NCFTA

The National Cyber-Forensics and Training Alliance

ONE TEAM, ONE GOAL. COMPANIES, GOVERNMENT, AND ACADEMIA WORKING TOGETHER TO NEUTRALIZE CYBER CRIME.

# Cryptocurrency and Blockchain

August 15, 2018
Analyst Code: 0310

**Confidential | Industry – TLP Amber**
This report is confidential and contains NCFTA proprietary information. The content is intended to be demonstrative and informational only. The source of all information must be independently confirmed before using the data as part of any investigation. Distribution of this product will follow the guidelines as set forth in the Traffic Light Protocol (TLP).

**NCFTA | PITTSBURGH** 2000 Technology Drive, Suite 450, Pittsburgh, PA 15219 | 412-802-8000
**NCFTA | NEW YORK** One Penn Plaza, 250 West 34th Street, Suite 2124, New York, NY 10119
**NCFTA | LOS ANGELES** Wilshire Building, 601 S. Figueroa Street, Suite 1460, Los Angeles, CA 90017

## 1.0 Executive Summary

Cryptocurrencies and the blockchain technology that underpins them have created major changes in the way financial institutions and consumers conduct commerce. This ranges from payments processing to new financial technology systems. Their use also enables new types of fraud and cybercrime. This new ecosystem of currencies and technologies is likely to influence the financial industry in a variety of ways, and its full impact can be difficult to predict. The financial industry, as well as law enforcement and consumers, will benefit from learning more about this technology as they adapt to changing consumer needs, criminal activity, and technological progress.

Cryptocurrencies are non-governmental currencies that use blockchain technology to settle and record transactions. There are several common intrinsic features of permissionless cryptocurrencies (e.g. Bitcoin, Litecoin, Ethereum, Monero, etc.) that are different from traditional digital currency:

- Decentralized: There is no central organization, government, or individual that can manipulate the network, for better or for worse.
- Psuedonymous or anonymous: There is no identity information required to create accounts or transact.
- Uncontrolled: Accounts and transactions cannot be frozen.
- Fast or instant settlement: Transactions are effectively permanent after as little as a few seconds.
- Commodity-like and deflationary: Monetary policy is defined by mathematical functions and, therefore, the supply (current and future) is known publicly.
- Low or zero transaction fees: Cryptocurrency transactions are low-cost, usually ranging from free to less than one dollar. Transaction fees are the same, no matter the amount transacted.

Financial institutions have an opportunity to capitalize on new blockchain technology that decreases cost, increases speed of settlement, and could decrease consumer fraud. This is an effective way to adapt to changing customer needs and improve transactions. Many major banks, merchants, and consumers use cryptocurrency and blockchain technology. Since blockchain implementations are often open source projects, anyone can use the technology and customize it for their own needs and requirements.

There are many innovative use cases of blockchain technology that are not necessarily cryptocurrency-related. These include identification systems, provably-authentic documentation, self-executing smart contracts, digital assets representing physical goods, and decentralized governance structures. The core benefit of blockchain technology is a solution to the longstanding challenge of ensuring scarcity and restricted ownership of data in a decentralized network. Recently, there have been non-blockchain attempts at accomplishing the same effect and these projects fall under the general category of decentralized ledger technology (DLT).

Criminal actors use cryptocurrency for its speed, low fees, lack of regulation, and relative anonymity. Analysts and investigators can use chain analysis tools and foundational blockchain knowledge to mitigate cryptocurrency-enabled crime. The SEC, IRS, CFTC, US legislators, and their international analogues have all begun to regularly discuss cryptocurrency and potential regulation that may be introduced. Existing regulations designed for traditional financial instruments may also apply to cryptocurrencies. Malware facilitated by anonymous payment systems has affected a variety of computer users, not just those that work with cryptocurrency.

Common criticisms of cryptocurrency and blockchain include energy waste of the mining process, limited scalability, and volatile prices. Despite these issues, cryptocurrency projects have recently seen significant institutional monetary and mental investment. Cryptocurrency and blockchain have a distinct business ecosystem, consisting of startups, established companies, and miners.

Users and businesses that hold cryptocurrency must adhere to stringent private key management practices to prevent losses or fraud. There are many tools and practices available that make storing cryptocurrency easier and more secure. Financial institutions may provide services to hold, insure, and secure cryptocurrency holdings for a multitude of purposes ranging from utility to investment.

# 2.0 Analytical Assessment

## 2.1 Technical Overview

### *2.1.1 Blocks*

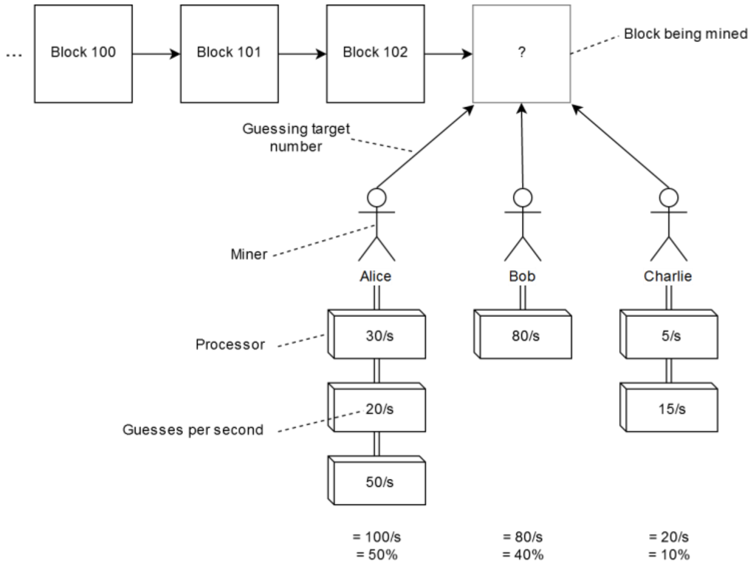
A **blockchain** is a transaction ledger containing a series of blocks chained together linearly. Each **node** within a cryptocurrency network is one instance of the node software, and each has a copy of the blockchain that is kept in sync. Since (most) blockchains are public and open source, all transactions that have ever occurred on the network are publicly viewable at all times. Each **block** is made up of multiple transactions that have occurred since the last block was created and appended to the blockchain. The **block time** is the approximate time between blocks, and is different for all cryptocurrencies, e.g. the Bitcoin block time is 10 minutes while the Ethereum block time is 15 seconds. A faster block time means that transactions are confirmed quicker, since they are included in the blockchain at shorter intervals. Blocks are chained together in a strict order using cryptographic hashing, where each block contains a hash of the previous block. Block integrity is maintained by hashing together a **Merkle tree root** comprised of the transactions and other metadata about the block.[1,2] This creates a unique identifier for each block that can be seen and verified by anyone viewing the blockchain.

### *2.1.2 Mining*

Blocks are appended to the blockchain through a crucial system called **mining**. Miners on the network are nodes that bundle transactions into new blocks and compete with other miners for the privilege of adding their block onto the chain. Miners earn all or most of the transaction fees from the transactions they include in a block. In many currencies, they also receive a bonus supply of newly minted coins known as the **mining reward**. When a miner finds a new block, they announce it to the network and all miners begin working on the next block. Mining occurs differently among cryptocurrencies, but the most common consensus mechanisms are **proof-of-stake** (PoS), **delegated proof-of-stake** (DPoS), and **proof-of-work** (PoW).

PoW is used by Bitcoin, Ethereum, Monero, and several other cryptocurrencies. A system's processing power is used to find a predetermined value by a process similar to brute forcing. Miners attempt to process as many hashes as possible until their systems 'guess' a correct value that is cryptographically predetermined by the network, known as "finding a block". Computing hashes requires processing power, so the more processing power a computer has, the more hashes it can guess and the more chance it has at collecting block rewards (if any) and transaction fees. If a miner tries to publish an invalid block or a shorter chain, they will be ignored. An invalid block could be caused by anything from an incorrect hash to an invalid transaction.[3] Cryptocurrency networks will automatically adjust the difficulty of finding the correct value so that blocks are being found at a predetermined block time interval.[4] The more miners a network has, the more competition exists to find new blocks. The below diagram is a simplified visual explanation of the proof-of-work system:

[1] hxxps://www.blockchain-council.org/blockchain/what-is-merkel-tree-merkel-root-in-blockchain/
[2] hxxps://www.whitehatsec.com/blog/blockchain-technology/
[3] hxxps://www.cryptocompare.com/coins/guides/how-does-a-bitcoin-node-verify-a-transaction/
[4] hxxps://bitcoin.stackexchange.com/a/5840



Mining can be **pooled** or individual. Pooled mining involves many individuals collaboratively mining and sharing the rewards, much like a group of people that buy lottery tickets together. Pooled mining stabilizes profits because there is a payout (proportional to contributed processing power) whether or not the miner is successful in finding blocks. This style of mining is more common among miners without significant individual processing power.

There is a distinction between **application specific integrated circuit** (ASIC) mine-able coins and CPU mine-able coins. An ASIC is a processor chip designed for a specific purpose rather than general use such as a CPU.[5] ASIC coins are cryptocurrencies that are only viable to mine with specialized hardware, and non-ASIC coins (also known as CPU coins) can be mined on any general purpose processor. The middle step between ASIC and CPU are graphical processing units (GPUs) such as those found on PCs that do graphics-intensive processing. GPUs are designed for graphic calculations but are also better suited for creating hashes than CPUs in most algorithms.[6]

PoS or DPoS are used by many other cryptocurrencies, including Ethereum in a future release. Instead of expending processing power, a stake of the currency is put up as collateral. **Stakers** (the PoS analogue to miners) put up funds (a **stake**) and may be granted the ability to make a new block. The chance of being chosen to create a new block is proportional to amount of staked collateral and the total collateral of all stakers on the network. Stakers, in most cryptocurrencies, receive a block reward for creating new blocks. Upon creating a new block, if the block is invalid or cheats the system, the staker is ignored. PoS systems are often criticized for the resulting “rich-get-richer” effect and having a weaker form of consensus than PoW. Currently, PoS systems suffer from the nothing-at-stake problem where there is no incentive to only stake for the best chain.[7] Ethereum is attempting to fix this with their version of PoS called Casper.[8] PoW doesn’t have this problem because mining on the wrong chain will result in wasted processing power that could not have resulted in reward.

Non-blockchain cryptocurrencies also exist and began to see more use in 2018. These non-blockchain currencies use a technology called **directed acyclic graph** (DAG) where transactions are not stored in a linear fashion, but rather as a graph structure. This includes an internet of things (IoT) communication

[5] hxxps://www.pcmag.com/encyclopedia/term/38030/asic
[6] hxxps://en.bitcoin.it/wiki/Why_a_GPU_mines_faster_than_a_CPU
[7] hxxps://www.coindesk.com/ethereum-casper-proof-stake-rewrite-rules-blockchain/
[8] Ibid.

network called IOTA, and a feeless instant currency called Nano. Instead of the network collectively maintaining one central ledger, nodes only need to store a subsection of the data. Ledger size increases with the number of users instead of transaction volume. These non-blockchain cryptocurrencies offer a horizontal approach to scaling that may make them more attractive than blockchain-based cryptocurrencies. Some sources predict that DAG cryptocurrencies will replace blockchain technologies and cryptocurrencies due to this easier scaling.[9,10,11]

### *2.1.3 Permission*

A majority of cryptocurrencies today are run on **permissionless blockchains** (also known as **public blockchains**). "Permissionless" is a term that describes a network or technology does not require prior permission to use or create.[12] Bitcoin, for example, doesn't require any prior authorization to generate addresses, mine coins, create transactions, or fork the network with new protocol rules (see "Forks and Contention").

**Permissioned blockchains** are the opposite. Permissioned blockchains require the participants in a network to be known, and the network consensus rules may be different.[13] The benefits of using this type of blockchain over traditional systems are improvements in speed, security, and trust between users.[14] Private blockchains may be faster due to use of a proof-of-stake model, since decentralization isn't a priority.[15] Decentralization may not be a priority in private blockchains because the participants are known and their intentions are aligned. This type of blockchain is able to confirm transactions quickly, and with the added benefit of understanding the users' infrastructure capabilities for optimal block sizes and timing. Blockchains that require prior permission to access may have disadvantages in efficiency and multi-party verification for security compared to public blockchains. However, financial institutions may not be able to use public blockchains due regulatory challenges, so a permissioned blockchain offers a non-public alternative for use among authorized organizations or individuals.

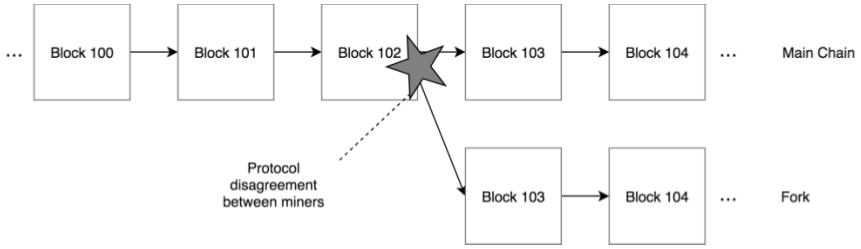
There are two leading open source blockchain frameworks that businesses can freely use to develop a blockchain upon. Corda, developed by R3, is a blockchain platform for streamlining business to business (B2B) payments in a private network.[16,17] Hyperledger is an umbrella project used to describe several different implementations of blockchain technology for different uses. This includes plug-and-play blockchain setup, permissioned smart contract ledgers, and decentralized identity management.[18]

### *2.1.4 Forks and Contention*

When a miner mines a block that adheres to a set of protocol rules or monetary policy that are contrary to the majority of the mining power, at that instant they will **fork** the blockchain. The fork of the blockchain will be a distinct parallel chain that uses the new set of rules and will not ever be interoperable with the **main chain** again, which is the original blockchain. In most cases, forks die off after a few blocks due to no longer being profitable to mine on, because essentially a new currency with no market value is temporarily created. Forks most often occur by accident when miners find a block at relatively the same

[9] hxxps://disruptionhub.com/dag-blockchain-alternative/
[10] hxxps://cointelegraph.com/news/future-of-digital-currency-may-not-involve-blockchains
[11] hxxps://medium.com/@clemahieu/hi-im-colin-lemahieu-the-lead-developer-of-raiblocks-d81f3d864b8b
[12] hxxps://coincenter.org/entry/what-does-permissionless-mean
[13] hxxps://www.investopedia.com/news/public-private-permissioned-blockchains-compared/
[14] hxxps://www.ibm.com/developerworks/cloud/library/cl-ibm-blockchain-101-quick-start-guide-for-developers-bluemix-trs/index.html
[15] hxxps://blog.chronicled.com/how-to-choose-between-public-and-permissioned-blockchain-for-your-project-3c5d4796e3c8
[16] hxxps://www.r3.com/about/
[17] hxxps://www.corda.net/introduction/
[18] hxxps://www.hyperledger.org/projects

time. However, forks can be purposefully caused, such as during a scheduled network upgrade or when a development team designs a new implementation of a cryptocurrency that they intend as an improvement.



Purposeful forks can create economic confusion because the concept does not exist with any traditional financial analogy. When a fork occurs at a specific point in time, the blockchain splits into two distinct currencies, where each address on either side has the full history and balance of the transactions up to the point of forking. From that point on, the transactions involving an address on either side are independent from the same address on the opposing chain.

For example, Alice has 5.00 BTC. A Bitcoin fork occurs at block #1,234,000, where a competing development team enacts new network rules for a new currency called BTC2. Alice now has 5.00 BTC and 5.00 BTC2. She doesn't touch her BTC2, and does many BTC transactions over the course of several months. Her BTC balance may be 2.20 BTC after these transactions, but her BTC2 balance remains untouched.

This has potential implications for financial regulations. A user/institution that holds a cryptocurrency during a fork involuntarily receives a second copy of their balance in a new currency. Financial regulators may consider this a taxable event, given that forks can be triggered by anyone at any time without notice. Markets may also be uncertain as to how to react to a fork and introduce fluctuations into the value of the original and the fork-created cryptocurrencies. The price ratio between a fork and main chain currency may determine which version has more support among miners and users.

From a development perspective, forking takes a slightly different definition. **Hard forks**, with regards to building cryptocurrency projects, are changes that would cause a network fork if they are implemented. A project's marketing team, if there is one, will then attempt to get miners and node operators committed to the new, post-fork version of the cryptocurrency/blockchain. In many planned forks, miners will vote on the changes they support by attaching arbitrary text into the metadata of the blocks they mine. If the consensus threshold is reached or a specific block number is met, the change will be enacted by miners publishing blocks with the new changes. **Soft forks** are changes to the protocol that do not cause a network fork. In other words, soft fork changes are interoperable with previous iterations of the protocol. Soft forks have been criticized for introducing **technical debt**, which is the added difficulty and complication of future updates that must adhere to old rules. Overall, every change to a blockchain protocol must be done as either a soft fork or hard fork.

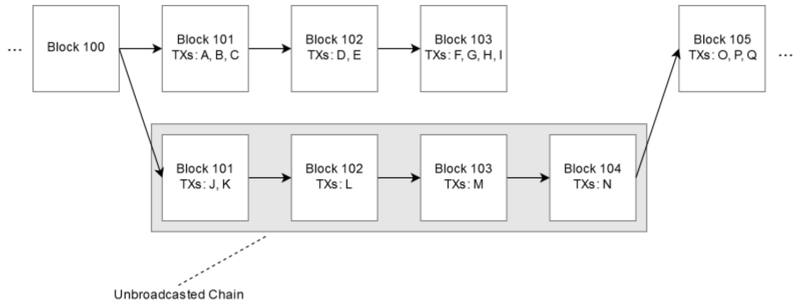
### *2.1.5 Settlement and Attacks*

In most cryptocurrencies, settlement is not just true or false, as it is with bank payments. Instead, settlement is a gradient. Using a metric called **confirmations**, transactions can be referred to as settled or not yet settled depending on the value of the transaction and factors about the sender.[19] Every transaction has a confirmation count, which is the number of blocks that have been added since the block

[19] hxxps://support.bitfinex.com/hc/en-us/articles/115003291405-Where-is-my-cryptocurrency-deposit-or-withdrawal-

it was included in. For example, a transaction that occurs in block #100 has 5 confirmations if the last block found by the network is #104.

The more confirmations a transaction has, the lower the chance that it will be dropped in the event of an accidental or purposeful **reorg** (reorganization). Reorgs occur when a hidden miner mines on a chain without announcing their new blocks to other miners.[20] If they have a majority of the mining power, or are lucky, they can wipe out all transactions since they stopped broadcasting new blocks.[21] This occurs because miners are incentivized to work on the longest chain, so if a new longer chain becomes visible, they will drop the original. **Orphan blocks** are recent blocks that are dropped from the network due to no longer being on the longest chain. Fortunately, reorgs are exponentially unlikely, exponentially more expensive, and exponentially more difficult to pull off depending on how far back an attacker wants to target. The difficulty of a purposeful reorg is also compounded by the total mining power of the network, as having a significant portion is required. The largest organic Bitcoin reorg was in 2015 when 6 blocks (~60 minutes) were lost due to a longer chain being published.[22] In Bitcoin, this number has been standardized to be the upper limit for how many confirmations an important transaction needs to be considered fully settled. For small Bitcoin transactions where the sender is trustworthy or the amount is insignificant, just one or two confirmations are necessary. The following is an illustration of reorgs and their effect on a blockchain:



1. Alice is a powerful miner. She mines blocks 101-104 without broadcasting them to the network.
2. Alice mines block 105, then broadcasts it to the network.
3. Alice's chain is 105 blocks long, and the accepted chain is 103 blocks long. The protocol defines the chain with the most work as the correct chain. Alice's chain is accepted as the new chain.
4. Blocks 101-103 on the original chain are orphaned and transactions A-I are erased.

Reorg chance is determined by the processing power of the network and the block timing, not necessarily the confirmation count. The work completed by miners since a transaction is what determines the level of settlement; confirmation count is just a human-friendly number used to quantify amount of work done. Ethereum has a much faster block interval (15 seconds) and therefore would require more confirmations to reach the level of settlement of a bitcoin transaction with fewer confirmations. The only benefit of a fast block interval with regards to settlement is that the first confirmation comes sooner, reducing **zero conf** (zero confirmation) turnaround time. See Appendix 3.2 for an example of an exchange's settlement policy.

Micropayment merchants often accept zero conf payments which, as the name implies, do not require any confirmations before considered as settled. Organizations accepting these payments may consider the time savings of accepting zero conf payments as an acceptable tradeoff versus waiting for confirmation.

[20] hxxps://cointelegraph.com/news/if-hard-fork-happens-chain-backed-by-majority-of-miners-will-likely-win
[21] Ibid.
[22] hxxps://bitcoin.org/en/alert/2015-07-04-spv-mining#cause

Threat actors with access to significant mining power can use reorgs to **double-spend**. Double spending is when an attacker sends a transaction to a merchant, receives the product, and submits another transaction sending funds to an address they control. In a successful double spend the miner accepts the second transaction (instead of the first), effectively giving the product to the attacker for free. Double spending with reorgs is possible, but not a certainty as it requires the associated mining power to find blocks faster than legitimate miners. Zero conf payments are theoretically easy to double spend because a miner is incentivized to prefer a larger transaction fee over an older transaction. Zero conf or low confirmation payments are acceptable if the amount transacted is negligible or the receiver trusts the sender to not attempt a double spend.

Reorgs can cause significant disruptions, but do not compromise the security of settled funds in the network.[23] Manipulation by a majority miner or individual miners can not access or send funds from wallets in this scenario.[24] The maximum known effect from such an attack would allow erasing unsettled transactions, possibly double spending, and delaying transactions.[25] This is known as a **51% attack**, although technically an attack with less than half of the network's processing power is still possible. As a miner's processing power increases relative to the total processing power in a cryptocurrency network, the ease of pulling off these effects increases as well.[26] The feasibility of these attacks can vary by cryptocurrency. For example, with Bitcoin's current mining difficulty levels, an attack is extremely unlikely even for the most well-equipped threat actors.[27]

### *2.1.6 Accounts*

An **account** (also known as an **address** or **wallet address**) can be thought of as a single container for holding cryptocurrency. A **wallet** is a collection of accounts, typically associated by a single **hierarchical deterministic key** (also known as **Xpriv**, **seed***,* or **mnemonic phrase**).[28] Each address is a publicly shareable string of letters and numbers, usually between 26 and 64 characters. Addresses use different lengths depending on the cryptocurrency. Many cryptocurrencies choose a letter or number to prefix all addresses, e.g. all Bitcoin addresses start with '1' or '3'. This address is used to receive funds from anyone that knows it, like an email address. For example, a Bitcoin address looks like:

```
1EjhNZjEnbZhhg2nRPwKoHB2SvbHwV1qkN
```

…and the associated **private key** would be:

```
5JiA94EmoK7SDasLfp5HhXvUzBNMGaCvEF546BomgpEYfhXMyPx
```

A private key acts like a password to access an account's holdings. All addresses are (effectively) mathematically derived from a specific private key. However, this derivation is not reversible (i.e. you cannot use an address to generate the private key). The private key is required to cryptographically sign transactions, which is the only way to authorize the spending of funds from an account. The effect is that funds cannot be frozen and the creation of valid transaction strings cannot be prevented.

In many cryptocurrencies, private keys can be combined to form **multisig** (multisignature) addresses. Instead of one private key being used to authorize transactions, multiple private keys must be used in conjunction. Most businesses with significant holdings in cryptocurrency use multisig addresses to mitigate risk.[29] For example, instead of giving an employee complete access to an institution's wallet,

[23] hxxps://learncryptography.com/cryptocurrency/51-attack
[24] Ibid.
[25] Ibid.
[26] Ibid.
[27] Ibid.
[28] hxxps://en.bitcoin.it/wiki/Deterministic_wallet
[29] hxxps://coincenter.org/entry/what-is-multi-sig-and-what-can-it-do

multiple private keys are distributed between multiple custodies.[30] Depending on the specific cryptocurrency, there are varying levels of customization one can use with multisig such as Boolean logic…

```
(private_key_A AND private_key_B) OR private_key_C
```

…or proportional access (e.g. "at least 3 of 5 private keys owned by the board of directors are needed to authorize transactions").

Generating addresses or wallets is done by generating a random private key. This is typically done by a wallet app that allows the user to configure their wallet and store their private key. An account can be created without internet access since there's no announcement of address ownership upon creation. It is possible to receive funds at an address that has never connected to the internet.

Funds are **burnt** when they are at an address of which the private key is lost or unknown. There's no requirement that an account owner still has access to a private key for the wallet to receive funds. Users self-report that millions of dollars worth of funds have been burnt since the inception of cryptocurrency.[31] It's also possible to send funds to an address of which a private key has never been generated. It is virtually impossible to recover settled burnt funds, and therefore it is extremely important to back up private keys.

### *2.1.7 Private Key Management*

Private keys and hierarchical deterministic wallet seeds are highly important and easily portable pieces of data. Decentralized cryptocurrencies have no regulatory oversight and no central authority, and therefore it is virtually impossible to undo a settled transaction of any amount. A business can lose all cryptocurrency holdings almost instantly if their wallets are compromised or funds sent to an incorrect wallet address. It is strongly recommended that any company storing permissionless cryptocurrency follows very strict private key management process.

Consumers, who understand the security risks of hosting their own private keys, store relatively small amounts of cryptocurrency on mobile wallet apps and desktop programs. Most cryptocurrencies use a transparent blockchain in which the balances of addresses in a wallet are publicly visible. Therefore, the amount stored correlates to the risk of targeted attacks. For business holdings, or individuals with a large amount of cryptocurrency funds, there are more secure methods of storage. **Hardware wallets** store private keys on a device that is mostly disconnected from other devices. When a transaction needs to be authorized, the user plugs the hardware wallet into a computer's USB port.[32] The computer will send an unsigned transaction to the hardware wallet to be cryptographically signed, then returning the signed transaction to the computer for broadcast on the network.[33] Although less convenient than a hardware wallet, it is also a good idea to generate a wallet in a virtual environment lacking internet access or booting into an offline operating system. As a general guideline for larger holdings, never generate the private key on an operating system that is connected to the internet or ever will be connected to the Internet.

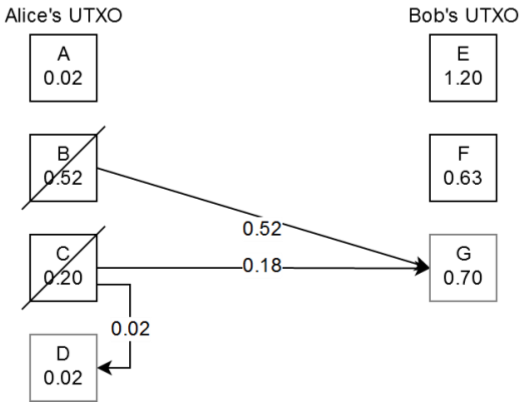
Online wallet services that control key management and may even insure funds are another option for storing and receiving cryptocurrencies. Centralized online exchanges and services are designed to facilitate easy use of cryptocurrencies as well as funding wallets through purchasing cryptocurrencies with fiat currency. However, all wallets and funds on these services are controlled by the operators of the

[30] hxxps://en.bitcoin.it/wiki/Multisignature
[31] hxxp://fortune.com/2017/11/25/lost-bitcoins/
[32] hxxps://support.ledgerwallet.com/hc/en-us/articles/360000617934-How-to-send-and-receive-cryptocurrencies-using-the-Ledger-Nano-S
[33] Ibid.

service. This can expose those wallets and funds to exit scams by malicious operators. Security is also the responsibility of the service's operators, and a compromise of their systems can allow outside threat actors to initiate transfers of customers' funds. For example, Japan-based exchange Coincheck experienced a compromise in January 2018 where approximately $500M USD of the NEM cryptocurrency was stolen from the exchange's wallets.[34]

### *2.1.8 Transactions*

A **transaction** (often abbreviated **tx**) is a movement of funds between two or more addresses. From a high level, it is possible to think of cryptocurrency transactions as moving value from one container to another. However, the technical details are more complex. Many cryptocurrencies (such as Bitcoin) use **outputs** in the **UTXO set** (unspent transaction outputs set) to determine the movement of funds throughout multiple transactions. The sum of unspent outputs an address has is the balance. A diagram is best used to explain:



1. Alice sends 0.70 BTC to Bob. (Transaction fees are omitted for this example.)
2. Her B output is depleted.
3. Her C output is also depleted.
4. Since not all of her C output is needed, two outputs are created: the necessary amount to Bob, and the rest to herself as new output D. The new output to herself is known as **change**.
5. Bob has new output G that he can spend, increasing his balance from 1.83 BTC to 2.53 BTC.

A **transaction fee** is the amount claimed by a miner for processing a transaction. The transaction fee is set by the user sending the transaction, but the miner decides whether to include it in the next block. Blocks of transactions are limited in size; Bitcoin, for example, uses 1 MB. This creates the **fee market**, which is the competition between transaction senders to be included in the limited block space. If the fee included in a transaction is too low, then the miner will choose to include a different transaction that has a higher fee. The competition is multifaceted: transaction fees pay a large role, but so does the size. In practice, transactions can have as few as one input, or as many as hundreds. The more inputs/outputs a transaction has, the larger the size of the transaction will be. In Bitcoin, each input costs 181 bytes, each output costs 34 bytes, and every transaction has an additional 10 bytes added. Therefore, the smallest transaction size is 225 bytes. Miners are incentivized to include transactions that are balanced between low in size and high in fee. In cryptocurrencies with fees and the UTXO model, small outputs that would cost more in fee to spend than the value itself are called **dust**.

[34] hxxps://motherboard.vice.com/en_us/article/ne4xdk/a-cryptocurrency-theft-bigger-than-mt-gox-just-happened-in-japan-coincheck-nem

There are exceptions to the UTXO set model of storing currency. Most notably is Ethereum, which stores a list of balance and address pairs as the current state of the network.[35]

### *2.1.9 Monetary Policy*

Decentralized cryptocurrencies are unable to have a central issuing authority. New coins are minted and enter circulation based on a specific set of mathematical rules that are different for each currency. Bitcoin is deflationary: the number of newly minted coins in blocks halves every four years until the network is left with a grand total of 21M units.[36,37] Monero is slightly inflationary by adding a decreasing amount of new XMR into circulation every minute in the form of block rewards.[38] Many centralized cryptocurrencies or project-oriented tokens are **pre-mined** by a central authority and distributed manually.[39]

### *2.1.10 Future Evolution of Blockchain*

"Blockchain technology" has become the umbrella term for decentralized ledgers. However, there are other cryptocurrency projects that use different decentralized ledger methods that are not strictly blockchains, yet retain many of the same effects of a blockchain. These underlying technologies include Tangle, block lattice, and MimbleWimble. These different ledger methods may have advantages in efficiency or other attributes that make them better suited to particular use cases.

Tangle is the decentralized ledger used by the IOTA project. Instead of miners confirming transactions, each individual user in the network must confirm two previous transactions. This creates a pay-it-forward approach to consensus, where the security and efficiency theoretically improves as the number of users increases. The benefits of this protocol include quantum protection, fast transactions, high throughput, and no fees. IOTA's Tangle has one important downside: currently a central "Coordinator" must be used to create transaction finality. The IOTA Foundation intends to find a way to remove the Coordinator in the future. IOTA is geared towards IoT infrastructure message and value transfer instead of being an end-user currency. The Internet of Things (IoT) is a technology that involves connecting large numbers of smart devices together for the purposes of making day to day life more efficient. IOTA is a project attempting to standardize the communication between these devices in a scalable way.

Nano, a DAG cryptocurrency, uses a block lattice to store transactions. The underlying technology gives each account its own blockchain, as opposed to a single blockchain being shared for the entire network. This allows each account to mine send/receive their own blocks, giving Nano unrestricted transaction throughput, a feeless payment system, and much better energy efficiency (there's no mining) compared to traditional cryptocurrencies. Nano consensus uses delegated proof-of-stake (DPoS), which is a model in which users delegate voting power to nodes that catch invalid transactions. Nano is criticized for having a weaker consensus mechanism than blockchain currencies due to its theoretical inability to recover from a 51% attack.

MimbleWimble is an in-development technology that will support the coin Grin. MimbleWimble uses new cryptographic methods that remove the need for addresses and improves scalability by making blockchain history **prunable**. Pruning is the act of removing old transactions from the blockchain that are no longer needed to verify the validity of current transactions. Currently, the biggest downside is that transactions are interactive, meaning that both the sender and receiver must actively communicate to transact. MimbleWimble is in very early development.

[35] hxxps://steemit.com/ethereum/@sagar/understanding-ethereum-part-1
[36] hxxps://www.investopedia.com/news/what-happens-bitcoin-after-all-21-million-are-mined/
[37] hxxps://bitcoinblockhalf.com/
[38] hxxps://getmonero.org/resources/moneropedia/tail-emission.html
[39] hxxps://www.cryptocompare.com/coins/guides/what-is-a-premine/

## 2.2 Cryptocurrency Profiles

****Disclaimer: The cryptocurrency profiles listed are for reference only. The list is not intended to be all-inclusive, nor does the NCFTA expressly endorse any of the listed cryptocurrencies. All end-users should use their own due diligence when evaluating a cryptocurrency.*

### *2.2.1 Bitcoin*

Bitcoin is the original cryptocurrency released in 2008 as published by a whitepaper entitled “Bitcoin: A Peer-to-Peer Electronic Cash System”.[40] It was initially created by Satoshi Nakamoto, a pseudonym for an anonymous entity.[41] The moniker’s involvement reportedly ceased in 2011, and its untouched Bitcoin wallet is currently valued at $6.8B.[42] From then on, the development of Bitcoin has mainly been done by a team of mostly publicly named individuals.[43] This development team works on the reference implementation of the protocol and does not manage or curate the Bitcoin network.[44]

What differentiates Bitcoin from previous attempts at previous digital coin projects is the invention of “Nakamoto Consensus”, which is now known as proof-of-work. This is a practical solution to the long-standing computer science problem of double-spending and copy-able assets in a decentralized network.

Bitcoin is used primarily by legitimate users as an alternative to fiat currency, mainstream investors, investment firms, and criminal actors such as dark web market buyers and sellers. It is commonly used as the de facto reserve currency in the cryptocurrency market, mainly due to its popularity and the length of time it has existed. Nearly all other cryptocurrencies trade against it on most exchanges, and is one of the only supported cryptocurrencies on traditional financial exchanges via indexes such as the Bitcoin Investment Trust (GBTC).[45]

The history of Bitcoin is the longest of any cryptocurrency, lasting almost a decade as of 2018. For a majority of its existence, the price hovered under $400.[46] Around 2012, adoption started to increase as many core cryptocurrency businesses formed, such as Coinbase, BitPay, several exchanges, and various mining pools.[47] Interest in Bitcoin increased in early 2017, including among legitimate investors, with the USD value reaching over $20,000 per unit at its peak.[48]

Around 2015, the block size debate began in the cryptocurrency community. After Bitcoin reached a level of adoption where 1 MB blocks were considered by many to be too small for the growing network, an argument started over whether the Bitcoin block size of 1 MB should be increased. Transaction fees during this time peaked at over $50 per transaction.[49] Many on the core team that developed Bitcoin believed that the size should remain the same and off-chain methods of processing transactions should be developed with the blockchain being a bilaterally netted settlement layer. The opposing side believed that all transactions should be on chain, stating that their own solution favored simplicity and paid tribute to Nakamoto’s intentions. On August 1, 2017, the Bitcoin network split into two separate currencies for each side in the largest instance of a cryptocurrency hard fork to date. Competition between Bitcoin (BTC) and Bitcoin Cash (BCH) still exists. As of June 2018, BCH is valued at 13% of the BTC price.

[40] hxxps://bitcoin.org/bitcoin.pdf
[41] hxxps://www.investopedia.com/terms/s/satoshi-nakamoto.asp
[42] hxxps://www.coindesk.com/information/who-is-satoshi-nakamoto/
[43] hxxps://bitcoin.org/en/development#bitcoin-core-contributors
[44] hxxps://bitcoin.org/en/development
[45] hxxps://quotes.wsj.com/GBTC
[46] hxxps://blockchain.info/charts/market-price?daysAverageString=7&timespan=all
[47] hxxps://en.bitcoin.it/wiki/Comparison_of_mining_pools
[48] hxxps://99bitcoins.com/bitcoin-all-time-high-chart/
[49] hxxps://bitinfocharts.com/comparison/bitcoin-transactionfees.html

Presumably due to the split, BTC now has transaction fees consistent with pre-contention levels. By June 2018, the Bitcoin blockchain reached 171 GB in size.

### *2.2.2 Monero*

Monero's main feature is transaction anonymity. The development team's stated mission is to create technology that is secure, private and decentralized.[50] Only the owner of an account is able to view their balance and incoming/outgoing transactions. This is achieved by utilizing a technology called **ring signatures** where transactions are bundled with multiple signers so that ownership is theoretically untraceable.[51] A **ring size** determines the number of signers for a transaction, and a larger size results in more anonymity, to an extent.[52] A standard ring size is seven, which according to most users, provides an acceptable level of anonymity.

Some issues in Monero may allow it to be tracked under certain circumstances. An actor may use a unique ring size that could be used to weakly link suspicious transactions. One feature of Monero is the use of **integrated addresses** which are addresses derived from a wallet address along with a specific payment identifier.[53] It's possible that an actor may not realize this, and could publish an integrated address that could be strongly linked with other integrated addresses. If an investigator has a transaction hash, they could determine (within 2-3 minutes) when that transaction occurred by searching it in a Monero block explorer. 62% of Monero transactions prior to February 2017 are traceable due to a protocol weakness that was changed.[54] Centralized exchanges will know the balance of an address for an account, addresses to which have been withdrawn, amounts of the withdrawals, and amounts from trades. Many exchanges will also have a copy of a user's IP address, moniker, and/or contact information.

### *2.2.3 Ethereum*

Ethereum is a smart contracts platform developed by the Ethereum Foundation and includes a cryptocurrency called Ether. The Ethereum Foundation is operated by publicly-known members.[55] User-created **smart contracts** are a secure, self-executing, and trustless type of digital contracts that are built upon the Ethereum platform. Smart contracts can range from simple currencies to complex organizations complete with a governance structure. Most smart contracts on Ethereum are **tokens**, which are virtualized currencies that are secured along with the rest of Ethereum. Anyone can create a token with Ethereum for very little cost. Tokens are very popular for trading as currencies and as fuel for smart contracts. (See "Profile: Ethereum Foundation and the Enterprise Ethereum Alliance")

### *2.2.4 Litecoin*

Litecoin was released in 2011 and is similar in function to Bitcoin, but lower in price and adoption.[56] Litecoin is frequently used as a vehicle to move temporary funds between exchanges due to its low fees and quick block times. It is widely regarded as the first successful cryptocurrency alternative to Bitcoin.

### *2.2.5 Comparing Privacy Coins*

Implementing privacy features in cryptocurrencies can take the form of several techniques. The three most prominent methods are:

[50] hxxps://getmonero.org/resources/about/
[51] hxxps://en.wikipedia.org/wiki/Ring_signature
[52] hxxps://getmonero.org/resources/moneropedia/ring-size.html
[53] hxxps://monero.stackexchange.com/questions/3179/what-is-an-integrated-address
[54] hxxps://monerolink.com/
[55] hxxps://ethereum.org/foundation
[56] hxxps://en.wikipedia.org/wiki/Litecoin

- Mixing (used by Dash PrivateSend)
- zk-SNARKS (used by Zcash)
- Ring Signatures (used by Monero)

Dash's PrivateSend is an optional feature built on top of the normally transparent cryptocurrency. Users that wish to transact with added privacy must first mix their coins, which is security by obfuscation.[57] Mixing involves a user's wallet communicating with masternodes on the network, which will then mix with other users that want to anonymize their coins as well.[58] Mixing must be done in denominations of 0.01, 0.1, 1, or 10 DASH.[59] This process takes several hours. PrivateSend is often criticized for being an incomplete solution to privacy method and potentially exposing PrivateSend information to masternodes. The Dash PrivateSend feature is used on 0.5% of all Dash transactions.[60]

zk-SNARKS, as used in Zcash, is a more secure model of privacy than Dash PrivateSend. However, despite the currency being marketed as privacy-focused, only 14% of transactions use the "shielded transaction" feature to add anonymity.[61] Lack of adoption of the main Zcash feature could be due to an immense amount of processing power required to use the address format in the wallet. Academic research concluded that users that transact with shielding are, at least partially, identifiable by chain analysis due to the small number of users who utilize the optional feature.[62,63]

Monero uses ring signatures to combine user transactions together, such that it is very difficult to determine which transactions are relevant. The transactions used for combination can be from any point in the blockchain history. Ring signatures have gone through years of research as a general cryptography concept.[64] In addition, Monero uses Ring CT to hide the amounts in transactions.[65] All of these features together create an opaque blockchain. Anonymity with Monero is not optional, therefore all coins are fungible and the volume of money within the blockchain is unknown.[66]

Monero accounts for 95% of the private currency market, after weighting the market capitalizations of these privacy coins by the percentage of transactions in each that use the respective privacy features. Market capitalization is usually an inaccurate metric, but since anonymous transaction amounts cannot be seen, it can be an adequate method of estimating usage. Monero and Dash seem to be decoupling from the price of Bitcoin, which could potentially indicate increased organic usage (see Appendix 3.7 for a chart).[67]

### *2.2.6 Comparison Table*

The below table is a snapshot of a few popular cryptocurrencies and details about the respective ecosystems:

| | **Market Capitalization** | **Daily Transaction Volume** | **Smart Contracts** | **Consensus** | **Transparent Blockchain** | **Central Authority** | **Current Use** |
|---|---|---|---|---|---|---|---|

[57] hxxps://docs.dash.org/en/latest/introduction/features.html#privatesend
[58] Ibid.
[59] Ibid.
[60] hxxps://dashradar.com/charts/privatesend-transactions-per-day
[61] hxxps://explorer.zcha.in/statistics/network
[62] hxxps://smeiklej.com/files/usenix18.pdf
[63] hxxps://deepblue.lib.umich.edu/bitstream/handle/2027.42/143130/quesnelle-thesis.pdf?sequence=1&isAllowed=y
[64] hxxps://link.springer.com/chapter/10.1007%2F11424826_65
[65] hxxps://lab.getmonero.org/pubs/MRL-0005.pdf
[66] hxxps://getmonero.org/get-started/what-is-monero/
[67] hxxps://www.sifrdata.com/cryptocurrency-rolling-correlations/

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Bitcoin** | $116B (#1) | $5.35B[68] | Limited | PoW | Yes | No | Digital currency, investing firms, settlement. |
| **Ethereum** | $52B (#2) | $1.24B[69] | Turing Complete | PoW | Yes | No | ICOs, investing firms, decentralized applications. |
| **Ripple (Public Currency)** | $22B (#3) | $18.76B[70] | No | Validators | Yes | Yes | Interbank settlement, B2B transactions. |
| **Litecoin** | $4.5B (#6) | $0.22B[71] | Limited | PoW | Yes | No | Arbitrage, digital currency. |
| **Monero** | $2.1B (#13) | Unknowable | No | PoW | No | No | Digital currency, illicit payments, asset haven. |
| **Dash** | $2.0B (#14) | $0.05B[72] | No | PoS | Optional | Yes | Digital currency, illicit payments. |

## 2.3 Criminal Uses

### *2.3.1 Illicit Payments*

Decentralized cryptocurrencies are an ideal method of payment for illegal purchases. Anyone can start using them without prior permission, and decentralized cryptocurrencies are not subject to regulations or procedures that can prevent illicit use as with regular financial transactions. Privacy coins like Monero are anonymous, which adds a new layer of difficulty for law enforcement and regulatory efforts. For the most part, all illicit goods that can be purchased with traditional currencies can also be purchased with cryptocurrencies. In 2016, research indicated that 9.3% of drug users bought drugs from dark net vendors with these numbers likely to increase.[73] A 2017 Europol report stated:

> Cryptocurrencies continue to be exploited by cybercriminals, with Bitcoin being the currency of choice in criminal markets, and as payment for cyber-related extortion attempts, such as from ransomware or a DDoS attack. However, other cryptocurrencies such as Monero, Ethereum, and Zcash are gaining popularity within the digital underground.[74]

High fees and settlement times for Bitcoin led to dark web actors using other cryptocurrencies more frequently.[75,76] Bitcoin remains the primary payment method for dark web transactions, though confidence in the cryptocurrency appears to be declining.[77] Litecoin is the second most popular dark web currency and is accepted by 30% of vendors.[78] At least 26% of all dark web transactions are done with an anonymous-capable currency.[79] Researchers in one study predicted that by the end of 2018, Bitcoin will lose its dominant position in dark web markets to Monero, Litecoin, and Dash.[80]

[68] hxxps://coinmetrics.io/charts/#assets=btc_roll=30_left=txVolume
[69] hxxps://bitinfocharts.com/comparison/sentinusd-eth.html#3m
[70] hxxps://coinmetrics.io/charts/#assets=xrp_roll=90_left=txVolume
[71] hxxps://coinmetrics.io/charts/#assets=ltc_roll=90_left=txVolume_zoom=1521504000000,1529280000000
[72] hxxps://coinmetrics.io/charts/#assets=dash_roll=90_left=txVolume
[73] hxxps://nulltx.com/the-role-of-cryptocurrency-in-crime-darknet-activity-soars/
[74] hxxps://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017
[75] hxxps://www.cnet.com/news/bitcoin-wont-be-the-dark-webs-top-cryptocurrency-for-long/
[76] hxxps://darkwebnews.com/cryptocurrency/darknet-users-abandon-btc/
[77] hxxps://www.recordedfuture.com/dark-web-currency/
[78] Ibid.
[79] Ibid.
[80] Ibid.

### *2.3.2 Unregulated Trading*

Cryptocurrency trading features lower barriers to entry and fewer regulations than regular asset trading. An email address is typically all that is needed to set up an account on a cryptocurrency exchanger or trading website. Most of these services do not impose waiting periods or a requirement to connect the exchange account to a bank account. They also do not impose region restrictions. Most exchanges operate globally. Regulation or trader protections on these exchanges are uncommon.[81] However, some regulations and legal definitions may apply according to national laws. For example, the U.S. Securities and Exchange Commission (SEC) classifies cryptocurrencies as securities.[82] Services that engage in cryptocurrency trading are subject to U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) regulations pertaining to money services businesses (MSBs.)[83]

Cryptocurrencies can function as a method of holding funds without bank/government knowledge, and thus without paying taxes. Currently there is no way to pay taxes with cryptocurrency. Cryptocurrency mining income is also often not reported because the coins generated are not fiat currency and may not be covered by regulations or laws in the miner's home country. Cryptocurrency payments and income are addressed by the U.S. Internal Revenue Service (IRS.) All cryptocurrency payments over $600 need to be reported to the IRS.[84] This is filed through a standardized tax form, Form 8949.[85] More than a third of cryptocurrency investors in one survey knowingly omitted capital gains on their 2017 taxes and only 1 in 3,500 Americans that owned any Bitcoin reported their holdings on their 2015 taxes per a second survey.[86]

### *2.3.3 Money Laundering*

Cryptocurrency offers a relatively easy and private way to send illicit funds globally especially when privacy coins such as Monero and Zcash are used. There are no global standards for AML programs within cryptocurrency exchanges, and exchanges' policies can range from holding no information on a user to full AML compliance.[87]

Criminal actors can use cryptocurrencies to launder money by starting with the purchase of widely traded coins (e.g. BTC, ETH, and LTC) with a bank account, Bitcoin ATM, or decentralized physical exchange such as LocalBitcoins. For added privacy, an actor may use an anonymous VPN and encrypted mail service. After using illicit funds to acquire cryptocurrency, an actor may use a **tumbling** service (also known as a **mixer**) to obfuscate the blockchain records, which will combine actors' funds and return funds in varying amounts to new addresses at an average fee of about 2%.[88,89] From there, the coins are traded for privacy coins, such as Monero or Zcash, where they are stored until the funds are needed. To withdraw value, an actor will convert their privacy coins back into primary coins on a different exchange account and then sell them for fiat currency or use them to make purchases. Purchases may include physical goods or property that is used or resold by the threat actors, or illicit goods from online underground markets such as drugs or stolen data.

[81] hxxps://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading
[82] Ibid.
[83] hxxps://www.fincen.gov/news/news-releases/fincen-issues-guidance-virtual-currencies-and-regulatory-responsibilities
[84] hxxps://www.irs.gov/pub/irs-drop/n-14-21.pdf
[85] hxxps://nulltx.com/the-role-of-cryptocurrency-in-crime-darknet-activity-soars/
[86] Ibid.
[87] hxxps://www.reuters.com/article/bc-finreg-aml-cryptocurrency/crypto-cleansing-strategies-to-fight-digital-currency-money-laundering-and-sanctions-evasion-idUSKCN1FX29I
[88] hxxps://bitcoin.stackexchange.com/questions/17807/what-is-a-bitcoin-tumbler#17809
[89] hxxps://cdn2.hubspot.net/hubfs/4345106/crypto_aml_report_2018q2.pdf

Law enforcement is beginning to pursue money laundering that uses cryptocurrency. In June 2018, the first ever Bitcoin money laundering sting resulted in 40 arrests and $3.6M in cryptocurrency confiscated.[90] HSI agents posed as a money laundering service to multiple dark net vendors involved with narcotics trafficking.[91] The money laundering was done via trading cryptocurrency for cash sent through the mail.[92] Previous cases included the takedown of exchange service BTC-e and the arrest of its operator following coordinated U.S. and Greek law enforcement action.[93] The operator was charged with 21 counts for allegedly operating a money laundering scheme that moved over $4 billion in cryptocurrency.[94]

Chain analysis tools can be used to track the movement of transparent blockchain cryptocurrencies. Blockchain **taint** is the measure of how many coins in an address originated from another specific address.[95] Elliptic and Chainalysis displays addresses and transactions visually to assist with investigation.[96,97] Since 2015, the FBI has spent more than $330k on Chainalysis products.[98]

There are several potential cryptocurrency-unique methods of laundering money. One involves an actor purchasing a mining contract or mining hardware with dirty funds, then reporting the mining profit as clean income. The Philippines has issued regulation attempting to end cloud due to its potential to break anti-money laundering laws.[99] Gambling services are sometimes used as the final destination for laundered cryptocurrency. 12.2% of laundered cryptocurrency ended up being gambled according to a 2016 survey, and there are up to 200 active cryptocurrency gambling sites.[100,101]

### *2.3.4 Cryptojacking*

**Cryptojacking** is the unauthorized use of processing power for cryptocurrency mining.[102] This can be done either by malware running on a victim's system, or malicious code placed on a compromised website that forces visitors' systems to mine. By June 2018, there were as many as 2.9M reported cryptojacking detections, which is a growth of 629% from Q4 2017.[103] In China, a piece of malware spread via browser plug-ins to over a million computers netted attackers about $2 M over the course of two years.[104] This form of malware has grown in recent years as the value of non-ASIC coins increased. Threat actors attempt to mine non-ASIC coins using infected systems due to their ease of mining on typical victim systems. Once a hacker infiltrates a network, they can put mining software on as many computers as they can access since CPU mining can run on virtually any device. Cryptojacking malware can be spread in any of the ways other types of malware can be spread, such as malicious phishing

[90] hxxps://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged
[91] hxxps://www.theverge.com/2018/6/27/17509444/dark-web-drug-market-money-laundering-hsi-dark-gold
[92] Ibid.
[93] hxxps://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged
[94] Ibid.
[95] hxxps://bitcoin.stackexchange.com/a/48356
[96] hxxps://www.elliptic.co/about
[97] hxxps://www.chainalysis.com/
[98] hxxps://motherboard.vice.com/en_us/article/7xz35e/us-law-enforcement-have-spent-hundreds-of-thousands-on-bitcoin-tracking-tools
[99] hxxp://www.sec.gov.ph/advisory-on-cloud-mining-contracts/
[100] hxxps://nulltx.com/the-role-of-cryptocurrency-in-crime-darknet-activity-soars/
[101] hxxps://cdn2.hubspot.net/hubfs/4345106/crypto_aml_report_2018q2.pdf
[102] hxxps://hackerbits.com/programming/what-is-cryptojacking/
[103] McAfee Labs Threat Report, June 2018
[104] hxxps://www.coindesk.com/1-million-computers-hacked-to-mine-2-million-worth-of-cryptos/

attachments, download via dropper malware, exploit kits, or RDP access. Cryptojacking web page scripts are also deployed by the same methods websites can be compromised by other types of attacks, including by accessing poorly secured content management systems or website vulnerabilities. A unique feature that needs to be considered when defending against this attack is that most implementations of cryptojacking do not have any call-home requests. Access to the victim's hardware is the goal of these attacks, rather than access to the data on the system or its connections with other systems.

Threats to victim's systems take several forms. Any system or website compromised to run a cryptojacker could also be compromised for other uses. Access to the system has been obtained and threat actors may conduct other actions such as steal data, establish a backdoor, deploy additional malware, or delete files prior to activating a cryptojacker. Cryptojackers can also result in a denial of service (DoS) state as the malware causes slow downs and service disruptions. The high strain placed on compromised systems can also cause physical damage. CPUs and GPUs constantly running at a high load due to mining may become damaged or degrade at a faster than expected rate, leading to service outages and increased costs. The increased energy use of compromised systems can also impose additional costs on an impacted victim.

JavaScript miners can be injected into web pages via browser add-on, framework plug-ins, or the served page code itself.[105] In particular the CoinHive mining script for Monero made browser-based mining more accessible for threat actors.[106] Incidents of browser-based mining grew significantly following CoinHives public release in September 2017.[107] It's worth mentioning that JavaScript miners have potentially positive uses as an alternative to on-site advertising or micropayments, but CoinHive's popularity as an attack tool is undeniable. CoinHive mining code is often delivered via embedded page advertisements, also known as malvertising.[108] One notable incident was when CoinHive was able to be deployed through YouTube via malicious DoubleClick ads in videos.[109]

Cryptojacking is detectable. A running piece of cryptojacking malware will need to be connected with other cryptocurrency nodes to receive and broadcast block information. There may be a default port used for this communication, which could aid in detection. The miner will need to receive regular similarly-size packets of data from other nodes since it needs the latest block data to engage in mining.[110] If the mining software is connecting to specific IPs every time, it may be connecting to a hard-coded node. By definition, mining involves spending computing power so the most telltale sign of mining is unusually high CPU usage by a browser or unknown process.[111] Miners often use a mining pool, which is a method to allow multiple devices to contribute to the same mining work, connected to through a specific URL. A system would only connect to a mining pool URL to engage in mining.

In practice, the most popular cryptocurrency for cryptojacking is Monero.[112] Monero is a non-ASIC coin with a relatively low barrier of entry for low-powered devices to mine. The cryptocurrency is also designed to be anonymous, so the mining profit receiving address will not yield useful information in blockchain analysis. However, mining pool addresses can be identified by analyzing the mining malware, potentially offering clues to the threat actor's identity or other mining activity (see "Profile: Monero".)

[105] hxxp://www.cbc.ca/news/technology/cryptojacking-mining-1.4572360
[106] hxxps://coinhive.com
[107] hxxps://www.bleepingcomputer.com/news/security/the-internet-is-rife-with-in-browser-miners-and-its-getting-worse-each-day/
hxxps://www.bleepingcomputer.com/news/security/report-three-of-top-four-malware-threats-are-in-browser-cryptocurrency-miners/
[108] NCFTA Cryptocurrency Miners Report
[109] Ibid.
[110] hxxps://securityboulevard.com/2018/04/how-to-stop-cryptomining-and-cryptojacking-attacks/
[111] hxxps://www.which.co.uk/news/2018/02/cryptojacking-how-your-pc-can-be-hacked-to-mine-bitcoin-for-others/
[112] hxxps://blogs.cisco.com/security/cryptojacking-hijacking-your-computer-resources

Prevention and mitigation of cryptojacking malware can take specific and general forms. Browser add-on such as NoCoin can be used to prevent mining scripts from running.[113] Cryptojacking malware is deployed onto a system much like any other type of malware, so typical malware protection practices apply such as regular patching, use of antivirus software, traffic analysis, and other methods.

Cryptojacking attacks will likely continue to rise and perhaps overtake ransomware in total number of attacks. Cryptojacking offers criminals a potentially more profitable and less detectable form of cybercrime compared to ransomware.[114] It also may attract less attention from law enforcement since it typically does not cause overt disruptions or damage to the victim's systems and thus may be reported less frequently. However, cryptojacking attacks are dependent upon the value of easily-minable cryptocurrencies. The frequency of cryptojacking attacks could be impacted should these cryptocurrencies' values fall or their mining become more difficult.

### *2.3.5 Malware*

Cryptocurrencies play a significant role in two other types of cyberattacks. Ransomware is malware that encrypts a user's entire drive and requires a payment to release the private key to access files again. This payment evolved over time from traditional financial instruments such as pre-paid debit cards or money transfer services, to cryptocurrency. Bitcoin remains the most common cryptocurrency demanded as ransom payment due to its widespread use among both legitimate and criminal users. Cryptocurrency made ransomware a viable criminal business model for two main reasons. Use of Bitcoin standardized a method of payment for ransoms, in contrast to past use of various payment systems. The growth of exchanges, Bitcoin ATMs, and other services made Bitcoin and other cryptocurrencies more accessible to the general public. Thus ransomware actors were able to standardize one set of instructions to their victims using a relatively easy to obtain cryptocurrency

Cryptocurrency wallets can also be directly targeted by malware, or with simple social engineering. These types of attacks can be attractive for threat actors due to the irreversible nature of cryptocurrency transactions and ambiguity in some jurisdictions over how to report and investigate cryptocurrency thefts. Threat actors who obtain access to a user's private keys or that can execute or trick their victims into executing transactions can potentially obtain significant amounts of cryptocurrency in a short amount of time. Clipboard malware can detect cryptocurrency addresses in the victim's clipboard and replace them with a wallet address controlled by the threat actor.[115] Clipboard malware is typically hardcoded with a list of wallets controlled by the threat actor and will substitute a wallet address in the clipboard with one of its own when the 'paste' command is input. This works because cryptocurrency addresses are not human-friendly to read, and it is difficult for most users to notice differences in the address. A similar attack can occur when a website displaying a wallet address is compromised and a different wallet address is substituted by the threat actor. Users wishing to purchase ICO tokens then send their funds to a wallet the threat actors control. This is a common scenario during ICO events.[116] More sophisticated wallet malwares will search the victim computer for unencrypted wallet files, look for un-patched wallet instances running, or inject malicious code into the browser via a man-in-the-middle phishing scheme in order to gain access to wallets or exchange accounts.[117] Often times, cryptocurrency wallet stealing malware is

[113] hxxps://chrome.google.com/webstore/detail/no-coin-block-miners-on-t/gojamcfopckidlocpkbelmpjcgmbgjcl?hl=en
[114] McAfee Labs Threat Report, June 2018
[115] hxxp://marketing.blueliv.com/asset/5:blueliv-the-credential-theft-ecosystempdf
[116] hxxps://www.cnbc.com/2017/07/17/coindash-website-hacked-7-million-stolen-in-ico.html
hxxps://www.bleepingcomputer.com/news/cryptocurrency/scammers-steal-over-1-million-worth-of-ethereum-from-bee-token-ico-participants/
[117] Ibid.

included as a module of more well-known types of malware, such as Andromeda, TrickBot, or Emotet/Geodo.[118]

By July 2018 YTD, almost $1.2 B in cryptocurrency had been stolen by cyber criminals, which almost three times as much that was stolen in all of 2017.[119]

## 2.4 Business Ecosystem

Comparing the importance or usage of cryptocurrencies based on market capitalization can be misleading. The price of a cryptocurrency is often not correlated with innovative features, development progress, or real usage. Currently, most cryptocurrency prices are solely based on marketing and speculation.

### *2.4.1 Centralized Exchanges*

Exchanges are online services that enable users to buy, sell, and exchange cryptocurrencies using fiat currency or other cryptocurrencies. These often serve as the starting point for new cryptocurrency users. A vast majority of trading volume occurs on centralized exchanges run by private organizations.[120] Exchange revenue comes from a maker/taker fee charged per trade, which is typically below 1%. Some exchanges even create their own cryptocurrency specifically for inner-exchange workings and trading fees.[121] There are hundreds of such exchanges, but few have meaningful volume. Below is a list of some exchanges:

| Exchange | Headquarters | Normal 24h Volume[122] |
|---|---|---|
| Binance[123] | Hong-Kong | $1,100 M |
| Huobi | Hong-Kong | $800 M |
| Bitfinex[124] | Hong-Kong | $750 M |
| HitBTC | Hong-Kong | $250 M |
| Coinbase Pro[125] | United States | $200 M |
| Poloniex[126] | United States | $50 M |
| Gemini[127] | United States | $25 M |

(USDT is valued the same as USD, but exists in the form of a cryptocurrency called Tether. See “Tether” profile for more information.)

Full custody of the traders’ funds is held by the exchange and not the traders. Exchanges are therefore lucrative targets for threat actors. In the past, several exchanges have been compromised, resulting in millions of dollars worth of cryptocurrency lost to unauthorized transfers.[128] However, some users and open source reporting speculate that some of these apparent thefts were in fact conducted by exchange

[118] Ibid.
[119] hxxps://cdn2.hubspot.net/hubfs/4345106/crypto_aml_report_2018q2.pdf
[120] hxxps://cryptocoincharts.info/markets/info
[121] hxxps://coinmarketcap.com/currencies/binance-coin/
[122] hxxps://cryptocoincharts.info/markets/info
[123] hxxps://www.binance.com
[124] hxxps://www.bitfinex.com
[125] hxxps://www.gdax.com
[126] hxxps://www.poloniex.com
[127] hxxps://www.gemini.com
[128] hxxp://fortune.com/2018/02/11/bitgrail-cryptocurrency-claims-hack/

operators themselves.[129] This reflects the frequent lack of trust in the cryptocurrency world due to a lack of central authority and regulations to help protect users' funds.

Cryptocurrency prices remain volatile and have been over the course of cryptocurrencies' history. Cryptocurrencies do not enjoy the backing of a central reserve and can not be subject to monetary policy. However, a general relationship between the price of Bitcoin and the price of other cryptocurrencies has brought their values into a rough dependency or alignment. Almost all cryptocurrencies follow the price of Bitcoin via a strong positive correlation (see Appendix 3.9).[130] It remains the top by market cap, the most used in daily transaction volume, is supported by the most raw network processing power, and is the most frequently used by legitimate investors.[131,132] Bitcoin's central position and longer history means its price often influences the price of other cryptocurrencies. As of June 2018, Bitcoin accounted for about 40% of the total cryptocurrency ecosystem market cap.[133] Bitcoin's price may decouple from that of Ethereum, Litecoin, and other popular currencies that may serve as a more convenient exchange medium. This is commonly referred to as **the flippening** in the cryptocurrency community.[134]

In August 2018, Intercontinental Exchange Inc (ICE, owner of the New York Stock Exchange) announced plans to form a regulated exchange for digital asset and is working closely with Microsoft and Starbucks to enable mainstream trading, storage, and spending of cryptocurrencies.[135,136] Named Bakkt, the new exchange aims to bring institutional investors to this new asset class on a global scale.[137] Shortly after the announcement of Bakkt, Germany's second largest stock exchange, Boerse Stuttgart, announced that they would be developing an ICO platform, trading platform, and a custodial wallet service.[138]

### *2.4.2 Decentralized Exchanges*

Decentralized exchange services also exist, and may include physical locations. LocalBitcoins is an example of this type of exchange. The service allows cryptocurrency buyers and sellers to identify each other, communicate, and then conduct transactions in cash.[139] A price mark-up of approximately 0-2% is charged on the transactions.[140]

Another form of decentralized exchange service is Bitcoin ATMs. Bitcoin ATMs are machines that accept USD cash and send Bitcoin to the purchaser. Bitcoin ATMs have spread quickly since 2015, with a total of 2,662 machines worldwide.[141] Bitcoin ATMs appeal to some customers due to the ease of processing transactions and relative anonymity. Some Bitcoin ATMs allow users to sell their Bitcoin for cash, potentially providing a system for criminals to enter and exit cryptocurrency. The premiums on cash-to-cryptocurrency ATMs are typically high compared to other exchange services, averaging approximately

[129] hxxps://www.coindesk.com/missing-mt-gox-bitcoins-inside-job-japanese-police/
hxxp://time.com/money/5056652/the-70-million-bitcoin-hack-was-the-4th-largest-breach-in-cryptocurrency-history/

[130] hxxps://www.sifrdata.com/cryptocurrency-correlation-matrix/

[131] hxxps://coinmarketcap.com/currencies/bitcoin/

[132] hxxps://bitcoinwisdom.com/bitcoin/difficulty

[133] hxxps://coinmarketcap.com/charts/#dominance-percentage

[134] hxxps://motherboard.vice.com/en_us/article/gypwqq/bitcoiners-are-freaking-out-over-the-flippening

[135] hxxps://www.businessinsider.com/bitcoin-platform-by-ice-could-lure-wall-street-institutions-2018-8

[136] hxxps://www.reuters.com/article/us-ice-cryptocurrency-bakkt/nyse-owner-ice-to-form-new-company-for-digital-assets-idUSKBN1KO1QN

[137] Ibid.

[138] hxxps://ci.covesting.io/news/cryptocurrency-news/german-stock-exchange-announces-crypto-infrastructure

[139] hxxps://www.localbitcoins.net

[140] hxxps://data.bitcoinity.org/markets/arbitrage/USD

[141] hxxps://www.statista.com/statistics/343127/number-bitcoin-atms/

9%.[142] About half of these machines support non-Bitcoin cryptocurrencies, such as Litecoin, Ether, and Dash.[143]

There are digital decentralized exchanges, but they have low levels of adoption. Some implementations of decentralized exchanges are built on the Ethereum platform for trading only Ethereum tokens. There are a few unique qualities of most decentralized exchanges:

- No personal information required. Identities are cryptographic addresses in a smart contract.
- Designed to be more secure from external and internal threats
- Low trading fees
- No central point of failure that could cause an exchange to go offline

Examples of decentralized exchanges include Bisq, OpenBazaar, EtherDelta, Bancor, cross blockchain atomic swaps, and a project by Binance slated for release in late 2018.[144,145,146,147,148,149] Some decentralized exchanges are run by DAOs, which can lead to difficulties regulating the exchange of digital assets (see "Decentralized Autonomous Organizations").

### *2.4.3 Initial Coin Offerings (ICOs)*

Initial coin offerings (ICOs) are a fundraising mechanism where a prospective company or product seeks funding by offering tokens, which function in a similar way to stocks issued in an initial public offering. Investors can purchase tokens during or ICO or use exchanges to acquire these tokens, and they are traded like shares in a company. Their value can increase as more investors join the market or the product gains a following. ICOs can be used for legitimate funding purposes. However, a large portion of ICOs are scams, pyramid schemes, or pump-n-dumps.[150] Creating new tokens and organizing an ICO is a relatively simple process, which can allow threat actors to take advantage.

In just the first few months of 2018, there have been 480 ICOs that have raised a cumulative $1.66B.[151] It is estimated that about $317 M raised by ICOs was lost to fraud.[152] About 70% of ICO funding volume goes to high quality projects and 80% of ICOs are considered scams.[153]

### *2.4.4 Legal Status*

Legal issues surrounding cryptocurrencies can involve several regulatory jurisdictions, such as trade, business, criminal, and personal finance.

[142] hxxps://coinatmradar.com/charts/#fees
[143] Ibid.
[144] hxxps://bisq.network/faq/#1
[145] hxxps://www.openbazaar.org/features/
[146] hxxps://medium.com/@Edward_Giraffe/decentralized-exchanges-on-ethereum-q1-2018-aa6750ad5d48
[147] Ibid.
[148] hxxps://www.coindesk.com/atomic-action-will-2018-year-cross-blockchain-swap/
[149] hxxp://www.globalcryptopress.com/2018/07/binance-prepares-to-launch-new.html
[150] hxxps://www.bleepingcomputer.com/news/cryptocurrency/81-percent-of-recent-icos-were-scams-research-finds/
hxxps://cointelegraph.com/news/sec-launches-mock-ico-to-show-investors-warning-signs-of-fraud
hxxps://techcrunch.com/2018/04/13/exit-scammers-run-off-with-660-million-in-ico-earnings/
[151] Rep. Bill Huizenga, Virtual Currencies Hearing, March 2018
[152] hxxps://www.wsj.com/articles/sec-launches-cryptocurrency-probe-1519856266
[153] hxxps://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ

As per IRS guidance, like other private currencies, companies are able to do business accepting cryptocurrency as payment.[154] For tax purposes, cryptocurrencies are considered a commodity akin to stocks. Payments and wages must be reported as income on the same tax forms according to the valuation at the time of transaction.[155] Payments made with cryptocurrency are subject to the same reporting as transferring any other property.[156] Much like other commodities, relevant capital gains must be reported as well[157]. Taxation of cryptocurrency transactions and trade activity has been a large issue for the IRS since 2013. Despite more than 14,000 Coinbase users alone transacting more than $20,000 worth of Bitcoin each, only 800 total taxpayers reported any cryptocurrency gains. In November 2017, the IRS served Coinbase to look into the identities of those who did not pay taxes.[158]

There is much legal debate over whether cryptocurrencies are securities with investment potential, or merely for consumptive use (i.e. as a currency). Precedence dictates that a security is defined by: “an investment of money in a common enterprise with a reasonable expectation of profits to be derived primarily from the entrepreneurial or managerial efforts of others.”[159]

No ICOs or coins have been approved, registered with, or reviewed by the SEC.[160] The SEC has further stated that the rapid growth of the ICO market poses risks to investors and potentially complicates SEC efforts to take action against fraudulent actors.[161] Broadly, the SEC asserts that a majority of cryptocurrencies are not securities and are therefore out of their jurisdiction, yet a keen eye will be kept on the progress of this technology. The SEC will continue to watch over ICO funding and cryptocurrencies as investments, which are still subject to procedure and regulation.

In the business world, cryptocurrency startups have different licensing requirements depending on the state.[162] Some states define these businesses as money transmitters, which subjects them to typical the requirements of a financial institution. Other states don’t have any specific regulation at all, introducing a legal grey area where businesses don’t know whether their practices are legal.

A high-level perspective of the legal status of cryptocurrency, by country, can be found in Appendix 3.8.

## 2.5 Blockchain and Cryptocurrency Company Profiles

****Disclaimer: The company profiles listed are for reference only. The list is not intended to be all-inclusive, nor does the NCFTA expressly endorse any of the listed providers. All end-users should use their own due diligence when selecting a company.*

### *2.5.1 Coinbase*

Coinbase is a California-based digital currency wallet platform founded in June 2012 that deals in Bitcoin, Ethereum, and Litecoin.[163] The exchange functions as a broker for cryptocurrencies and aims to provide a user-friendly interface for retail customers. Coinbase has processed approximately $150B in trades and hosts approximately 20M user wallets according to the exchange’s website.[164] The exchange also operates GDAX (Global Digital Asset Exchange) which hosts 12 different trading pairs between BTC,

[154] hxxps://www.irs.gov/newsroom/irs-virtual-currency-guidance
[155] Ibid.
[156] Ibid.
[157] Ibid.
[158] hxxps://corpgov.law.harvard.edu/2018/02/08/cryptocurrency-2018/
[159] SEC v. W.J. Howey Co., 328 U.S. 293, 301 (1946)
[160] hxxps://www.sec.gov/news/public-statement/statement-clayton-2017-12-11
[161] Ibid.
[162] hxxps://www.bitcoinmarketjournal.com/bitcoin-state-regulations/
[163] hxxps://support.coinbase.com/customer/en/portal/articles/2630943-supported-digital-currencies
[164] hxxps://www.coinbase.com/about

LTC, ETH, USD, EUR, and GBP.[165] The Coinbase wallet service is available in 190 countries, and the exchange service is available in 31 countries and most states.[166,167]

Coinbase's stated aim is to provide easy-to-use cryptocurrency services to the non-technical general public and custodial service for company holdings.[168]

### *2.5.2 BitPay*

BitPay is a cryptocurrency payments processing company that was founded in May 2011 and headquartered in Atlanta, Georgia.[169] BitPay's main service is providing Bitcoin and Bitcoin Cash wallet hosting for businesses that wish to accept cryptocurrency, but prefer to have a service handle the actual transactions, storage, and currency exchanging. BitPay customers have the option of automatically converting all or a portion of the cryptocurrency they receive to fiat currency. The fee for their merchant service is 1% on transactions.[170] BitPay also offers a cross-border blockchain payments service that is intended to compete with wire transfers and claims to offer lower costs and next day bank settlement.[171] In 2016, BitPay began to offer a Bitcoin debit card that enables users to spend their Bitcoin anywhere Visa cards are accepted using an instant currency conversion process.[172] In late 2016, BitPay reported processing 200,000 transactions for these cards monthly.[173] The company develops and maintains the BitPay Wallet app and the Copay wallet app for multisignature addresses. BitPay maintains partnerships with several retail services, including Microsoft, Newegg, and TigerDirect.[174] The service also supports the open source projects BitCore and Insight, which are a Bitcoin node implementation and a block explorer respectively.[175]

### *2.5.3 Ripple Company*

Ripple is an institutional payments company founded in 2012 and based in California. Their stated mission is to provide a backbone settlement and payments network to financial institutions using blockchain technology.[176] Ripple offers three main products: xCurrent, xRapid, and xVia. xCurrent is a payment settlement platform for banks designed to compete with SWIFT on price and ease of use.[177] The xRapid service is designed to lower capital requirements when transacting in emerging markets.[178] xVia is a service that enables real-time global invoice payments for business customers based on an API.[179]

[165] hxxps://support.gdax.com/customer/en/portal/articles/2424961-what-is-gdax-
[166] hxxps://support.coinbase.com/customer/portal/articles/1392031
[167] hxxps://support.gdax.com/customer/en/portal/articles/2425188-which-countries-and-states-can-access-gdax-?b_id=13522
[168] hxxp://www.thecryptotea.com/index.php/2018/07/03/coinbase-launches-custodial-service-already-has-10-institutional-customers/
hxxps://www.coinbase.com/mission
[169] hxxps://bitpay.com/about
[170] hxxps://bitpay.com/pricing
[171] hxxps://bitpay.com/cross-border
[172] hxxps://bitpay.com/card/
[173] hxxps://bitpay.com/about
[174] hxxps://azure.microsoft.com/en-us/blog/azure-blockchain-as-a-service-update-3
hxxps://www.newegg.com/Info/NewsroomDetail.aspx?ID=1271
hxxps://www.coindesk.com/tiger-direct-accept-bitcoin/
[175] hxxps://bitcore.io/
hxxps://insight.is/
[176] hxxps://ripple.com/company/
[177] hxxps://ripple.com/solutions/process-payments/
[178] hxxps://ripple.com/solutions/source-liquidity/
[179] hxxps://ripple.com/solutions/send-payments/

Ripple claims to offer several benefits for partnering with banks: new revenue through global reach, lower transaction costs with fewer liquidity requirements, better interbank standards, and an single integration point for using the service.[180]

XRP is the token behind Ripple's services. Individuals are able to purchase and trade XRP much like a cryptocurrency, however there are several key differences. XRP cannot be mined, and is instead released at the will of the Ripple Company for reasons of price stability and security.[181] It is debatable whether Ripple is technically not a decentralized cryptocurrency due to its reliance on a central authority for transactions and monetary supply. Ripple uses a permissioned blockchain-like transaction ledger called the Ripple Protocol, which is a distributed network of trusted node validators such as the Massachusetts Institute of Technology and various ISPs.[182] Instead of miners, these validators determine transactions as valid or invalid which increases speed and energy efficiency compared to mining-based systems.[183]

### *2.5.4 Tether Ltd.*

Tether is a Hong-Kong headquartered company founded in July 2014 that has undergone a change in ownership. The service purports to provide a 1:1 reserve of USD to its USDT tokens.[184] USDT tokens are cryptocurrency representations of actual USD. This enables traders to alternatively store, trade, and transact USD without restrictions or bank accounts.[185] Tether is the only company in the space that provides such a service.

Tether is controversial for several reasons. The company has never been properly audited to verify a full reserve of deposits, which it claims amount to $2.5B.[186] Although not a proper accounting audit, a law firm did look into Tether's bank accounts in June 2018 and stated it was "confident" that the reserve is maintained.[187] The Tether CEO also runs Bitfinex, a popular Hong-Kong based exchange.[188] The two companies also share many of the same shareholders, but further involvement between the two is unknown. The U.S. Commodity Futures Trading Commission has sent multiple subpoenas to Tether around late 2017 seeking further information.[189]

### *2.5.5 Ethereum Foundation and the Enterprise Ethereum Alliance*

The Ethereum Foundation is a Swiss nonprofit organization and the main source of development and marketing for the Ethereum platform. The organization is comprised of volunteer developers from around the world.[190] The main source of funding is 12M ETH that was pre-mined when the project started.

The Enterprise Ethereum Alliance (EEA) is a group of blockchain startups, research groups, and major companies that promote and use Ethereum's technology. Notable organizations in this group are Microsoft, Cornell University, Toyota Research Institute, Samsung, Intel, J.P. Morgan, Deloitte, National

[180] hxxps://ripple.com/use-cases/
[181] hxxps://ripple.com/xrp/
[182] hxxps://www.coindesk.com/ripples-distributed-ledger-network-passes-50-validator-milestone/
[183] hxxps://en.wikipedia.org/wiki/Ripple_%28payment_protocol%29
[184] hxxps://tether.to/
[185] hxxps://coinmarketcap.com/currencies/tether/
[186] Ibid.
[187] hxxps://tether.to/wp-content/uploads/2018/06/FSS1JUN18-Account-Snapshot-Statement-final-15JUN18.pdf
[188] hxxps://www.bloomberg.com/news/articles/2018-01-30/crypto-exchange-bitfinex-tether-said-to-get-subpoenaed-by-cftc
[189] hxxps://www.bloomberg.com/news/articles/2018-01-30/crypto-exchange-bitfinex-tether-said-to-get-subpoenaed-by-cftc
[190] hxxps://entethalliance.org/

Bank of Canada, MasterCard, and Cisco Systems.[191] There are 150 member organizations as of July 2017.[192] The goal of the EEA is to create global standards to accelerate the adoption of enterprise use cases of the Ethereum platform.[193]

### *2.5.6 Bitcoin Investment Trust (GBTC)*

The Bitcoin Investment Trust is a global security with the objective of providing mainstream investors a way to speculate on Bitcoin using traditional exchanges and financial means. GBTC price closely follows Bitcoin price because the security value is solely derived from Bitcoin, being the asset that the trust holds. The trust was started in Q3 2013, and has 192 M outstanding shares.[194] The total valuation of assets under trust management is $1.13 B.[195] GBTC is traded on via OTC markets.

### *2.5.7 SWIFT gpi*

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a major traditional bank settlement system for global payments. In 2017 SWIFT introduced a new payment system in response to blockchain technology known as SWIFT global payments innovation (gpi.)[196] Using a new message standard within the SWIFT protocol, the gpi system enables same-day payments if the amount is received before the beneficiary bank's cut off time in their time zone.[197] SWIFT states that gpi will introduce a transparent fee structure.[198] Also provided is the ability to check the status of payments from the centralized Deutsche Bank Cash Inquiry tool. SWIFT gpi offers an alternative to blockchain-based interbank transfers while offering improved speed and ease of use within an existing, time-tested system.[199]

### *2.5.8 Cryptocurrency Debit Cards*

Cryptocurrency debit card services allow users to store cryptocurrency in an online wallet and spend this cryptocurrency with a normal debit card wherever the issuing payment processor's brand is accepted. The Shift Card and the BitPay Card are both powered by partnerships between Coinbase and BitPay respectively, with a credit card company.[200] Merchants then receive USD that was either instantly converted from cryptocurrency at the time of transaction, or when the user deposited the cryptocurrency into their wallet.[201]

## 2.6 Other Applications for Blockchain-derived Technologies

The decentralized ledger technology used for most cryptocurrencies has a variety of other potential applications, with or without a currency attached to it. Blockchains offer a new method of tracking the

[191] hxxps://entethalliance.org/members-2/
[192] hxxps://en.wikipedia.org/wiki/Ethereum#Enterprise_Ethereum_Alliance_(EEA)
[193] hxxps://entethalliance.org/
[194] hxxps://grayscale.co/bitcoin-investment-trust/
[195] Ibid.
[196] hxxps://www.swift.com/our-solutions/global-financial-messaging/payments-cash-management/swift-gpi
hxxps://www.euromoney.com/article/b161v3lt7v5b40/swift-gpi-the-revolution-in-cross-border-payments-is-here
[197] hxxp://cib.db.com/docs_new/Deutsche_Bank_SWIFT_gpi_White_Paper_December2017.pdf
[198] Ibid.
[199] hxxps://www.gtreview.com/news/fintech/ripple-dismisses-marginal-improvement-of-swift-gpi
[200] hxxps://www.shiftpayments.com/card
hxxps://bitpay.com/card/
[201] Ibid.

ownership and veracity of digital information.[202] This can provide solutions that avoid issues with some non-blockchain systems by adding further ways to control and verify the integrity of data.

### *2.6.1 Payments Network and Store of Value (Permissionless Blockchains)*

The most common use of cryptocurrency is as a payments network. This offers potential improvements over existing systems. Transactions can confirm quickly and settle faster than traditional methods, anywhere from seconds to minutes depending on the currency.[203,204] Settlement is designed to be fast and trustless, meaning that no entity can break the validity or security of a transaction once executed. Payments are peer-to-peer which removes intermediaries such as  clearing houses or central authorities. Decentralized cryptocurrency networks offer no authority to any entity, not even developers. The result is an immutable transaction ledger where no actor can reverse settled transactions, freeze accounts, or add/remove from balances arbitrarily. Any entity can create any number of accounts without permission or negatively impacting the network. This offers potential cost saving advantages and ease of use, but also means that there are fewer or no mechanisms to prevent or recover fraudulently or mistakenly executed transactions, stabilize prices, or comply with regulations.

Cryptocurrencies are extremely divisible for micropayments, which can increase utility for very small or precise transactions. Each Bitcoin is divisible to 100M pieces, while some newer cryptocurrencies, such as Ethereum, are divisible up to 10^18 pieces.[205] This granularity combined with zero or low fees can enable new uses for digital transfers. Fees in most cryptocurrencies are between zero and $2.00 per transaction, irrespective of the amount transacted.[206,207] Each cryptocurrency has a different fee structure and some are feeless by design, while others have zero fees due to low use.[208]

### *2.6.2 Identification*

One application of blockchain technology is the ability to cryptographically secure identities. A digitized national proof of identity is possible, reducing storage of an identity to a smartphone app or NFC chip. A digital identity can be cryptographically verified instantly on an always-online ledger, greatly reducing the issue of fake identification documents. On a smaller scale, cryptographic identity can also be used for building access cards, securing credit cards, or security clearances. One project working on blockchain cryptographic identity is Civic, which is a project attempting to put digital identities on a blockchain for purposes of authentication.[209]

### *2.6.3 Smart Contracts*

Smart contract platforms have been developed in tandem with cryptocurrency, starting from the basic scripting language included in early versions of Bitcoin. Smart contracts are scripts that execute or transact upon certain conditions being met. These contracts are self-executing, meaning that the blockchain itself executes the script exactly according to the code that’s written. Much like transactions, smart contract execution is trustless, incorruptible, and guaranteed. Ethereum is the most popular smart contracts platform and boasts of a Turing-complete language for writing scripts. Turing-complete means

[202] hxxps://www.ibm.com/blogs/blockchain/2018/03/blockchain-explained-why-its-not-just-about-bitcoin/
[203] hxxps://nano.org/en
[204] hxxps://bitinfocharts.com/comparison/bitcoin-confirmationtime.html
[205] hxxps://ethereum.stackexchange.com/questions/363/why-is-ether-divisible-to-18-decimal-places
[206] hxxps://nano.org/en
[207] hxxps://bitinfocharts.com/comparison/bitcoin-transactionfees.html
[208] hxxps://bitinfocharts.com/comparison/dogecoin-transactionfees.html
[209] hxxps://www.civic.com/

that any computational problem can be theoretically solved with Ethereum's scripting language.[210] Many innovations involving blockchain are actually applications using smart contracts.

### *2.6.4 Digital Assets*

Digital assets can be token representations of real-world objects. One application of blockchain technology is associating specific tokens to physical products in a supply chain so that they may be tracked and managed.[211] The benefits are trustless communication of tokens between companies, a stored complete history of each unit, and the ability to verify products are genuine. Internet-connected sensors or IoT devices are used to track and monitor for quality throughout a supply chain. Representative tokens could potentially be used in smart contracts for more accurate and efficient contract negotiation by automating compliance and obligations. A decentralized marketplace of suppliers that use digital assets can also be formed which drives greater efficiency in buyer/seller matching. Tokens can also be given custom attributes such as shelf life, storage temperature, and routes to assist with maintaining supply chain efficiency. The main criticism of supply chain blockchain management is data accuracy, known as the "garbage-in-garbage-out" conundrum.[212] Currently, Walmart, Kroger, and Nestlé use blockchain technology to track food items from origin to customer with success.[213]

Another use for digital assets is representing financial securities. Blockchain tokens can be used to represent ownership of a share, bond, or commodity. This could potentially reduce costs, increase security, and give investors the ability to store their assets themselves and operate on more exchanges. One prominent project in this space is tZero, which is attempting to connect decentralized ledger technology with existing market processes.[214,215]

### *2.6.5 Decentralized Autonomous Organizations*

*Decentralized autonomous organizations* (DAOs) are an experimental new form of organization hierarchy. Most DAOs to date use a system of proposals to accomplish tasks, and the purpose of the tasks is different depending on the goals and shareholders of the organization.[216] Shareholders hold a specific token that gives them voting power proportional to the amount of other shareholders' stake.[217] Individuals can create proposals for specific actions or request funds from shareholders and are voted on by the shareholders.[218] Upon the completion of a proposal, the individual is paid as per the terms of the proposal. The SEC has looked into one project in the past and has concluded that DAO (as in, "The DAO") shares are unregistered securities for regulatory and legal purposes.[219]

DAOs are a radical and controversial concept, as it removes accountability from shareholders by enabling anonymous widespread control of organizations. This lack of definite ownership combined with potentially significant assets or funds means that in the future, DAOs could present legal and regulatory issues.

[210] hxxps://ethereum.stackexchange.com/questions/2464/what-does-it-mean-that-ethereum-is-turing-complete#2465
[211] hxxps://www.ibm.com/blogs/blockchain/2018/04/digital-transformation-next-gen-procurement-and-supply-chain/
[212] hxxp://supplychainmit.com/2017/10/19/blockchains-garbage-in-garbage-out-challenge/
[213] hxxps://www.wsj.com/podcasts/can-blockchain-fix-our-food-chain/F8CCD98A-5630-40EC-8460-BD4A619AE51F.html
[214] hxxps://www.tzero.com/
[215] hxxps://www.investopedia.com/tech/what-overstocks-cryptocurrency-tzero/
[216] hxxps://eprint.iacr.org/2018/435.pdf
[217] Ibid.
[218] hxxps://eprint.iacr.org/2018/435.pdf
[219] hxxps://corpgov.law.harvard.edu/2018/02/08/cryptocurrency-2018/

There are several implementations of DAOs with varying degrees of success. The most notable DAO was called 'The DAO'. However, The DAO dissolved after an error in its smart contract code allowed a threat actor to steal $50M worth of ETH from the entity.[220] This loss resulted in Ethereum forking into a new currency to preserve lost funds.[221] Dash and Decred are two examples of successful DAOs managing cryptocurrency platforms.[222] Token holders in these cryptocurrencies vote on funding proposals that are meant to increase adoption or fund development.

### *2.6.6 Decentralized Communication/Social Networking*

Almost any type of data can be stored in a decentralized ledger. Instead of the tokens representing ownership or value, the idea to give tokens themselves value was one of the first blockchain ideas. Several blockchain projects are focused on providing a social networking service or instant messaging client that allows users to connect and share information in a trustless manner. [223] Without a central server, these communication platforms are very difficult to take offline or regulate. The IOTA network has the ability to send arbitrary messages among addresses.[224]

Blockchain technology could also potentially be applied to the telecom industry and internet infrastructure. DNS, SSL certificate authorities, and other security chokepoints could utilize such a system to secure and decentralize their services. The Namecoin uses blockchain to provide a decentralized DNS-like service.[225] Substratum is a project focused on decentralized web hosting.[226] It is predicted that the blockchain market within the telecom sector will increase by over 2,000%, to $1 billion, by 2023[227].

### *2.6.7 Trade Finance*

Trade finance is a trillion dollar industry that involves a bank loaning money to a large trading seller for the purposes of receiving payment quickly.[228] When a bank receives a purchase agreement from a buyer and notification of compliance from the seller, a letter of credit is given to the seller.[229] The letter of credit is a guarantee that the issuing bank will pay the seller once the product is received.[230] Blockchain technology could be applied to this process by replacing the letter of credit with a "debt" token issued by the bank, reducing processing time. This can also allow the debt token to be traded among those using the same platform

In May 2018, HSBC made the first trade finance transaction with blockchain technology. A shipment of soybeans between Argentina and Malaysia was made using a blockchain system to handle the trade financing.[231] HSBC estimated this could result in a 31% reduction in costs and a 44% reduction in time required to export goods if applied to all of the bank's Asia-Pacific trade documents.[232]

## 2.7 Criticism and Adoption Difficulties

[220] hxxps://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/
[221] Ibid.
[222] hxxps://decred.org/
[223] hxxps://www.investopedia.com/news/steemit-disruptive-blockchainbased-media-community/
[224] hxxps://blog.iota.org/introducing-masked-authenticated-messaging-e55c1822d50e
[225] hxxps://www.namecoin.org/
[226] hxxps://substratum.net/
[227] hxxps://www.researchandmarkets.com/research/383qcp/blockchain_in?w=4
[228] hxxps://www.investopedia.com/terms/t/tradefinance.asp
[229] Ibid.
[230] Ibid.
[231] Ibid.
[232] hxxps://www.businessinsider.com/hsbc-ing-blockchain-trade-finance-cargill-soybeans-2018-5

There potential downsides to blockchain and cryptocurrency technology. Until these concerns are alleviated, adoption will be slow for individuals, institutions, and governments. These criticisms can be broken down into a few broad categories: needed improvements to the technology, price volatility, and lack of regulation.

### *2.7.1 Energy Waste*

The Bitcoin proof-of-work model was an effective solution to a long-held computer science problem. It enabled the ability to store unique digital values and declare ownership. However, the electrical cost of proof-of-work is significant. Bitcoin mining is estimated to use about the same amount of electricity as Denmark by 2020.[233] Proof-of-stake is one solution to this problem because it doesn't rely on processing power. Some existing cryptocurrencies are attempting to adjust and improve their use of proof-of-stake. For example, Ethereum plans on moving to a new, modified, proof-of-stake model that is better decentralized in the future.[234]

### *2.7.2 Limited Throughput*

Blockchains have a very low data storage capacity. Since a copy of the entire blockchain is meant to be kept forever by every node, or by at least a subsection of the nodes, the cost per byte of data is very high. Storing data larger than simple messages or transactions is infeasible until major innovations in computer storage and internet bandwidth occur. Blockchains require consensus, and achieving consensus among nodes can be slow in some (especially older) cryptocurrencies. The network must agree on a block before it can accept it and begin working on the next one. Transactions are fast to settle, but the total throughput of a blockchain is very small compared to centralized servers, e.g. Bitcoin can only process 100 KB per minute.[235] There are other cryptocurrencies in development that use a block lattice or a graph to store transactions, which gives potentially unrestricted throughput and increased speed.[236] If successful, these new implementation could alleviate current limitations.

### *2.7.3 Volatile Prices*

Price volatility can be a significant barrier to entry for prospective cryptocurrency users or investors. Volatility is widespread in the cryptocurrency market for many reasons, making 10-20% daily swings a normal occurrence.[237] The market is new, the assets have questionable value, market hype/panic is common, there are no price manipulation protections, and the assets can trade at any time of day. Market confusion can also play into price volatility. Currently there are over 1500 cryptocurrencies and new ones can be created at any time, potentially diluting prices. Individuals often do not want to store cryptocurrency for fear of their buying power changing daily, and companies would need to see sufficient demand from consumers in order to risk acquiring and storing such a volatile asset. Fixing this issue is a controversial subject among current cryptocurrency users because the solution usually involves increased regulation, something that many cryptocurrency traders do not want.[238] Since transactions in public blockchains are permissionless, a regulated exchange could be skirted using over-the-counter trading and underground exchanges. There is also debate over whether cryptocurrency markets will stabilize over time or remain volatile.

### *2.7.4 Security*

[233] hxxps://motherboard.vice.com/en_us/article/aek3za/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020
[234] hxxps://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/
[235] 1 MB divided by 10 minutes
[236] hxxps://nano.org/en/whitepaper
[237] hxxps://www.forbes.com/sites/jayadkisson/2018/01/29/bitcoin-cryptocurrency-and-the-government-regulation-paradox
[238] hxxps://www.investopedia.com/news/should-cryptocurrency-exchanges-selfregulate-themselves/

Cryptocurrencies' use of irreversible transactions presents a significant security issue for many users. Transactions may be verified and secured by multiple parties, but a wallet's private key can be stolen and fraudulent transactions authorized that can not be stopped, frozen, or reversed. Proper private key management is the single most important rule to dealing with permissionless cryptocurrencies. Organizations considering using or investing in cryptocurrencies should bear this in mind and take appropriate security precautions.

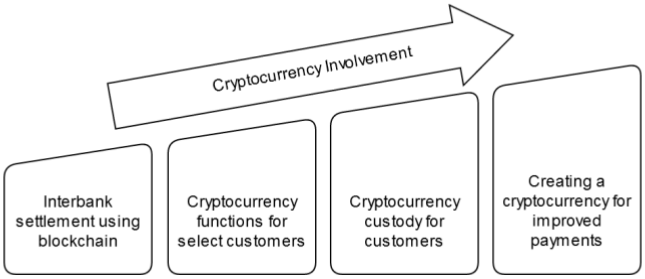
Indirect risks are also present that do not reflect issues in the core blockchain technology or cryptography. Cryptocurrency wallet apps are software like any other and can contain vulnerabilities that can be exploited. Vulnerabilities in several wallet apps were identified, with some leading to funds being stolen from users' wallets.[239] Online exchange services can also experience security issues with their systems that allow threat actors access to the exchange's wallet or user wallet accounts.[240]

Cryptocurrencies may also be vulnerable to an emerging technology. Quantum computing is a new type of technology that uses quantum physics to perform advanced calculations. Most cryptocurrencies use cryptographic functions that are not quantum-proof. Although the technology is very young and extremely limited these new types of computers are theorized to be able to break the strongest current encryption algorithms. A capable quantum computer could theoretically crack the security protecting digital communications, most blockchains, and encrypted data storage.[241] Blockchains affected will need to fork to use either an existing quantum-proof algorithm or one that has not been invented yet. The IOTA cryptocurrency is an exception; it uses Winternitz signatures, which are designed to be quantum-proof.[242]

## 2.8 Working with Cryptocurrency

### *2.8.1 Financial Institutions*

The main question a financial institution will ask with regards to cryptocurrency is: *would this technology be useful to us, and if so, how can we implement it?* Cryptocurrency offers a new form of settling payments that can operate on several layers: consumer, business, or bank. The first thing to consider is the extent to which a financial institution wishes to implement a blockchain solution.


Cryptocurrency Involvement
Interbank settlement using blockchain
Cryptocurrency functions for select customers
Cryptocurrency custody for customers
Creating a cryptocurrency for improved payments

At the most basic level, cryptocurrency offers a potential alternative for interbank settlement and wire transfers. Instead of passing messages between banks for payment orders, funds themselves can be

[239] hxxps://www.zdnet.com/article/security-flaw-leaves-android-bitcoin-wallets-vulnerable-to-theft/
hxxps://thenextweb.com/hardfork/2018/03/20/ledger-nano-s-hack-cryptocurrency/
[240] hxxps://blockgeeks.com/guides/cryptocurrency-hacks/
hxxps://www.japantimes.co.jp/news/2018/03/13/business/corporate-business/hacked-japanese-cryptocurrency-exchange-coincheck-refunds-customers/
hxxps://www.theguardian.com/technology/2018/jun/11/bitcoin-price-cryptocurrency-hacked-south-korea-coincheck
[241] hxxps://www.wired.co.uk/article/quantum-computers-quantum-security-encryption
[242] hxxps://docs.iota.org/introduction

sent directly between correspondent parties without prior notice or requesting a federal reserve bank to send a payment. Financial institutions using a cryptocurrency for interbank settlement are able to do so in a time-agnostic manner, instead of waiting for a daily settlement window. Time-agnosticism is achieved by allowing banks to transact directly with other banks autonomously using a cryptocurrency, as opposed to holding an account with a federal reserve bank that acts as a transaction agent.

There are several possible implementations of blockchain-enabled interbank systems. The Ripple Company is one such system and is currently used by over 100 clients.[243] Advantages to joining an existing system include easier interoperability with other uses of the same system. If an in-house development solution is required, there are several open source solutions. These include Corda, Hyperledger, Microsoft Azure Blockchain Workbench, and Chain.[244,245] These three are tools for building blockchains, not ready-to-use networks for integration like Ripple.

Financial institutions may wish to provide additional cryptocurrency functionality for select customers. Such customers may include cryptocurrency exchanges, businesses that hold cryptocurrency for operations, companies that transact partially with cryptocurrency, or customers that wish to transact in ways that aren’t possible within the current system. Companies of this type are few in number but the model may be applicable in blockchain startup hubs like Southern California, New York, Boston, and Chicago where cryptocurrency companies are growing.[246]

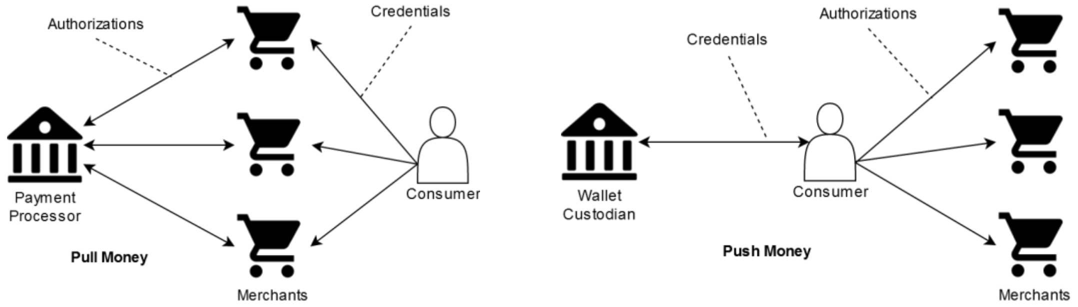
A step further into adopting cryptocurrency may look like a financial institution that holds custody over customer cryptocurrency funds, as though it were a traditional bank account. The benefit for the customer would be a secure and user-friendly way to use cryptocurrency, potentially increasing general adoption of the technology. If permissionless cryptocurrencies are held, secure private key management would be the highest priority for a security team. This may satisfy risk requirements for companies that wish to hold permissionless customer funds. Fund custodians in the past have gotten insurance plans to guarantee user deposits.[247,248,249] Generally, the insurance falls under the category of a crime/theft plan, which typically does not cover digital currencies by default.[250]

Digital peer-to-peer payments services have grown immensely for informal payments; PayPal and Venmo, just to name a couple. Customers desire the ability to easily move money between friends, between family, and for small informal dealings. Venmo, a service for consumer-to-consumer transactions, has seen an increase in transaction volume each quarter since the beginning of 2017.[251]

There are many digital payments services that have appeared in recent times: Google Pay, Apple Pay, Samsung Pay, and many more.[252] These NFC-enabled apps are digital wrappers for credit cards.[253,254,255,256] Replacing credit cards with a cryptocurrency could greatly reduce fraud by a simple

[243] hxxps://www.cnbc.com/2017/10/10/ripple-has-over-100-clients-as-mainstream-finance-warms-to-blockchain.html
[244] hxxps://azure.microsoft.com/en-us/solutions/blockchain/
[245] hxxps://chain.com/sequence/
[246] hxxps://www.forbes.com/sites/jeffkauflin/2018/02/26/the-top-15-cities-for-blockchain-technology-jobs-in-america
[247] hxxps://support.coinbase.com/customer/portal/articles/1662379-how-is-coinbase-insured-
[248] hxxps://www.theguardian.com/technology/2014/sep/29/bitcoin-circle-cryptocurrency-jeremy-allaire
[249] hxxps://blog.xapo.com/xapo-adds-a-and-a-rated-insurers-to-vault-insurance/
[250] hxxps://www.coindesk.com/great-american-insurance-bitcoin-coverage-businesses/
[251] hxxps://www.statista.com/statistics/763617/venmo-total-payment-volume/
[252] hxxps://money.usnews.com/money/blogs/my-money/articles/2018-03-16/what-you-need-to-know-about-mobile-wallets
[253] Ibid.
[254] hxxps://www.pocket-lint.com/apps/news/google/135017-what-is-android-pay-how-does-it-work-and-which-banks-support-it

change in the mechanics of how end users transact. Credit and debit cards are 'pull money', and cryptocurrency is 'push money'. When transacting with credit or debit cards, credentials (card number, customer name, etc.) are given to a merchant so that they can pull money out of the customer's account. The issue with this is that the credentials can be stolen either by a brick-and-mortar merchant's employee, a data breach in an online store, or by modified card readers. The result is illegitimate transactions and imperfect anti-fraud monitoring methods. In 2016, there were over 400k card identity theft cases, 1.3M fraud-related complaints, and conservatively $750M in fraudulent credit card transactions.[257] Push money, like cryptocurrency, is different. The credentials never leave the customer and can be stored via a card, smartphone app, or chip. Instead of giving a merchant access to a customer's account, the customer can approve transactions on a per-payment basis. Merchants never receive a copy of the customer's credentials because authorization information is stored in only one secure location: the user's bank account. Push-money technologies can suffer from the same attacks as credential based payments, however, such as phishing and malware. The figure below illustrates the differences between pull and push money systems:



In this scenario, the current roles filled by a financial institution may change from:

- Account manager
- Delegate for transferring funds
- Payment Processor

…to the following roles after a widely-adopted cryptocurrency is used for payments:

- Wallet custodian
- Insurer/security for funds
- Exchanger
- Currency maintainer

This table is a comparison of different ways a financial institution can work with cryptocurrency/blockchain:

| | Traditional System | Private Blockchain | Public Cryptocurrency Custody | USD-backed Cryptocurrency |
|---|---|---|---|---|
| **Implementation** | Current system using traditional payment technology. | Using Ripple protocol for interbank settlement. | Holding users' cryptocurrency funds. Not just for interbank settlement. | Bank or cooperative creates a USD cryptocurrency. |
| **Potential Bank Theft** | No | No | Yes | No |
| **Distributed Server Infrastructure** | Yes | No | No | Yes |
| **Bottom Line** | No Change | Less Fees | New Customers | Less Fees, New |

[255] hxxps://www.bustle.com/articles/44654-how-does-apple-pay-work-exactly-all-your-questions-answered
[256] hxxps://www.cnet.com/how-to/samsung-pay-what-you-need-to-know-faq/
[257] hxxps://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php

| | | | | Customers |
|---|---|---|---|---|
| **Domestic Settlement** | 2-3 days | Instant | Usually within 30 minutes | Instant |
| **International Settlement** | 5-15 days | | | |
| **Potential Regulatory Issues** | No | No | Yes | Yes |
| **Public Ledger Access** | No | No | Yes | Yes |
| **Non-USD Tokens** | No | No | Yes | No |
| **Modern Protocol** | No | Yes | Yes | Yes |
| **Time Tested** | Yes | No | No | No |
| **Unfamiliar User Experience** | No | No | Yes | Yes |
| **Adopted by Other Financial Institutions** | Yes | Many | Potentially | No |
| **Undo Illicit Transactions (Consumer Level)** | Yes | Yes | No | Yes |

### *2.8.2 Criminal Investigation*

All cryptocurrency users can benefit from increased security, anonymity, and instant settlement. However, this also extends to criminal users. Cryptocurrency, especially Bitcoin and Monero, are commonly used to make illicit purchases, conduct extortion, launder money, and engage in other types of crime.[258] This does not make cryptocurrencies themselves inherently criminal, but it does create new challenges for law enforcement. However, some aspects of cryptocurrencies can also be useful in identifying and prosecuting criminals.

Decentralized ledger technology can aid in investigations. A majority of illicit transactions are committed with transparent blockchains, providing hard proof of the movement of money. If law enforcement can connect an identity with an address, they have immutable proof of the entire wallet's history. Blockchain transaction history has been used as evidence in a number of criminal cases or as the basis for subpoenas and other legal actions.[259] A class of software tools is used for **chain analysis**, which quantifies the association between addresses and visualizes transactions. Analyzing transaction cash-out points can lead to a subpoena of a financial company.

Anonymous currencies that deprecate popular chain analysis programs are quickly growing in popularity among criminals on the dark web. New tools will need to be developed to analyze these blockchains. Anonymity weaknesses can be found in private cryptocurrencies (see "Profile: Monero"). A new focus should be obtaining an actor's private key or private view key, which will yield much of the same information offered publicly by a transparent blockchain.

### *2.8.3 End Users*

[258] hxxps://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group
hxxps://techcrunch.com/2018/04/13/exit-scammers-run-off-with-660-million-in-ico-earnings/
hxxps://www.bleepingcomputer.com/news/security/beware-of-extortion-scams-stating-they-have-video-of-you-on-adult-sites/
hxxps://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged
hxxps://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/

[259] hxxps://www.technologyreview.com/s/608763/criminals-thought-bitcoin-was-the-perfect-hiding-place-they-thought-wrong/
hxxps://www.coindesk.com/catch-bitcoin-ransomer-inside-fbis-cyber-investigation-process/

Below is a table of the different forms of money and how well they fit the essential qualities of an effective currency:

| | Physical Cash | Current Digital Money | Permissionless Cryptocurrencies | USD-backed Cryptocurrency |
|---|---|---|---|---|
| **Acceptability** | Accepted everywhere by law. Instant. | Fractured. Many methods of payment and different transaction processors. Seemingly instant, days to settle. | Low, difficult to increase without a central pushing force. Near-instant settlement. | Until network effect, low. Institutions capable of pushing adoption. Instant settlement. |
| **Portability** | Peer-to-peer transactions included. | Physical cards predominantly used. Peer-to-peer transactions possible. | Available using app or traditional card/chip. Organic peer-to-peer transactions. | |
| **Durability/Security** | Fairly durable. Security varies. | Timeless durability. High incidence of card fraud. | Timeless durability. Cryptographic security. | |
| **Divisibility** | Divisible up to 100 pieces. | Transaction fees and overhead make small digital payments (< $2.00) infeasible. | Virtually infinitely small transactions. | |
| **Fungibility** | For the most part, coins and bills are treated the same. | Money stored in different unequally preferred transaction vehicles or middlemen. | All tokens are identical. The vehicle or method of storage is irrelevant. | |
| **Recognizable** | USD is highly recognizable. | | About half of Americans | USD is highly recognizable. |

End users of cryptocurrency should follow several security principles that will keep their funds safe:

1. Follow proper private key management practices.
   a. If using a custodial service like Coinbase or an exchange, use non-SMS two-factor authentication tool and a strong password. Make sure the email connected to your account is up to date. Consider whitelisting specific IP addresses for large account holdings. If possible, it's better to use a control-your-own-keys wallet since custodial accounts are notorious for being hacked, spoofed in phishing campaigns, or at the mercy of browser code injection. Well-known services like Coinbase are trustworthy, but risk still remains.
   b. If using a hot control-your-own-keys wallet like mobile apps or a full node on a computer, make sure your wallet is encrypted when not in use. Use a strong password.
   c. In all cases, including cold wallets and multisignature address use, make sure your seed phrase and encryption keys are backed up offline on a piece of paper or engraved in metal. Store in a safe or safety deposit box to protect against physical theft.
2. Choose safe, well-vetted, and easy-to-use wallet software.
3. Consider multisignature addresses for business holdings.
4. When sending funds, double check the receiving address to verify accuracy.
5. For large holdings, generate keys on offline operating systems that will never be connected to the internet. This is free to do using open source Linux distributions booted via live USB stick, such as Ubuntu. For extremely large holdings, a physical computer that is always air gapped may be necessary for generating private keys and signing transactions. Air gapped computers require the manual movement of funds via USB drive, but the number of attack vectors will be reduced to just physical access.

# 3.0 Appendices

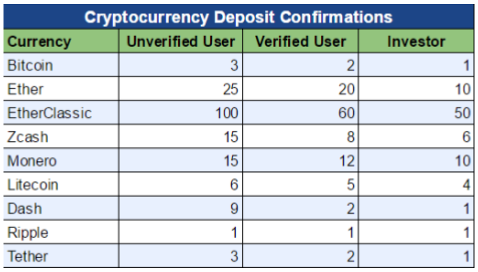
## 3.1 Glossary

| | |
|---|---|
| **ASIC** | Type of hardware that can only process a specific algorithm. Very powerful for mining certain cryptocurrencies. |
| **Account** | Single container for cryptocurrency tokens. |
| **Address** | Public string of alphanumeric characters that identifies an account. |
| **Block** | Bundle of transactions. |
| **Blockchain** | Collaboratively maintained ledger of transactions. |
| **Blockchain Explorer** | Website used to view blockchain data. This includes blocks, transactions, addresses, and mining information. |
| **Block Height** | Number of mined blocks in a blockchain. |
| **Block Reward** | Revenue given to the miner. Includes transaction fees and coinbase. |
| **Block Time** | Interval between blocks in a cryptocurrency. |
| **Burnt** | Coins in an account of which the private key is unknown. |
| **Chain Analysis** | Using a blockchain to trace transactions for investigation. |
| **Coin** | Single unit of a cryptocurrency. Also used interchangeably with “cryptocurrency”. |
| **Coinbase** | (Technical) Generation of minted coins that are awarded to the miner of a new block. |
| **Cold Wallet** | Wallet that is analog or disconnected from the internet. |
| **Confirmations** | Number of blocks that have been mined since the block a transaction was included into. |
| **Cryptojacking** | Unauthorized use of processing power to mine cryptocurrency. |
| **DAG (Directed Acyclic Graph)** | Post-blockchain technology that offers improved throughput and speed for cryptocurrencies. |
| **Digital Asset** | *See* “Coin” |
| **Double Spend** | Sending a transaction that is considered settled by the merchant, but doesn’t end up or is removed from the blockchain later on. |
| **Dust** | Outputs that have a value smaller than the fee required to spend. |
| **Fee Market** | Competition between senders to choose a high price-per-byte fee to include with their transaction. |
| **Fiat** | Traditional government-sanctioned currency. |
| **Flippening, The** | Bitcoin losing its dominance as the main cryptocurrency to another coin. |
| **Fork** | Nodes that follow different protocol rules will diverge into two separate currencies. |
| **Hard Fork** | (Development) A change to the protocol that will cause a fork. |
| **Hardware Wallet** | Air gapped device used to sign transactions. |
| **Hierarchical Deterministic Key** | Single private key used to generate virtually infinite number of addresses. |
| **Hot Wallet** | Wallet on a device connected to the internet. |
| **ICO** | Initial coin offering. Like an IPO, but unregulated uses cryptocurrency coins as shared. |
| **Integrated Address** | Address generated from a main address and a payment ID. Can be |

| | |
|---|---|
| | undone without a private key. |
| **Ledger** | Abstraction of a blockchain. All blockchains are ledgers, but not all ledgers are blockchains. |
| **Main Chain** | Canonical chain commonly accepted by nodes. |
| **Merkle Tree** | Cryptographic method of hashing large sets of data into one root hash. |
| **Miner** | Node that is mining. |
| **Mining** | Working on mining new blocks to append to the blockchain. |
| **Mixer** | Service that collects cryptocurrency from multiple actors and sends it back out. Used to obfuscate the blockchain paper trail in non-private coins. |
| **Mnemonic** | *See* "Hierarchical Deterministic Key" |
| **Multisig** | Multisignature addresses that require multiple private keys to authorize transactions. |
| **Node** | Running and connected instance of cryptocurrency network software. Has a copy of the blockchain. Might be a miner. |
| **Orphan** | Block that was valid, but was removed from the main chain after a reorg. |
| **Permissioned Blockchain** | Blockchain that requires prior authorization to use. Participants known. |
| **Permissionless Blockchain** | Blockchain that doesn't require prior authorization to use. Participants unknown. |
| **Pool** | Group of miners mining together to stabilize profits. |
| **Pre-mine** | All or a portion of the tokens are in circulation when a cryptocurrency is publicly released. |
| **Private Blockchain** | *See* "Permissioned Blockchain" |
| **Private Key** | String used to authorize transactions. |
| **Proof-of-Stake** | Nodes putting up collateral for the chance of being granted to create a new block. |
| **Proof-of-Work** | Miners repeatedly attempt to guess a correct target value, which will grant them the ability to append a new block to the blockchain. |
| **Pruning** | Removing old transactions on a blockchain to save space. |
| **Public Blockchain** | *See* "Permissionless Blockchain" |
| **Reorg** | New chain of two or more blocks that orphans previous blocks due to having a larger block height. |
| **Ring Signature** | Used in Monero to make transactions anonymous. |
| **Ring Size** | Number of signers to bundle into a transaction. Higher means more anonymous, to an extent. |
| **Seed** | *See* "Hierarchical Deterministic Key" |
| **Smart Contract** | Self-executing, immutable contract that lives on a blockchain. |
| **Soft Fork** | Change to the protocol that will not cause a fork. |
| **Staker** | Node that has put up collateral for proof-of-stake blockchains. |
| **Taint** | Metric that shows how related two addresses are based on the movement of funds. |
| **Technical Debt** | Added development confusion when including code workarounds to be compatible with an older version of a protocol. |

| | |
|---|---|
| **Token** | *See* "Coin" |
| **Transaction** | Movement of funds between two or more accounts. |
| **Transaction Fee** | Fee offered by the sender to any miner that accepts the transaction into a block. |
| **TX** | *See* "Transaction" |
| **Tumbler** | *See* "Mixer" |
| **Wallet** | Collection of addresses that are usually generated using a single hierarchical deterministic key. |
| **Xpriv** | *See* "Hierarchical Deterministic Key" |
| **Zero-conf** | Zero confirmations required for a transaction to be considered settled, i.e. as soon as it is sent. |

### 3.2 Confirmation Requirement Policy for "Bitfinex" Exchange

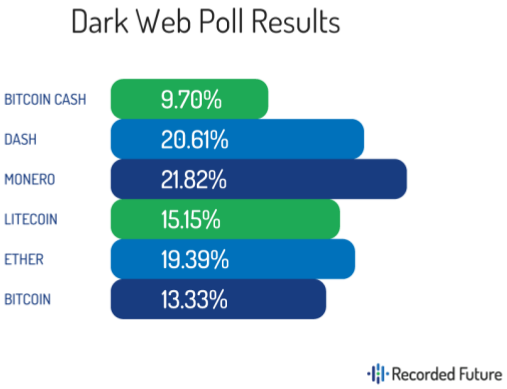


Cryptocurrency Deposit Confirmations

| Currency | Unverified User | Verified User | Investor |
|---|---|---|---|
| Bitcoin | 3 | 2 | 1 |
| Ether | 25 | 20 | 10 |
| EtherClassic | 100 | 60 | 50 |
| Zcash | 15 | 8 | 6 |
| Monero | 15 | 12 | 10 |
| Litecoin | 6 | 5 | 4 |
| Dash | 9 | 2 | 1 |
| Ripple | 1 | 1 | 1 |
| Tether | 3 | 2 | 1 |

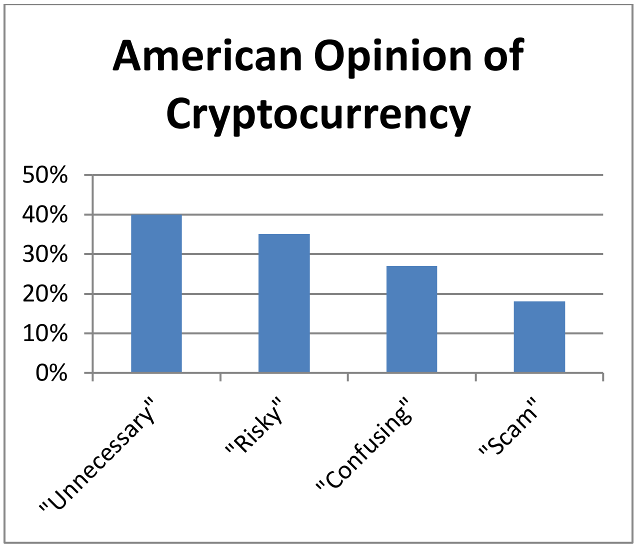
hxxps://support.bitfinex.com/hc/en-us/articles/115003291405-Where-is-my-cryptocurrency-deposit-or-withdrawal-

### 3.3 Preferred Cryptocurrency for Illicit Dark Web Purchases, Hackers Polled



hxxps://www.recordedfuture.com/dark-web-currency/

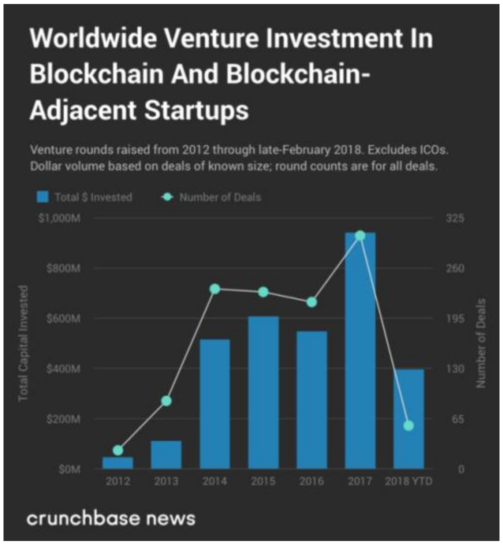
### 3.4 Stated Reasons by Americans for Not Owning Cryptocurrency



American Opinion of Cryptocurrency

hxxps://www.finder.com/why-people-arent-buying-cryptocurrency

### 3.5 Venture Investment in Blockchain Startups (as of March 2018)



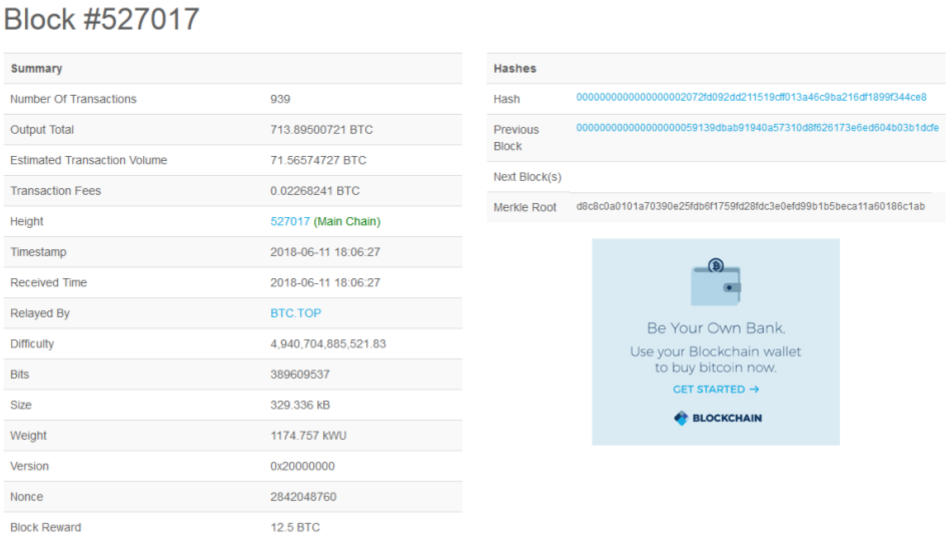
Worldwide Venture Investment In Blockchain And Blockchain-Adjacent Startups

Venture rounds raised from 2012 through late-February 2018. Excludes ICOs. Dollar volume based on deals of known size; round counts are for all deals.

crunchbase news

hxxps://techcrunch.com/2018/03/03/2018-vc-investment-into-crypto-startups-set-to-surpass-2017-tally/

### 3.6 Block Content Example



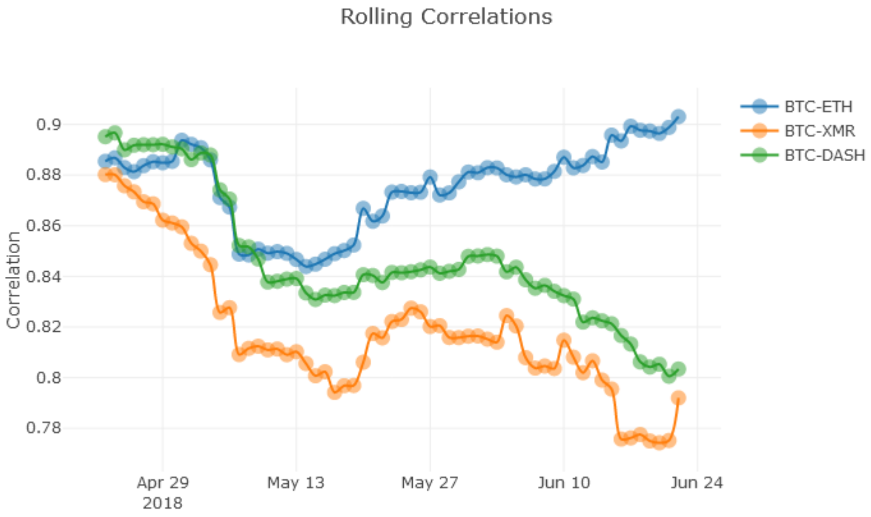
Block #527017

| Summary | |
|---|---|
| Number Of Transactions | 939 |
| Output Total | 713.89500721 BTC |
| Estimated Transaction Volume | 71.56574727 BTC |
| Transaction Fees | 0.02268241 BTC |
| Height | 527017 (Main Chain) |
| Timestamp | 2018-06-11 18:06:27 |
| Received Time | 2018-06-11 18:06:27 |
| Relayed By | BTC.TOP |
| Difficulty | 4,940,704,885,521.83 |
| Bits | 389609537 |
| Size | 329.336 kB |
| Weight | 1174.757 kWU |
| Version | 0x20000000 |
| Nonce | 2842048760 |
| Block Reward | 12.5 BTC |

| Hashes | |
|---|---|
| Hash | 0000000000000000002072fd092dd211519cff013a46c9ba216df1899f344ce8 |
| Previous Block | 00000000000000000059139dbab91940a57310d8f626173e6ed604b03b1dcfe |
| Next Block(s) | |
| Merkle Root | d8c8c0a0101a70390e25fdb6f1759fd28fdc3e0efd99b1b5beca11a60186c1ab |

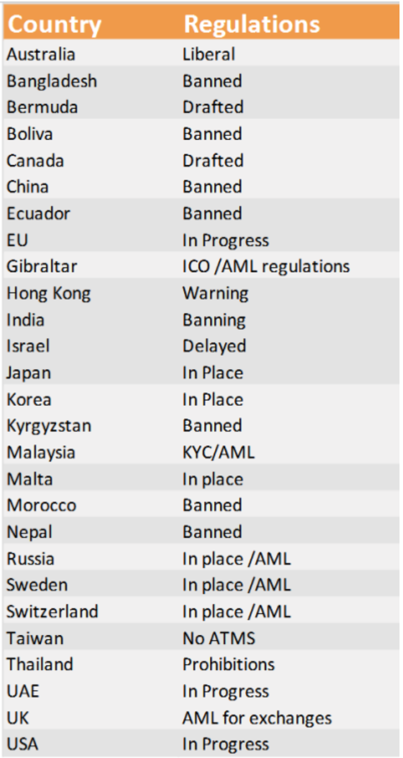
hxxps://blockchain.info

### 3.7 Monero and Dash Prices Decoupling from Bitcoin Market Trends



hxxps://www.sifrdata.com/cryptocurrency-rolling-correlations/

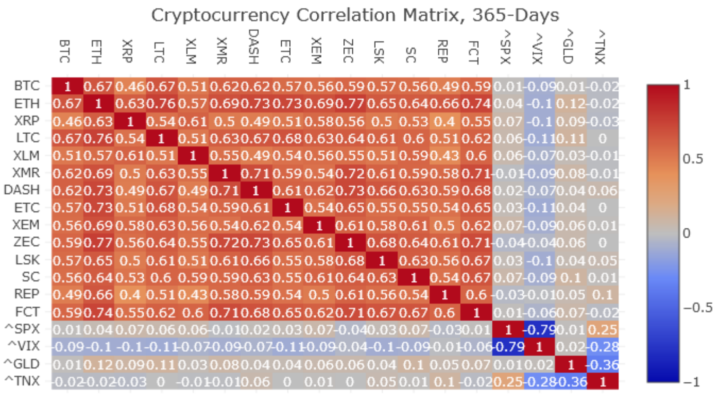
### 3.8 Cryptocurrency Legal Statuses by Country in 2018



| Country | Regulations |
|---|---|
| Australia | Liberal |
| Bangladesh | Banned |
| Bermuda | Drafted |
| Boliva | Banned |
| Canada | Drafted |
| China | Banned |
| Ecuador | Banned |
| EU | In Progress |
| Gibraltar | ICO /AML regulations |
| Hong Kong | Warning |
| India | Banning |
| Israel | Delayed |
| Japan | In Place |
| Korea | In Place |
| Kyrgyzstan | Banned |
| Malaysia | KYC/AML |
| Malta | In place |
| Morocco | Banned |
| Nepal | Banned |
| Russia | In place /AML |
| Sweden | In place /AML |
| Switzerland | In place /AML |
| Taiwan | No ATMS |
| Thailand | Prohibitions |
| UAE | In Progress |
| UK | AML for exchanges |
| USA | In Progress |

hxxps://cdn2.hubspot.net/hubfs/4345106/crypto_aml_report_2018q2.pdf

### 3.9 Cryptocurrency Market Correlations



Cryptocurrency Correlation Matrix, 365-Days

|  | BTC | ETH | XRP | LTC | XLM | XMR | DASH | ETC | XEM | ZEC | LSK | SC | REP | FCT | ^SPX | ^VIX | ^GLD | ^TNX |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| BTC | 1 | 0.67 | 0.46 | 0.67 | 0.51 | 0.62 | 0.62 | 0.57 | 0.56 | 0.59 | 0.57 | 0.56 | 0.49 | 0.59 | 0.01 | -0.09 | 0.01 | -0.02 |
| ETH | 0.67 | 1 | 0.63 | 0.76 | 0.57 | 0.69 | 0.73 | 0.73 | 0.69 | 0.77 | 0.65 | 0.64 | 0.66 | 0.74 | 0.04 | -0.1 | 0.12 | -0.02 |
| XRP | 0.46 | 0.63 | 1 | 0.54 | 0.61 | 0.5 | 0.49 | 0.51 | 0.58 | 0.56 | 0.5 | 0.53 | 0.4 | 0.55 | 0.07 | -0.1 | 0.09 | -0.03 |
| LTC | 0.67 | 0.76 | 0.54 | 1 | 0.51 | 0.63 | 0.67 | 0.68 | 0.63 | 0.64 | 0.61 | 0.6 | 0.51 | 0.62 | 0.06 | -0.11 | 0.11 | 0 |
| XLM | 0.51 | 0.57 | 0.61 | 0.51 | 1 | 0.55 | 0.49 | 0.54 | 0.56 | 0.55 | 0.51 | 0.59 | 0.43 | 0.6 | 0.06 | -0.07 | 0.03 | -0.01 |
| XMR | 0.62 | 0.69 | 0.5 | 0.63 | 0.55 | 1 | 0.71 | 0.59 | 0.54 | 0.72 | 0.61 | 0.59 | 0.58 | 0.71 | -0.01 | -0.09 | 0.08 | -0.01 |
| DASH | 0.62 | 0.73 | 0.49 | 0.67 | 0.49 | 0.71 | 1 | 0.61 | 0.62 | 0.73 | 0.66 | 0.63 | 0.59 | 0.68 | 0.02 | -0.07 | 0.04 | 0.06 |
| ETC | 0.57 | 0.73 | 0.51 | 0.68 | 0.54 | 0.59 | 0.61 | 1 | 0.54 | 0.65 | 0.55 | 0.55 | 0.54 | 0.65 | 0.03 | -0.11 | 0.04 | 0 |
| XEM | 0.56 | 0.69 | 0.58 | 0.63 | 0.56 | 0.54 | 0.62 | 0.54 | 1 | 0.61 | 0.58 | 0.61 | 0.5 | 0.62 | 0.07 | -0.09 | 0.06 | 0.01 |
| ZEC | 0.59 | 0.77 | 0.56 | 0.64 | 0.55 | 0.72 | 0.73 | 0.65 | 0.61 | 1 | 0.68 | 0.64 | 0.61 | 0.71 | -0.04 | -0.04 | 0.06 | 0 |
| LSK | 0.57 | 0.65 | 0.5 | 0.61 | 0.51 | 0.61 | 0.66 | 0.55 | 0.58 | 0.68 | 1 | 0.63 | 0.56 | 0.67 | 0.03 | -0.1 | 0.04 | 0.05 |
| SC | 0.56 | 0.64 | 0.53 | 0.6 | 0.59 | 0.59 | 0.63 | 0.55 | 0.61 | 0.64 | 0.63 | 1 | 0.54 | 0.67 | 0.07 | -0.09 | 0.1 | 0.01 |
| REP | 0.49 | 0.66 | 0.4 | 0.51 | 0.43 | 0.58 | 0.59 | 0.54 | 0.5 | 0.61 | 0.56 | 0.54 | 1 | 0.6 | -0.03 | -0.01 | 0.05 | 0.1 |
| FCT | 0.59 | 0.74 | 0.55 | 0.62 | 0.6 | 0.71 | 0.68 | 0.65 | 0.62 | 0.71 | 0.67 | 0.67 | 0.6 | 1 | 0.01 | -0.06 | 0.07 | -0.02 |
| ^SPX | 0.01 | 0.04 | 0.07 | 0.06 | 0.06 | -0.01 | 0.02 | 0.03 | 0.07 | -0.04 | 0.03 | 0.07 | -0.03 | 0.01 | 1 | -0.79 | 0.01 | 0.25 |
| ^VIX | -0.09 | -0.1 | -0.1 | -0.11 | -0.07 | -0.09 | -0.07 | -0.11 | -0.09 | -0.04 | -0.1 | -0.09 | -0.01 | -0.06 | -0.79 | 1 | 0.02 | -0.28 |
| ^GLD | 0.01 | 0.12 | 0.09 | 0.11 | 0.03 | 0.08 | 0.04 | 0.04 | 0.06 | 0.06 | 0.04 | 0.1 | 0.05 | 0.07 | 0.01 | 0.02 | 1 | -0.36 |
| ^TNX | -0.02 | -0.02 | -0.03 | 0 | -0.01 | -0.01 | 0.06 | 0 | 0.01 | 0 | 0.05 | 0.01 | 0.1 | -0.02 | 0.25 | -0.28 | -0.36 | 1 |

hxxps://www.sifrdata.com/cryptocurrency-correlation-matrix/