Web Services (AWS) and Google Drive. It was developed by Juan Benet and his team at Protocol Labs after raising $250 million. They aim to disrupt the traditional model of centralized data storage by implementing a **publicly verifiable** and trustless storage product that does not rely on a single entity. Currently, the data storage and cloud computing market is highly concentrated with AWS and Azure alone capturing over half of the market.

Cloud Computing Market Share



Filecoin users pay fees to storage miners for storing their files on the network. These storage miners include the computers on the network that are responsible for offering continued storage space in exchange for the native filecoin token (FIL) as an economic incentive. Users can customize their storage preferences for cost, redundancy, and speed when selecting a miner before verifying the proof of storage on the Filecoin blockchain. This network operates as an **open market for storage** as anyone can participate as a storage provider and receive rewards in FIL. To ensure network security, unlike many proof-of-work (PoW) blockchains, Filecoin uses the proof-of-replication (PoRep) and proof-of-spacetime (PoSt) protocols. PoRep initially creates a proof of storage when miners first store a unique copy of the data on their system and PoSt ensures that the space continues to store the user's data. Miners are required to put up collateral before joining the ecosystem and are penalized if they fail to provide continued storage as per their agreement.

Sources: Ethereum.org, Coindesk, Statista

The Blockchain Technology

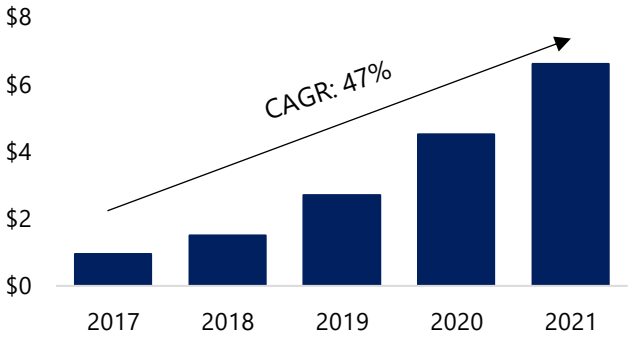
Overview

Blockchain technology facilitates transaction processes which allows individuals to track assets and their movement within a business network. A Blockchain ledger differs from a typical accounting ledger as it is shared and immutable; it is meant to be viewed by more than just an accounting department, and transactions cannot be hidden or deleted once they have taken place.

Blockchain was made to be decentralized so that information can be made widely available to ensure transparency for parties involved. There are various types of Blockchains which allow for several viewership and accessibility options as identified and explained below.

Given Blockchain's widescale applicability and its existing growth, global Blockchain expenditure is expected to reach $19 Billion USD by 2024. A growing number of organizations are expected to utilize the technology for data access and identity protection.

Global Blockchain Spending (in USD$B)



Types of Blockchain

Public — Anyone can join and participate. Requires significant computational power, minimal privacy, weaker security.

Private — Decentralized, peer to peer. Network is governed by an organization that controls participant access. Good for maintaining user trust.

Consortium — Multiple organizations can share responsibilities and control, reducing risks associated with single entity control.

Permissioned — Individual in control selects network of users who can see information and require an invitation/permission. Can be public or private.

Sources: IBM, Statista

The Mechanism of Blockchain

A block of data is created which represents a transaction

Another block representing a new transaction is connected

Blocks are chained together irreversibly

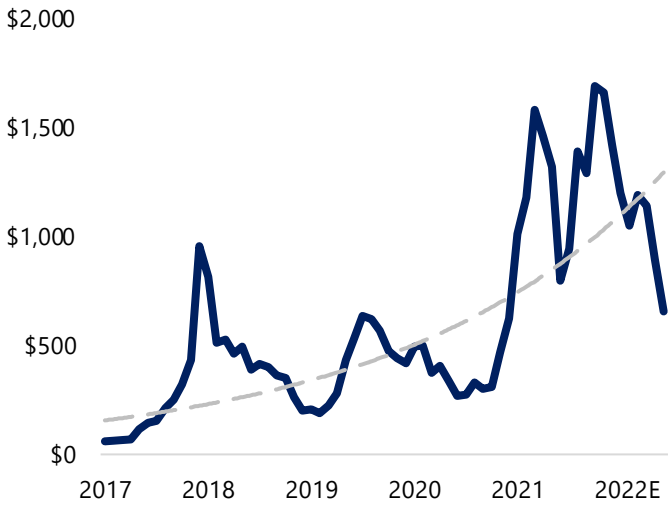
Any additional blocks will be connected to the one before

Mining

To complete the **"chaining"** process above, a process called mining must take place. Mining is completed with the **decoding of intricate equations** generated by the system of the Blockchain. The cryptography is so complex that succeeding in "Proof of work" – the technical term for solving these codes – uses an enormous amount of energy. For example, the amount of energy consumed by Bitcoin mining is estimated to have exceed the consumption of the 45 million people within Argentina.

Blockchains are setup with **"Smart Contracts"**, which automatically rewards miners as the block is added to the ledger upon completion. Only the first user to complete the mining process is given the reward, and thus lots of energy and computational power is used by individuals who do not end up receiving the reward.

Bitcoin Mining Revenue (in USD$M)



Sources: IBM, PCMag, Columbia Climate School, The Block

Benefits

Transparency: As Blockchain-based transactions are virtual, it is widely accessible. Depending on the privacy, the ledger can be viewed by exponentially more stakeholders than physical records, providing additional comfort.

Security: Cryptography is used for a reason; the code solutions for Bitcoin and other cryptocurrencies are not easily solved. Once a block is added to the network, it is relatively impossible for any further changes to be made to it.

Consistency: Smart contracts allow Blockchain processes to be automated. When any changes are made, the network will refer to a predetermined set of rules to determine the outcome.

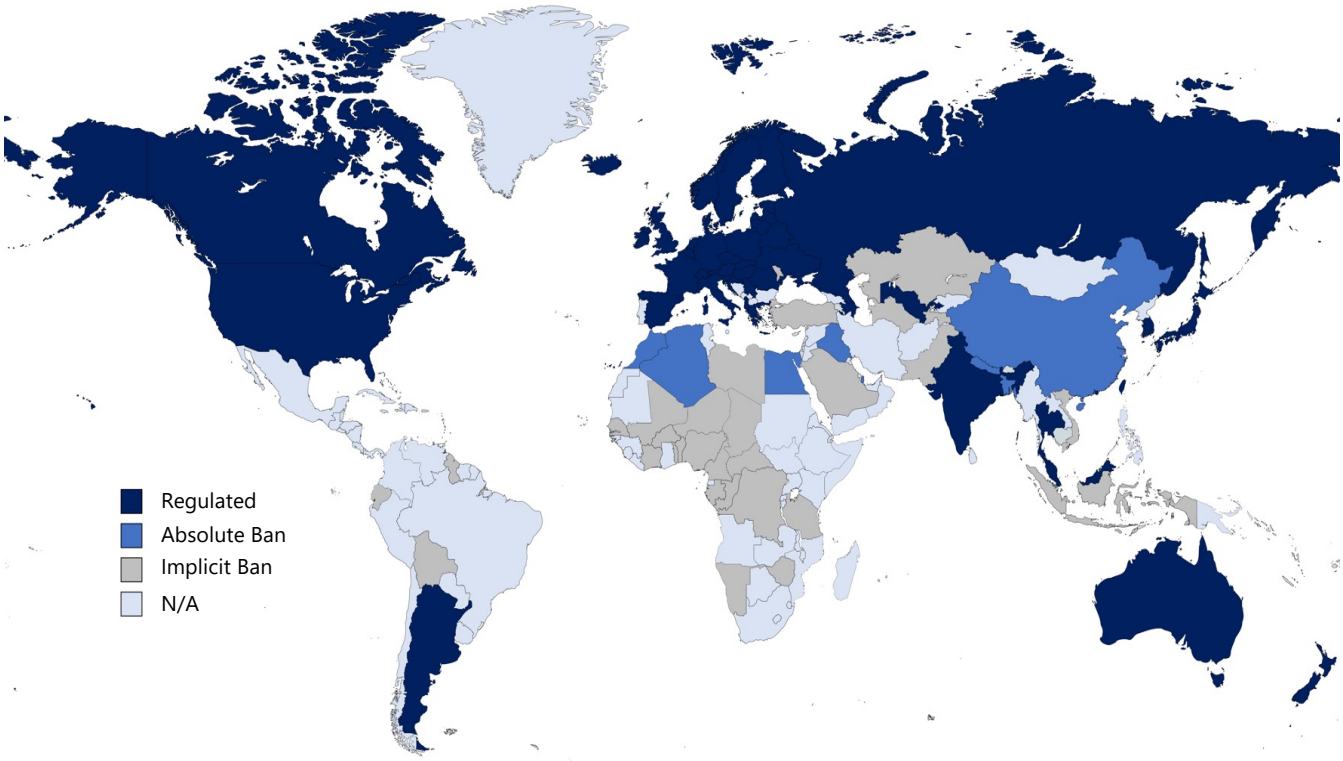
Constraints

Investor Apprehension: Blockchain is not well understood by Baby Boomers nor Generation X-ers, cryptocurrencies as a form of investment will be constrained as these generations hold 78% of wealth in the United States.

Scalability: When more people are involved in a Blockchain network, the pace slows. Conversely, centralized payment methods can handle thousands of transactions per second, while Bitcoin can only handle seven.

Political Threat: Politicians who make laws regulating cryptocurrencies often have little to no understanding of them nor Blockchain technology. Many countries are beginning to make such laws as discussed below.

Worldwide Regulations



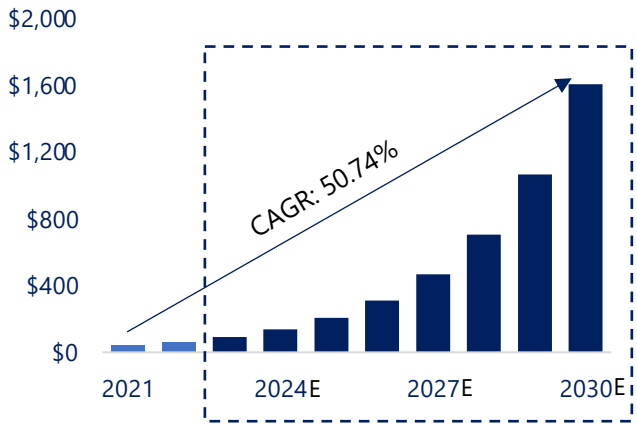
Sources: CNBC, Forbes, GLI, Statista

Recent News

Corporate Applications

KPMG has revealed the opening of its first metaverse collaboration hub to help its employees and clients pursue growth opportunities in the digital era, investing $30M in Web3 employee training. The hub will be focused on education, collaboration, training, events, and workshops. According to KPMG, it intends to hire people to build and expand it over time. The long-term objective is to examine other potential metaverse use cases such as health care, consumer, retail, media, and financial services.

Global Metaverse Market (USD$B)



Regulations & Legal Services

OSC — ONTARIO SECURITIES COMMISSION

BYBIT

KUCOIN

"Foreign crypto asset trading platforms that want to operate in Ontario must play by the rules or face enforcement action"

- OSC Director of Enforcement Jeff Kehoe

Problem

The Ontario Securities Commission, or OSC, issued financial penalties against Bybit and KuCoin, claiming violation of securities laws and operating unregistered crypto asset trading platforms

Result

OSC issued a deadline for crypto firms operating in the province to register in compliance with securities law by April. Despite this warning, Bybit and Kucoin did not contact the OSC by the deadline and continued operations in Ontario.

Future Outlook

The move by the regulatory body was the latest in a series of warnings and legal actions against offering services to Ontario residents. OSC looks to further strength its enforcement.

Sources: Cointelegraph, GlobalNewswire

Mergers & Acquisitions in the Market

Key Players

FTX — Centralized cryptocurrency exchange specializing in derivatives and leverage products; it supports most commonly traded cryptocurrencies

Bitvo — Bitvo is a Toronto-based crypto asset trading platform that facilitates trading cryptocurrencies through its in-class website and mobile applications. It offers eleven cryptocurrencies

Liquid — Liquid is based at Tokyo, Japan. Developer of a cryptocurrency trading platform designed to provide liquidity to the crypto economy

LedgerX

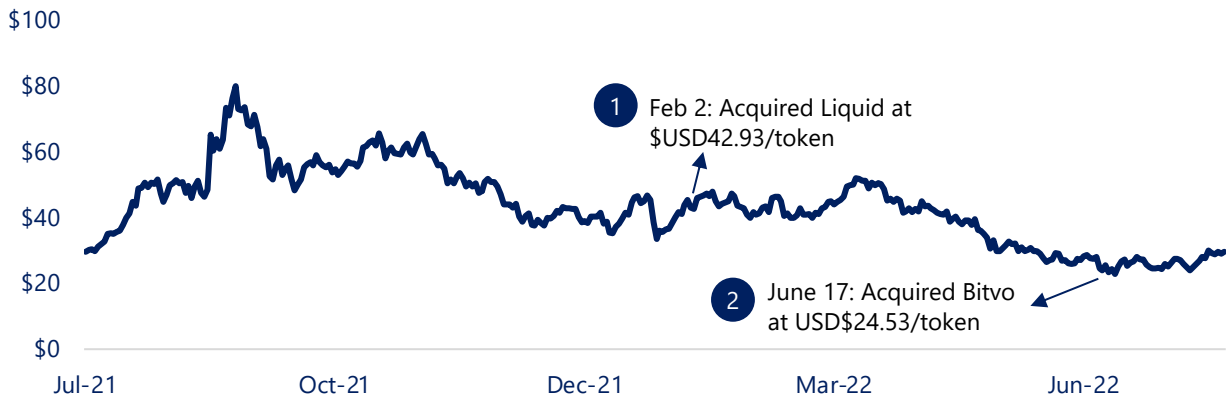
Deal Overview

FTX Trading Limited said it planned to **acquire Bitvo** as part of the crypto exchange's effort to offer its products and services to Canadia-based users. In addition to Bitvo, **FTX acquired Japanes crypto firm Liquid Group** and its subsidiaries in February as part of the company's expansion into Asian markets, following the firm buying BTC derivatives platform LedgerX in 2021.

Implications

From a market perspective, as funding for cryptocurrency start-ups are becoming more difficult, large crypto firms with solid capital would acquire start-ups to access more regulatory licenses around the globe and expand customer base. Global trading platforms like FTX are discovering interest into Canadian market, which allows FTX to enter the regulatory Canadian crypto market. Looking forward, it is expected that more M&A activities are about to happen in the industry.

FTX Token USD 1Y (FTT-USD)



Mergers and acquisition activity in crypto boomed in 2021 with the global value of such transactions totaling more than USD$55 billion, versus USD$1.1 billion in 2020, according to PWC.

Sources: Cointelegraph, CoinMarketCap

Blockchain Impact on the Capital Market

Current State of Growth

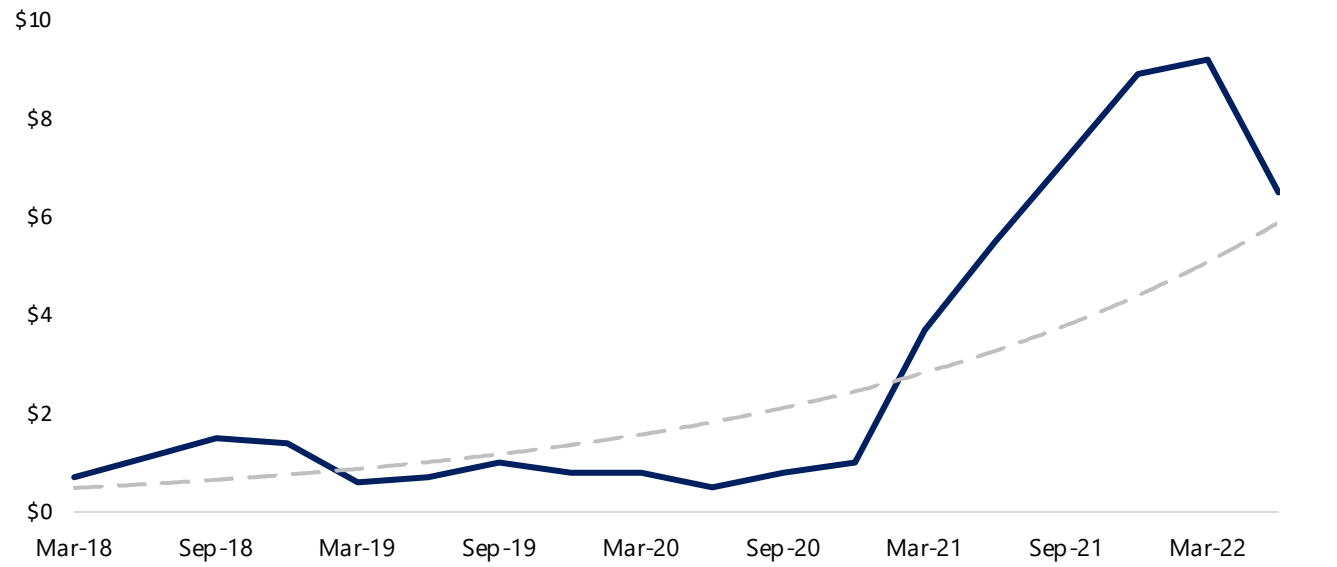
Current State: According to data compiled by CB Insights, for the first time since 2018, blockchain funding has decreased, with aggregate funding declining by 29.0% quarter over quarter. It is important to recognize that the decline is mainly driven by a loss of interest from investors in funding new centralized crypto platforms/exchanges like Coinbase, with this sector reaching only 36.0% of the 2021 funding level.

Behind the Numbers: Meanwhile, the decentralized finance (Defi) sector funding is already at 91.4% of the 2021 level, while funding for decentralized application (DApp) development has already surpassed the 2021 level by 26.3%. This shows that rather than a total loss of interest across the entire blockchain industry, investors are simply shifting attention away from the centralized crypto exchanges and into other sectors, specifically Defi and DApp.

Future Potential: Continuous growth within these two sectors is fueled by their potential application across different industries. A number of Blockchain solutions have the potential to change traditional banking, such as tokenization, simplifying international trade with smart contracts, and competing against traditional IPO's with initial Coin Offerings (ICO's).

Looking Ahead: Blockchain also has the ability to disrupt industries beyond banking, like the real estate industry, where it could simplify the transaction process, and cut out intermediaries. The redirection of capital away from the centralized exchanges may prove to be a positive change that accelerates the progress of blockchain's adaptation and applications in other areas.

Blockchain Funding (USD$B)



Sources: CB Insights, CNBC, Forbes, GLI, Statista

The SWIFT System: Basic Mechanism

With the SWIFT system, to perform a transfer of funds from one bank to another, the SWIFT needs to first search its network to identify a correspondent bank that can act as a bridge for a fee. Then, the individual ledgers of both parties will need to be reconciled respectively to reflect this. However, the actual transfer of the fund is completed via a complex chain of commands, most of the time even involving human interventions. As a result, the entire process is very complicated, lengthy, and involves small but recurring fees.

Potential Effect of Blockchain on SWIFT

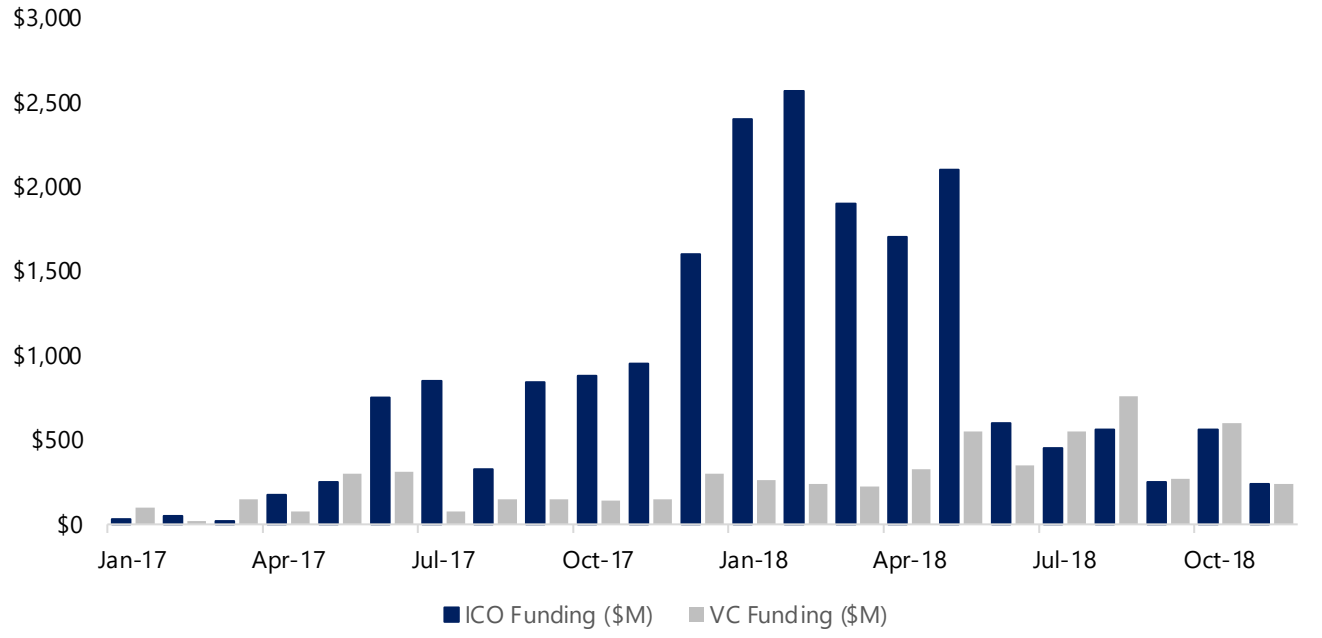
With the blockchain method, an interbank block chain will track and settle all the transactions on a public and transparent ledger, thereby eliminating the need to go through a correspondent bank. Furthermore, because of the full automation of the process, transactions can be settled almost instantaneously. This contrasts distinctively with the pricey, long, and complex process of the current system, making a blockchain revolution much more appealing to many users. Some of the leading firms making progress in this sector include Ripple and R3.

Initial Coin Offering (ICO)

Overview: An ICO is nearly identical to the common IPO process, except coins are issued rather than shares, and funding come in the form of cryptocurrencies (eg. Bitcoin). The benefit of the ICO model is that it is able to skip all the complex processes of going through an investment bank. The legal fees for an ICO is also much cheaper, making it much more affordable for the smaller companies. The ICO model is also similar to an IPO because the value of the coins are linked to the success of the project/company, and they will fluctuate just like real company shares.

Current State: While aggregate ICO funding peaked in early 2018, it has been on a dramatic decline since then. The driver behind this decline is also its benefit. Almost anyone can set up an ICO with the right technological equipment. The lack of governance and the ease of accessibility has led to an incredible number of scams within the space. To move forward, ICO needs to find a right balance between regulations and the accessibility aspect of ICO's that make it unique.

ICO Funding vs. VC Funding (USD$M)



Sources: CB Insights Financial Times