Fraud and Manipulation within Cryptocurrency Markets

#7915
COURSE MATERIAL
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Chapter 1: Fraud and Manipulation within Cryptocurrency Markets</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Introduction</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Beginning at the Beginning: What Blockchains Are</td>
<td>1</td>
</tr>
<tr>
<td>1.3 The Structure of Blockchains</td>
<td>3</td>
</tr>
<tr>
<td>1.4 Blockchain Applications</td>
<td>4</td>
</tr>
<tr>
<td>1.5 The Blockchain Life Cycle</td>
<td>4</td>
</tr>
<tr>
<td>1.6 Consensus: The Driving Force of Blockchains</td>
<td>5</td>
</tr>
<tr>
<td>1.7 Blockchains in Use</td>
<td>6</td>
</tr>
<tr>
<td>1.8 Cryptoassets</td>
<td>7</td>
</tr>
<tr>
<td>1.9 Why Do Fraud and Manipulation Occur in Cryptocurrency Markets?</td>
<td>11</td>
</tr>
<tr>
<td>1.10 Pump and Dumps</td>
<td>14</td>
</tr>
<tr>
<td>1.11 Inflated Trading Volume</td>
<td>16</td>
</tr>
<tr>
<td>1.12 Exchange DDoS Attacks</td>
<td>19</td>
</tr>
<tr>
<td>1.13 Hacks and Exploitations</td>
<td>22</td>
</tr>
<tr>
<td>1.14 Flash Crashes</td>
<td>28</td>
</tr>
<tr>
<td>1.15 Order Book-Based Manipulations</td>
<td>33</td>
</tr>
<tr>
<td>1.16 Stablecoins and Tether</td>
<td>36</td>
</tr>
<tr>
<td>1.17 Summary and Conclusions</td>
<td>42</td>
</tr>
<tr>
<td>Chapter 1: Test Your Knowledge</td>
<td>47</td>
</tr>
<tr>
<td>Chapter 1: Solutions and Suggested Responses</td>
<td>53</td>
</tr>
<tr>
<td>Glossary</td>
<td>59</td>
</tr>
<tr>
<td>Index</td>
<td>61</td>
</tr>
</tbody>
</table>

**NOTICE**

This course and test have been adapted from supplemental materials and uses the materials entitled *Corruption and Fraud in Financial Markets* © 2020 Carol Alexander and Douglas Cumming. Displayed by permission of the publisher, John Wiley & Sons, Inc., Hoboken, New Jersey.

Use of these materials or services provided by Professional Education Services, LP (“PES”) is governed by the Terms and Conditions on PES’ website (www.mypescpe.com). PES provides this course with the understanding that it is not providing any accounting, legal, or other professional advice and assumes no liability whatsoever in connection with its use. PES has used diligent efforts to provide quality information and material to its customers, but does not warrant or guarantee the accuracy, timeliness, completeness, or currency of the information contained herein. Ultimately, the responsibility to comply with applicable legal requirements falls solely on the individual licensee, not PES. PES encourages you to contact your state Board or licensing agency for the latest information and to confirm or clarify any questions or concerns you have regarding your duties or obligations as a licensed professional.

© Professional Education Services, LP 2020

Program Publication Date 8/24/2020
THIS PAGE INTENTIONALLY LEFT BLANK.
CHAPTER 1: FRAUD AND MANIPULATION WITHIN CRYPTOCURRENCY MARKETS

Chapter Objective

After completing this chapter, you should be able to:

- Identify the characteristics of cryptocurrencies.

1.1 INTRODUCTION

Digital currencies are electronic representations of value that include a broad range of common payment systems, such as gift cards, air miles, and mobile coupons. Virtual currencies are a subset of digital currencies which, rather than being denominated in fiat currency, (government backed currency, e.g. USD, GBP), use their own unit of account. Examples include those within online games or internet-based currencies. Cryptocurrencies are a type of virtual currency (and therefore a digital currency) but rely on techniques from cryptography for security, which allow them to function without a centralized authority, such as a central bank, government, or private company.1 (See Figure 1.1.) The rise of cryptocurrencies was led by the introduction of bitcoin in 2008, which was one of the first to use a decentralized public ledger, known as a blockchain, to record transactions without the use of a trusted central authority.

FIGURE 1.1 CRYPTOCURRENCIES AS A SUBSET OF A BROADER CATEGORY OF DIGITAL CURRENCIES.

<table>
<thead>
<tr>
<th>Digital Currencies</th>
<th>Virtual Currencies</th>
<th>Cryptocurrencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digitally represents value</td>
<td>Not denominated in legal tender</td>
<td>Uses techniques from cryptography to validate transactions</td>
</tr>
<tr>
<td>Convertible to real-world goods, services, money</td>
<td>Convertible</td>
<td>+ Over 1000 other cryptocurrencies</td>
</tr>
<tr>
<td>Decentralised</td>
<td>No central authority</td>
<td></td>
</tr>
</tbody>
</table>

1.2 BEGINNING AT THE BEGINNING: WHAT BLOCKCHAINS ARE

A blockchain is a data structure that makes it possible to create a digital ledger of data and share it among a network of independent parties. There are many different types of blockchains.

---

1 Cryptography is the study of techniques for private communication in the presence of third parties called adversaries.
- **Public blockchains**: Public blockchains, such as Bitcoin, are large distributed networks that are run through a native token. They’re open for anyone to participate at any level and have open-source code that their community maintains.

- **Permissioned blockchains**: Permissioned blockchains, such as Ripple, control roles that individuals can play within the network. They’re still large and distributed systems that use a native token. Their core code may or may not be open source.

- **Private blockchains**: Private blockchains tend to be smaller and do not utilize a token. Their membership is closely controlled. These types of blockchains are favored by consortiums that have trusted members and trade confidential information.

All three types of blockchains use cryptography to allow each participant on any given network to manage the ledger in a secure way without the need for a central authority to enforce the rules. The removal of central authority from database structure is one of the most important and powerful aspects of blockchains.

### Remember

Blockchains create permanent records and histories of transactions, but nothing is really permanent. The permanence of the record is based on the permanence of the network. In the context of blockchains, this means that a large portion of a blockchain community would all have to agree to change the information and are incentivized not to change the data.

When data is recorded in a blockchain, it’s extremely difficult to change or remove it. When someone wants to add a record to a blockchain, also called a *transaction* or an *entry*, users in the network who have validation control verify the proposed transaction. This is where things get tricky because every blockchain has a slightly different spin on how this should work and who can validate a transaction.

#### 1.2.1 What blockchains do

A blockchain is a peer-to-peer system with no central authority managing data flow. One of the key ways to removing central control while maintaining data integrity is to have a large distributed network of independent users. This means that the computers that make up the network are in more than one location. These computers are often referred to as *full nodes*.

To prevent the network from being corrupted, not only are blockchains decentralized but they often also utilize a *cryptocurrency*. A *cryptocurrency* is a digital token that has a market value. Cryptocurrencies are traded on exchanges like stocks.

Cryptocurrencies work a little differently for each blockchain. Basically, the software pays the hardware to operate. The software is the blockchain protocol. Well-known blockchain protocols include Bitcoin, Ethereum, Ripple, Hyperledger, and Factom. The hardware consists of the full nodes that are securing the data in the network.
1.2.2 Why blockchains matter

Blockchains are now recognized as the “fifth evolution” of computing, the missing trust layer for the Internet. This is one of the reasons that so many people have become excited about this topic.

Blockchains can create trust in digital data. When information has been written into a blockchain database, it’s nearly impossible to remove or change it. This capability has never existed before.

When data is permanent and reliable in a digital format, you can transact business online in ways that, in the past, were only possible offline. Everything that has stayed analog, including property rights and identity, can now be created and maintained online. Slow business and banking processes, such as money wires and fund settlements, can now be done nearly instantaneously. The implications for secure digital records are enormous for the global economy.

The first applications created were designed to piggyback on the secure digital value transfer that blockchains enable through the trading of their native tokens. These included things like the movement of money and assets. But the possibilities of the blockchain networks go far beyond the movement of value.

1.3 THE STRUCTURE OF BLOCKCHAINS

Blockchains are composed of three core parts:

- **Block**: A list of transactions recorded into a ledger over a given period. The size, period, and triggering event for blocks is different for every blockchain.

  Not all blockchains are recording and securing a record of the movement of their cryptocurrency as their primary objective. But all blockchain do record the movement of their cryptocurrency or token. Think of the transaction as simply being the recording of data. Assigning a value to it (such as happens in a financial transaction) is used to interpret what that data means.

- **Chain**: A hash that links one block to another, mathematically “chaining” them together. This is one of the most difficult concepts in blockchain to comprehend. It’s also the magic that glues blockchains together and allows them to create mathematical trust.

  The hash in blockchain is created from the data that was in the previous block. The hash is a fingerprint of this data and locks blocks in order and time.

- **Network**: The network is composed of “full nodes.” Think of them as the computer running an algorithm that is securing the network. Each node contains a complete record of all the transactions that were ever recorded in that blockchain.

  The nodes are located all over the world and can be operated by anyone. It’s difficult, expensive, and time-consuming to operate a full node, so people don’t do it for free. They’re incentivized to operate a node because they want to earn cryptocurrency. The underlying blockchain algorithm rewards them for their service. The reward is usually a token or cryptocurrency, like Bitcoin.
Although blockchains are a relatively new innovation, hashing is not. Hashing was invented over 30 years ago. This old innovation is being used because it creates a one-way function that cannot be decrypted. A hashing function creates a mathematical algorithm that maps data of any size to a bit string of a fixed size. A bit string is usually 32 characters long, which then represents the data that was hashed. The Secure Hash Algorithm (SHA) is one of some cryptographic hash functions used in blockchains. SHA-256 is a common algorithm that generates an almost-unique, fixed-size 256-bit (32-byte) hash. For practical purposes, think of a hash as a digital fingerprint of data that is used to lock it in place within the blockchain.

The terms *Bitcoin* and *blockchain* are often used interchangeably, but they're not the same. Bitcoin has a blockchain. The Bitcoin blockchain is the underlying protocol that enables the secure transfer of Bitcoin. The term *Bitcoin* is the name of the cryptocurrency that powers the Bitcoin network. The blockchain is a class of software, and Bitcoin is a specific cryptocurrency.

### 1.4 BLOCKCHAIN APPLICATIONS

Blockchain applications are built around the idea that network is the arbitrator. This type of system is an unforgiving and blind environment. Computer code becomes law, and rules are executed as they were written and interpreted by the network. Computers don’t have the same social biases and behaviors as humans do.

The network can’t interpret intent (at least not yet). Insurance contracts arbitrated on a blockchain have been heavily investigated as a use case built around this idea.

Another interesting thing that blockchains enable is impeccable record keeping. They can be used to create a clear timeline of who did what and when. Many industries and regulatory bodies spend countless hours trying to assess this problem. Blockchain-enabled record keeping will relieve some of the burdens that are created when we try to interpret the past.

### 1.5 THE BLOCKCHAIN LIFE CYCLE

Blockchains originated with the creation of Bitcoin. It demonstrated that a group of individuals who had never met could operate online within a system that was desensitized to cheat others that were cooperating on the network.

The original Bitcoin network was built to secure the Bitcoin cryptocurrency. It has around 5,000 full nodes.
and is globally distributed. It’s primarily used to trade Bitcoin and exchange value, but the community saw the potential of doing a lot more with the network. Because of its size and time-tested security, it’s also being used to secure other smaller blockchains and blockchain applications.

The Ethereum network is a second evolution of the blockchain concept. It takes the traditional blockchain structure and adds a programming language that is built inside of it. Like Bitcoin, it has over 5,000 full nodes and is globally distributed. Ethereum is primarily used to trade Ether, make smart contracts, and create decentralized autonomous organizations (DAOs). It’s also being used to secure blockchain applications and smaller blockchains.

The Factom network is the third evolution in blockchain technology. It utilizes a lighter consensus system, incorporates voting, and stores a lot more information. It was built primarily to secure data and system. Factom operates with federated nodes and an unlimited number of auditing nodes. Its network is small, so it anchors itself into other distributed networks building bridges across the carries blockchains.

1.6 CONSENSUS: THE DRIVING FORCE OF BLOCKCHAINS

Blockchains are powerful tools because they create honest systems that self-correct without the need of a third party to enforce the rules. They accomplish the enforcement of rules through their consensus algorithm.

In the blockchain world, consensus is the process of developing an agreement among a group of commonly mistrusting shareholders. These are the full nodes on the network. The full nodes are validating transactions that are entered into the network to be recorded as part of the ledger.

Each blockchain has its own algorithms for creating agreement within its network on the entries being added. There are many different models for creating consensus because each blockchain is creating different kinds of entries. Some blockchains are trading value, others are storing data, and others are securing systems and contracts.

Bitcoin, for example, is trading the value of its token between members on its network. The tokens have a market value, so the requirements related to performance, scalability, consistency, threat model, and failure model will be higher. Bitcoin operates under the assumption that a malicious attacker may want to corrupt the history of trades in order to steal tokens. Bitcoin prevents this from happening by using a consensus model called “proof of work” that solves the Byzantine general’s problem: “How do you know that the information you are looking at has not been changed internally or externally?” Because changing or manipulating data is almost always possible, the reliability of data is a big problem for computer science.

Most blockchains operate under the premise that they will be attacked by outside forces or by users of the system. The expected threat and the degree of trust that the network has in the nodes that operate the blockchain will determine the type of consensus algorithm that they use to settle their ledger. For example, Bitcoin and Ethereum expect a very high degree of threat and use a strong consensus algorithm called proof of work. There is no trust in the network.
On the other end of the spectrum, blockchains that are used to record financial transactions between known parties can use a lighter and faster consensus. Their need for high-speed transactions is more important. Proof of work is too slow and costly for them to operate because of the comparatively few participants within the network and immediate finality need for each transaction.

### 1.7 Blockchains in Use

Hundreds of blockchains and blockchain applications are in existence today. The whole world has become obsessed with the ideas of moving money faster, incorporating and governing in a distributed network, and building secure applications and hardware.

You can see many of these public blockchains by going to a cryptocurrency exchange.

Blockchains are moving beyond the trading value market and are being incorporated into all sorts of industries. Blockchains add a new trust layer that now makes working online secure in a way that was not possible beforehand.

#### 1.7.1 Current Blockchain Uses

Most up-and-running blockchain applications revolve around moving money or other forms of value quickly and cheaply. This includes trading public company stock, paying employees in other countries, and exchanging one currency for another.

Blockchains are also now being used as part of a software security stack. The U.S. Department of Homeland Security has been investigating blockchain software that secures Internet of Things (IoT) devices. The IoT world has some of the most to gain from this innovation, because it’s especially vulnerable to spoofing and other forms of hacking. IoT devices have also become more pervasive, and security has become more reliant on them. Hospital systems, self-driving cars, and safety systems are prime examples.

DAOs are another interesting blockchain innovation. This type of blockchain application represents a new way to organize and incorporate companies online. DAOs have been used to organize and invest funds via the Ethereum network.

#### 1.7.2 Future Blockchain Applications

Larger and longer-run blockchain projects that are being explored now include government-backed land record systems, identity, and international travel security applications.

The possibilities of a blockchain-infused future have excited the imaginations of business people, governments, political groups, and humanitarians across the world. Countries such as the UK, Singapore, and the United Arab Emirates see it as a way to cut cost, create new financial instruments, and keep clean records. They have active investments and initiatives exploring blockchain.

Blockchains have laid a foundation where the need for trust has been taken out of the equation. Where before asking for “trust” was a big deal, with blockchains it’s small. Also, the infrastructure that enforces the rule if that trust is broken can be lighter. Much of society is built on trust and enforcement of rules. The
social and economic implications of blockchain applications can be emotionally and politically polarizing because blockchain will change how we structure value-based and socially based transactions.

1.8 CRYPTOASSETS

In general, in this chapter, each financial instrument we discuss we refer to as a cryptocurrency. A cryptocurrency is in fact quite a narrow, albeit recognizable, description of a subset of an umbrella class of cryptoassets, a nomenclature appearing increasingly in regulatory frameworks. There is no single agreed definition of a cryptoasset, but in general they are cryptographically secured digital representations of value or contractual rights which can be stored, transferred or traded electronically. They are powered by a form of Distributed Ledger Technology (DLT). The different types of DLT are beyond the scope of this chapter, but DLT can be thought of as an umbrella of technological solutions which facilitate the distribution of records or information (the kind you might find on accounting ledgers), among all those who use it, either privately or publicly.\(^2\)

The Bitcoin blockchain was the first fully functional DLT, used and maintained by a network of communicating nodes which run the client software.\(^3\) Over time, many other projects have emerged. The level of innovation in these projects varies greatly: some are near clones of bitcoin or other cryptoassets and simply feature different parameter values (e.g. transaction speed, currency supply, and issuance scheme); however, some have emerged which, while sharing some familiar concepts, provide novel and innovative features that represent substantial differences.

Producing a universal taxonomy of all these new and emerging cryptoassets has proven difficult. However, recent published reports by the Financial Conduct Authority (FCA) and European Banking Association (EBA) settle on a similar framework, splitting cryptoassets into three categories as shown in Figure 1.2. The way a cryptoasset is used, or its features, mean it could fall under more than one category. For example, although bitcoin was initially intended as a means of exchange (exchange token), most current users of bitcoin hold it for investment purposes (security token).

This framework also identifies the three main use cases of cryptoassets:

1. As a means of exchange to enable the buying or selling of goods and services, or to facilitate regulated payment services.
2. For investment, by gaining direct exposure by holding and trading cryptoassets, or indirect exposure by holding and trading financial instruments which reference cryptoassets.
3. To support capital raising and/or the creation of decentralized networks through Initial Coin Offerings (ICOs).

ICOs, (or token sales), involve raising funds from the public by issuing project-specific exchange, security or utility tokens in exchange for an existing cryptoasset or fiat currency. They can be viewed as an alternative to traditional capital raising instruments and individuals and firms typically buy ICO tokens as an investment, to secure access to a specific service, or to gain other rights attached to a token.

---


\(^3\) A node is any device that connects to the Bitcoin network.
While ICOs are beyond the scope of this chapter, they present their own regulatory challenges: recent research identified that in 2017, 78% of ICO-initiated projects that achieved market capitalization over $50 million were scams.4

Crypto tokens are typically obtained via one of four methods: (1) participating in the transaction validation process (e.g. ‘mining’), which yields crypto as a reward for expending resources; (2) receiving directly from another crypto holder; (3) investing directly in an ICO; or (4), purchasing through a crypto exchange.

**FIGURE 1.2 TAXONOMY OF CRYPTOASSETS AS DESCRIBED BY FCA AND EBA REPORTS PUBLISHED IN OCT 2018 AND JAN 2019, RESPECTIVELY.**

Crypto exchanges form a fundamental part of the ecosystem as they offer a secondary market in which crypto can be bought or sold in exchange for either fiat currency or other crypto tokens. They are also the main target of a lot of the manipulations we examine, since they provide financial markets (which can be manipulated), and often become single stores of immense value (which can be hacked and stolen from). As shown in Figure 1.3, it is typical to see millions of dollars’ worth of crypto traded every 24 hours; this volume is required to be stored in exchange accounts. For example, Bittrex, a US-based crypto exchange holds $233.5 million worth of crypto tokens in one Ethereum wallet address.7

7 As measured on 16 February 2019 using the Bittrex’s Ethereum public hot-wallet address: 0xfb1b73c4f0bda4f67dca266ce6ef42f520fbb98.
The market price and traded volume of the 2000+ crypto tokens currently listed on exchanges combine to form an asset class with a market capitalization (market price multiplied by the number of existing currency units) of $121bn.\(^8\) While still relatively small compared to traditional asset classes, the growth of the crypto market in recent years has drawn the attention of traders and investors who look to profit from buying and selling units of cryptocurrency. Many traditional financial institutions, predominantly hedge funds, are reported to be moving into the area; partly attracted by the high volatility of prices (Chan, et al., 2017), and recent price rises.\(^9\)

**FIGURE 1.3 COMPARATIVE 2018 VS. 2019 DAILY CRYPTO EXCHANGE REVENUE ESTIMATED WITH COINMARKETCAP REPORTED 24HR VOLUME AND FEES LISTED ON EACH EXCHANGE’S WEBSITE. ALTHOUGH TRADE VOLUME HAS DROPPED CONSIDERABLY IN 2019, TOP EXCHANGES STILL MAINTAIN GOOD REVENUES.**

The first major exchange, Mt. Gox, originally designed in 2007 as an exchange for fantasy trading cards, was launched in 2010 allowing users to trade bitcoins and grew to handle most global bitcoin trading.\(^10\) Due to several technical issues throughout its existence, (as detailed later in Section 1.13), bitcoins were being removed over a prolonged period by an unknown entity. The loss of bitcoins caused Mt. Gox to collapse in 2013 and then file for bankruptcy in 2014. Despite Mt. Gox’s failure, replacements quickly emerged and running a crypto exchange proved a lucrative business: the top 10 exchanges in 2017 we estimated to be generating as much as $3 million in fees per day during 2017. Today there are over 200 exchanges operating globally, with $19bn transacted over a typical 24hr period.\(^11\)

One of the most important, often missed, factors of exchange trading is that a significant portion of trading occurs separately from the blockchain. Although normal cryptocurrency transactions are blockchain-based, i.e. if you were to send a friend some bitcoin from your wallet to theirs, you would be able to view this transaction on the public blockchain once completed with a provided transaction hash. However, trades on an exchange platform are done simply by updating a user’s account balance within

---

\(^8\) As measured on 11 February 2019 from coinmarketcap.com.


\(^10\) Mt. Gox was appropriately short for ‘Magic the Gathering Online eXchange’.

the service’s database. As such, when an exchange trade is completed, you are not actually sending crypto to another person, (or vice versa), you are relying on the exchange to reflect this update within their internal records. The primary reason for this, in general, is that blockchains are too slow to handle the frequency and volume of exchange trades.

To be able to trade, users must have funds in their exchange account. To fund an account with crypto, a user transfers their crypto into the exchange’s designated blockchain wallet, and the quantity received by the exchange is credited to the individual user’s trading account in their internal system. The wallet addresses that an exchange gives you to deposit into are not your addresses. The exchange is holding your crypto for you, and they can do whatever they want with it: you do not technically have complete ownership of the crypto until you choose to withdraw it. On some exchanges, known as ‘banked exchanges’, fiat currency can be used as funding via a transfer to the exchange’s bank account. Exchanges that do not accept fiat currency deposits and withdrawals are referred to as unbanked, since they do not (usually) possess a traditional banking license to facilitate this process. Whether crypto or fiat, once a deposit is completed, the user is then able to trade with other users of that exchange.

Withdrawals of cryptocurrencies or fiat are done in a similar way to how they are deposited. When you withdraw crypto, you are not sent crypto from ‘your’ addresses either, but rather from other addresses in the exchange’s wallet and, often, your withdrawal will be part of the same transaction as other people’s withdrawals.

Almost all crypto exchanges use a limit order book to facilitate trading. A limit order book represents the list of orders that an exchange uses to record the interest of buyers and sellers of a crypto-to-crypto or crypto-to-fiat instrument. At each price level, the number of shares being offered and demanded is recorded.

The two most basic types of order on a typical exchange are ‘limit’ and ‘market’ orders. Limit orders are those which indicate a price and quantity at which a trader is willing to buy (bid) or sell (ask) an asset (in this context, a particular crypto), and these are recorded in the order book. Traders who hold inventory and simultaneously post limit orders to both buy and sell are referred to as market makers. Market makers are important in providing liquidity and are compensated for the risk of holding assets through the spread (difference between bid and ask orders they post).

A market order does not specify a price, but a quantity and direction (buy or sell). Market orders are matched with limit orders from the opposite side of the order book. For example, a market order to buy one bitcoin would be filled from limit sell orders, starting from the lowest price level, (known as the ‘best ask’). If the quantity of the market order is greater than that of the before combined volume of limit sell orders at that price level, the order is partially filled at that price level and the next best price is used to fill the remaining quantity. The matching process continues until the entire order has been filled. Figure 1.4 gives a visual representation of an order book (on the left-hand side) with price on the x-axis and buy/sell limit order cumulative volume on the y-axis. The most recently filled orders are shown under ‘trade history’ (on the right-hand side) and list the price and quantity at which trades have been executed.

Other types of order include stop orders that specify a ‘stop price’, which if hit, triggers the placement of a pre-specified limit or market order. Stop orders can help traders protect profits, limit losses or initiate new positions but (as seen in Section 1.12) may unknowingly magnify the effect of market manipulation.
Most cryptocurrencies are cross-listed assets, i.e. traded on multiple exchanges. This results in a global price determined by multiple exchanges simultaneously, leading to inter-exchange dynamics and price discovery implications (Brandvold, et al., 2015). Each exchange will have its own price for a cryptocurrency, which may vary depending on factors such as local demand, exchange reputability and trading fee structure. If prices between two exchanges diverge enough, variants of exchange arbitrage (buying on the cheaper exchange, and selling on the more expensive exchange) tailored specifically to cryptocurrency markets, will be likely to cause the prices to converge, where possible. Due to this fragmented global nature of the market, manipulation occurring on one exchange in one region of the world may affect the price of a cryptocurrency on other exchanges around the world.

FIGURE 1.4 EXAMPLE LIMIT ORDER BOOK AS SEEN ON ONE CRYPTOCURRENCY EXCHANGE.

The purpose of this chapter is to provide an overview of the many alleged manipulations occurring within crypto trading markets. Firstly, in Section 1.9 we attempt to document and explain the reasons why the cryptocurrency markets are an attractive target for manipulation. Next, we discuss each manipulation in detail: Section 1.10 introduces ‘pump and dumps’ where influential entities target and manipulate the price of certain cryptos; in 8.4 we discuss the alleged historic inflation of trading volume by certain exchanges; 8.5 examines the combination of a DDoS attack with specific trading patterns to achieve profits by manipulating exchange market activity; 12 8.6 and 8.7 review hacks and flash crashes within crypto; 8.8 examines two order book-based manipulations known as quote stuffing and quote spoofing, which are designed to mislead or slow other traders; and 8.9 introduces the concept of a stablecoin and looks at the history and ongoing controversy of Tether, the largest stablecoin. Finally, 8.10 discusses the latest trends and how they might affect the propensity for fraud and regulation.

1.9 WHY DO FRAUD AND MANIPULATION OCCUR IN CRYPTOCURRENCY MARKETS?

Almost every fraud or manipulation we discuss in this chapter is derived from approaches seen elsewhere, often in traditional financial markets, which, while used historically without sanctions, would today be quickly reprimanded, given tighter modern regulation and accountability. In cryptocurrencies, however, their use remains prominent to this day (with the exception of inflated trading volume, which was stopped in early 2017). The occurrence of each manipulation covered in this chapter is linked to one or more of the reasons below.

12 A Distributed Denial of Service (DDoS) event is an attempt by an attacker to overwhelm a network target with a large volume of incoming messages (network traffic).
1.9.1 Lack of Consistent Regulation

Many regulators around the globe have been cautious about imposing potentially restrictive regulation on the areas of cryptocurrencies, cryptocurrency trading, and related blockchain technology. Even for those seeking to be proactive, correct regulation has posed considerable challenges, as summarized in Pieters and Vivanco, 2017. Simply providing a coherent definition of what a cryptocurrency is (and thus an appropriate regulatory framework) has proved challenging, with different jurisdictions providing varying classifications – including as a currency, commodity, or payment system. In certain cases, authorities within the same country have classified cryptocurrencies in different ways, depending on their own area of oversight (Sotiropoulou and Guegan, 2017). Where stances have been taken, they range considerably, from permissive to hostile; a summary of the rapidly evolving regional differences can be seen in other existing work (Chohan, 2017).

Whatever stance a regional regulator takes regarding cryptocurrencies, it may be circumvented due to the ability of cryptocurrency to be accessed and transacted globally: participants (especially trading exchanges) can choose to operate within the jurisdiction most amicable to their objectives (Sotiropoulou and Guegan, 2017). In 2017, it was found that 78% of North American-based exchanges held a government license/authorization, compared to only 15% of the exchanges in Asia-Pacific (Hileman and Rauchs, 2017). In addition to an exchange’s decision as to which jurisdiction they prefer to reside under, traders may also take similar considerations into account when deciding within which exchange to trade. Consequently, it has been observed that exchanges that do not require identity validation exhibit statistically different price dynamics than those that do require identity validation (Pieters and Vivanco, 2017).

1.9.2 Relative Anonymity

There is a high level of anonymity for participants in crypto markets when compared to other financial markets. Many traditional financial exchanges are required to enforce Know-Your-Customer (KYC) and Anti-Money-Laundering (AML) procedures, which include the detailed records of traders using their exchanges. Some cryptocurrency exchanges do enforce KYC and AML procedures; however, some do not. As such, cryptocurrency trading exchanges may be able to identify the suspicious trades or accounts but may not be able to link this to real-world individuals and prevent them from attempting manipulations again through different accounts.

The onboarding requirements of several leading exchanges in 2018 were reviewed by the New York State Office of the Attorney General, (henceforth referred to as the OAG report).13 The report found large variation in the information required to confirm a user’s identity. Most require customers to submit some form of government-issued identification, especially for fiat trading. However, others require little more than an email address to begin trading crypto only. Given that this review only encompassed the largest crypto exchanges, these limited KYC procedures are likely to be similar or worse at smaller venues.

13 New York State Office of the Attorney General (OAG), (18 Sep 2018), Virtual Markets Integrity Initiative, see: https://on.ny.gov/2QJIMGJ.
Most exchanges claim to stop customers from unauthorized jurisdictions from accessing their platform by monitoring IP addresses. However, the OAG report raised questions regarding the ability to enforce this. To evade such monitoring, users can mask their IP addresses using a virtual private network (VPN), which routes activity through a third-party network and obfuscates the location of a log-in. For IP monitoring to be effective, platforms must take reasonable steps to unmask or block customers that attempt to access their site via known VPN connections, yet only two of the ten surveyed, (Bitstamp and Poloniex), purported to limit VPN access.

Furthermore, whereas many traditional financial markets have monitored locations for electronic communication relating to certain price movements, the majority of the discussion of cryptocurrency markets happens publicly on social media – popular platforms include Twitter and Reddit – where it is common for people to use an alias unconnected to their real-life identity.

1.9.3 Low Barriers to Entry

Barriers to entry for cryptocurrency trading are extremely low. While real-time (live) data streams and direct market access are often costly in traditional financial markets, in cryptocurrency markets these are provided for free: either by the exchanges themselves or by public data providers. Many participants enter cryptocurrency trading with no real prior trading experience, often in search of quick profits. This produces two effects:

1. Inexperienced/naïve market participants may be more prone to being manipulated; for example, believing spoofed order book data/fake volume and fictitious statements about certain cryptocurrencies on social media.

2. Inexperienced/naïve market participants may engage in certain forms of manipulation without realizing what they are doing. For example, traders participating in pump and dump groups may not be aware that they are actively manipulating the price.

1.9.4 Exchange Standards and Sophistication

Traditional stock exchanges, such as the NYSE or NASDAQ, are subject to extensive disclosure obligations regarding their ownership, operation, and rules. In contrast, anyone can set up a cryptocurrency exchange. For example, in the US, crypto asset platforms are currently not registered as trading venues under federal securities laws.

The ability of anyone to set up a trading venue increases the likelihood of technical vulnerabilities; such vulnerabilities can be exploited through DDoS attacks (see Section 1.12) and hacks (see Section 1.13).

There are several well-understood security practices that exchanges would be expected to adopt, yet many do not or do not enable it by default. Firstly, two-factor authentication is a data security measure that requires a user to input both a password and an additional piece of information in order to log in to

---

14 An IP address acts as a unique identifier assigned to a computer connected to the internet, allowing a website operator to monitor the computers that connect to its site. Among other uses, monitoring IP addresses allows a website operator to determine the approximate geographic location of users and track suspicious behaviour coming from a particular computer connection.

15 For example, see coinmarketcap.com or cryptocompare.com.
an account. The additional piece of information is often a code sent to a phone, or a random number generated by an app or a token. Two-factor authentication helps protect an account even if a password is compromised. Most of the largest exchanges offer two-factor authentication; indeed all exchanges surveyed in the OAG’s report do, but none by default.

In theory, crypto exchanges should keep a high percentage of the crypto assets in their possession in so-called ‘cold storage’. Using cold storage is a security practice wherein the private keys to crypto are kept off the internet and thus not susceptible to hacking – in contrast to so-called ‘hot storage’, where keys are stored on a networked device. Several exchanges keep an alarming amount of crypto in their hot-wallets. The OAG report highlighted that some participating exchanges did not provide a meaningful response to the question of cold storage usage.

In an attempt to convince users of the safety of their funds held with the exchange, exchanges commonly perform security audits; 60% of large exchanges have their security audit performed by external parties; however, 65% of smaller exchanges have been found to perform their audits internally (Hileman and Rauchs, 2017), and may not provide details on the procedure of the audit.

Many crypto exchanges have no formal policies governing automated trading, market manipulation, and abusive trading. Some claim to monitor trading behaviour and have strategies to limit ‘message rates’ submitted to exchanges (high message rates are often a marker of an abusive trading system), or to suspend or block traders that submitted an excessive number of small orders in a given time frame (e.g. quote stuffing as discussed in Section 1.15.1). The OAG report identifies that ‘the industry has yet to implement serious market surveillance capacities, akin to detect and punish suspicious trading activity’.

1.10 PUMP AND DUMPS

The first manipulation we examine is known as a ‘pump and dump’. In general, a pump and dump scheme is an approach which involves an entity accumulating a large amount of a target asset, typically one with low market capitalization and a low unit price, and subsequently promoting its purchase as an opportunity for substantial future returns, (in traditional pump and dumps, promotions may claim to have inside information of future events that are expected to cause price increases). The promotion is designed to create a significant buying demand which increases the price (i.e. the ‘pump’). The promotion continues, and while others are still trying to enter, the initial position is fully unwound for a considerable profit. The promotion is then halted, and the price then crashes (i.e. the ‘dump’) often incurring significant losses for those slow to react.

Within cryptocurrency markets, a variation of the above has become popular. Groups are formed on social chat platforms where low market capitalization cryptocurrencies are selected and advertised by administrators. Members of the group then engage in intensive purchasing within a short time span (within a couple of minutes). The group’s mutual buying pressure causes a sudden rise in price. Unlike in more traditional markets, where those purchasing are doing so on false information (being duped by the promoter), members in these cryptocurrency groups are aware of what is occurring and are willing to participate in the belief they can sell to others who have been slower to act on the information.

16 Medium, (8 Aug 2018), Which crypto exchange is putting your funds most at risk?, see https://bit.ly/2IkzgK5
Numerous cryptocurrency pump and dump groups have been established with member counts ranging into the tens of thousands. The groups are advertised widely within the cryptocurrency social media ecosystem – across Twitter, Slack, Discord, and Reddit – to attract new members. Most pump and dump groups follow a similar process: the coordinating entity sends out one (or many) messages advertising the time and trading exchange upon which the ‘pump’ will occur, but not which cryptocurrency is being chosen. At the specified time, the coordinating entity informs the group of which target cryptocurrency to buy. People are willing to complete a purchase, (even at a premium compared to a few minutes before), based on their belief they can sell at a higher price while the cryptocurrency is being pumped. If members do make money, it is likely that they have done so at the expense of someone else in the group who has been slower at buying into the cryptocurrency. Some groups have tried to address this by prolonging price increases. One mechanism to do this is encouraging their members to promote the chosen cryptocurrency on social media platforms after it has been announced.

Groups are either free or cost a one-off or monthly fee to join. Those that cost money claim to offer better information or premium services, (including the release of information in advance of its dissemination to related free groups). Groups are also commonly locked so that only the coordinating entity can post. This avoids their notifications being lost in the noise of other messages. It also prevents any members who have grievances over losing money from communicating them with other members. The coordinating entities usually provide screenshots of previous pump events to show the price increases achieved historically.

There are historical examples of the price rising in the minutes before a cryptocurrency is announced. It has been suggested that this is the coordinating entity accumulating a large position in the chosen cryptocurrency before the announcement. They then place sell orders further up the order book, so any market orders placed in the frenzy caused by the pump event hit their sell orders. As the members are entering positions, the coordinating entity may be exiting their position.

Telegram is the most common mobile chat platform that groups are formed on, due to its high level of anonymity and encryption. This coupled with the relative anonymity of markets as discussed in Section 1.9.2, means it is difficult to identify perpetrators. Furthermore, with over 1000 cryptocurrencies, many of which have market capitalizations under $100,000, it is possible for the coordinating entities to own a substantial share of a cryptocurrency before commencing any pump and dump (Dierksmeier, 2016); the ability for anyone to coordinate an event, and the demand by traders looking for a quick profit, suggest this manipulation is also made possible by the low barriers to entry, see Section 1.9.3.

In the literature, Xu and Livshits (2018) are one of the first to provide a detailed study of pump-and-dump activities in cryptocurrency markets. They investigate 220 pump-and-dump activities organized in Telegram channels and construct a model which can predict the likelihood of a given coin pump prior to the event. This information is converted into a sample trading strategy where, given the exchange and time of a pump (information usually disseminated prior to a Telegram-coordinated event), the most likely coin to be pumped can be found from features such as market capitalization and recent return/volatility profiles.
While it is difficult to decipher true ‘pump and dumps’ without insider knowledge of such a scheme, we are able to present a case study which successfully identifies one clear example which occurred in July 2017. We were able to discover this post hoc by linking a free Telegram group’s historically time-stamped messages to publicly available market data during the same period.

1.10.1 Case Studies

On 12 July 2017, one Telegram group coordinated a pump event. Updates were given on their Telegram channel throughout the day, counting down to the pre-specified event time, and providing provisional instructions to members in the group. At 5 p.m., the chosen cryptocurrency was announced, one called Triggers (ticker: TRIG). Figure 1.5 shows the price evolution during the event. When the announcement was made the TRIG/USD price was $0.089. Once the announcement was made, trading volume increased within seconds, causing a sharp jump in the price. The price hit a high of $0.18 momentarily, before declining rapidly; subsequent volatility ensued before the price returned to its pre-announcement region. Consequently, the market capitalization of TRIG grew 102.2%, a change of millions of dollars.

FIGURE 1.5 TRIG/USD PRICE AND VOLUME DURING PUMP AND DUMP EVENT. JUST BEFORE 17:00 A SPIKE IN VOLUME CAUSES THE PRICE TO RAPIDLY INCREASE FROM BELOW $0.08 TO $0.18 IN A MATTER OF SECONDS. THIS IS QUICKLY FOLLOWED BY A SHARP DECLINE BACK TO THE EARLIER PRICE LEVEL. TRADING VOLUME AFTER THE EVENT DOES INCREASE, BUT WITH A DAMPENED EFFECT ON THE PRICE.

![Graph showing TRIG/USD price and volume during pump and dump event.]

It should be noted that although TRIG was chosen as a target, its development team would have had no involvement or knowledge of what was happening. Its price and trading volume have increased significantly since then, so it is unlikely to be the target of such an event again.

1.11 INFLATED TRADING VOLUME

The next manipulation we cover no longer occurs, but previously had a big impact on the perception of the global cryptocurrency trading ecosystem. Prior to January 2017, Chinese cryptocurrency exchanges dominated bitcoin cryptocurrency trading volume, with December 2016 data showing they held 98.3% of
global volume. However, it has been alleged that the volumes reported by certain Chinese exchanges at the time were in fact misleading and not an accurate representation of legitimate market activity. This belief was reinforced by the sudden and dramatic drop of trading volume in January 2017, following the increased involvement of the People’s Bank of China (PBoC), China’s central bank, which initiated the removal of mechanisms enabling the potential inflation of trading volume.

Trading data from the exchange further arouses suspicion due to counter-intuitive findings. In a study of cryptocurrency exchange dynamics using data between November 2016 and January 2017 (Dimpfl, 2017), it was found that Chinese exchanges exhibited the highest market liquidity when examined on a trading volume basis. However, when liquidity was instead measured via bid–ask spread, they displayed the lowest liquidity. These differing results are surprising as given a normally functioning trading market, both factors should indicate a similar level of liquidity.

One motivation for claiming large trading volume is that it implies a better environment for trading. Exchanges with larger trading volume should have smaller bid–ask spreads and more depth in the order book; a favourable environment for traders. Large volumes also act as a statement of trust in a certain exchange – something that is important in a market which has historically had a bad record of exchange closures and hacks. To the average trader, all of these characteristics are important and, as a result, may influence their decision on who they trade with. Finally, large volumes and high market share may be important factors when a particular exchange is seeking funding from investors.

Of the overarching motivations for manipulation detailed in Section 1.9, a combination of exchange standards and sophistication (1.9.4) and a lack of consistent regulation (1.9.1) made this manipulation possible. Throughout the period it was alleged to have been undertaken, there was little regulation/regulatory guidance preventing it from happening. It is likely that once one exchange started doing it, other exchanges followed so as not to lose their share of perceived market volume.

There are a variety of ways in which trading volume could have been inflated. These include:

- **Zero trading fees:** A trading fee is one which an exchange charges to execute a market or limit order on their platform. Starting in September 2013, many Chinese exchanges announced the introduction of zero fee trading. Whereas the announcement originally came from one exchange, others followed to ensure they remained competitive. Star Xu, CEO of OKCoin, acknowledged that zero fee trading distorts trading volume by a ‘large multiplier, maybe 5 times, maybe 10’. Note that trading exchange transactions are different from blockchain transactions, which do have to pay a fee.

- **Incentivizing large trading volume:** Although many of these exchanges had zero fee trading, exchanges charged certain fees for withdrawals. Tiered withdrawal fee systems were used, charging users less the more trading they had conducted. As such, this incentivized traders to increase their trading volume.

---

18 Bid–ask (buy–sell) spread is the amount by which the lowest sell order exceeds the highest buy order.
19 Order book depth provides an indication of the liquidity and depth for that security or currency. The higher the number of buy and sell orders at each price, the higher the depth of the market.
• **Wash trading:** In the pursuit of inflating their own trading volume without taking on the risk of price changes, an individual trader could decide to set up two separate accounts, and by carefully placing orders, trade against themselves repeatedly. Zero fee trading enables this to occur with no loss of funds. This would inflate their own traded volumes, allowing for better withdrawal fees and, as a result, inflate the overall volumes of the exchange. Periods of high trading volume have been observed without considerable changes in the price, a potential indication of wash trading.\(^{21}\)

• **Margin trading:** Many exchanges offer leveraged trading enabling users to trade in volumes 10 or 20 times their base capital.\(^{22}\) Some exchanges are alleged to have offered naked short selling, whereby bitcoins could be short-sold without borrowing them in the first place.\(^{23}\) This effectively allows bitcoins to be created from nothing.

As well as structuring their exchanges in a way that may encourage users to trade more, there are also allegations that exchanges were pursuing their own methods to further inflate trading volume. Bobby Lee, CEO of BTC-China, states: ‘We’ve known for a while that other Chinese bitcoin exchanges have been faking data. We’ve seen our trading volumes drop off heavily while others have, supposedly, witnessed massive surges.’\(^{24}\) The former OKCoin CTO, Changpeng Zhao, alleged that OKCoin ‘artificially inflates its volume through the use of bots that engage in self-trading’.\(^{25}\)

### 1.11.1 Case Study: January 2017 and PBoC Involvement

On 7 January 2017, news broke of interactions between the PBoC and the major Chinese exchanges. Among other things, including advising against offline marketing, and reiterating the need for KYC and AML laws, the PBoC had instructed the participating Chinese exchanges to stop inflating trading volume. By 12 January 2017, these exchanges halted margin trading. Reported trading volume (on the three major Chinese exchanges) dropped from an average of 8,382,983 bitcoins traded per day in the week before, to an average of 1,578,801 bitcoins traded per day in the week after: a decline of over 80%. On 24 January 2017, the exchanges introduced trading fees of 0.2% per transaction, preventing wash trading and strategies employed by users to inflate their personal trading volume.\(^{26}\) Their reported trading volume dropped from an average of 1,096,092 bitcoins traded per day in the week before, to an average of 48,617 bitcoins traded per day in the week after; a further decline of over 95%, (of the remaining 20% volume).

Figure 1.6 shows that, by February 2017, the three major Chinese exchanges’ joint trading volume was 0.5% of what had been reported in December 2016 and accounted for 32.2% of global trading volume.\(^{27}\) While a dramatic decline in trading volume is observed, it should be noted that the PBoC’s activity would

---

21 Coindesk, (13 Jan 2017), China’s Bitcoin Exchanges Quietly Made Policy Updates Overnight, see http://bit.ly/2nX5m9
22 Leveraging a position involves putting down collateral, known as a margin, to take on a position that is larger in value. For example, if the maximum leverage on a BTC-USD currency pair was 100:1, for each $1 of margin posted, you could trade the equivalent of $100 of BTC. As such, trading on leverage magnifies potential gains or losses from price movements.
23 Naked short selling is short selling a financial instrument without first borrowing the instrument, or ensuring it can be borrowed, as conventionally done in a short sale repurchase (repo) agreement.
26 Steemit, (22 Jan 2017), OKCoin, Huobi & BTCC will start charging trading fees from 24 January, see http://bit.ly/2BY9ZkP.
27 Based on data obtained from Bitcoinit, see: https://data.bitcoinity.org/markets/volume/5y?c=e&r=day&l=b.
also have dampened many traders’ enthusiasm about trading cryptocurrencies, causing many to decide to rein back their trading activities while uncertainty was still present.

**FIGURE 1.6 GLOBAL BITCOIN TRADING VOLUME.**

![Graph showing global bitcoin trading volume](image)

1.12 EXCHANGE DDoS ATTACKS

A Distributed Denial-of-Service attack (DDoS) is an attempt by an attacker to overwhelm a network target with a large volume of incoming messages (network traffic). To the victim, a DDoS attack will appear to originate from numerous separate sources. However, these sources are a linked collection of ‘zombie computers’, known as a Botnet, which is remotely controlled by an underlying attacker (Gregory, 2014). DDoS attacks are illegal and intended to disrupt the normal functionality of the target and prevent normal legitimate usage (Loukas and Oke, 2009). Often, the individual zombies, or Bots, are malware-infected machines whose owners are completely unaware of their participation in an attack. Typical targets of DDoS attacks include the servers of e-commerce websites, news websites, banks, and government websites.

Timed DDoS attacks can be launched on trading exchange servers in combination with specific trading activity to create a price manipulation strategy which, if successful, can be both quick and extremely lucrative (Feder, et al., 2016). Essentially, the approach is to disrupt normal market trading, preventing other market participants from submitting buy or sell orders, and creating an unfair advantage for the perpetrator.

The general form of the strategy deployed in cryptocurrency markets can be split into three steps:

1. **Initial sell order**: A large sell market order is placed on the exchange by the attacker just as the DDoS commences.
2. **Sustained DDoS attack**: The attacker initiates the DDoS attack preventing others from engaging in new trading. The large order to sell at the market price is filled with existing bid volume in the order book which creates downward pressure on that exchange’s market price as the buy volume is reduced. As no new buy orders arrive, the price continues to drop to fill the large sell order. This creates a cascading effect as stop-losses positions begin to trigger, causing a further downward price spiral.

3. **Position accumulation**: The attacker stops the DDoS attack and buys a large position for a favourable (low) price.

Relative anonymity (8.2.2) is a key factor enabling these attacks. It is unlikely the true identity of the perpetrator of a DDoS attack will be discovered. Exchange standards and sophistication (8.2.4) may also play a part as the infrastructure of unprepared exchanges may not be able to mitigate an attack. It should be noted some exchanges use DDoS protection services. As the attacks require some technical understanding, low barriers to entry do not apply in this case. Furthermore, as the attacks require participation in an activity that is already well known to be illegal, the lack of consistent regulation of cryptocurrency markets is unlikely to be a contributory factor.

Historically, DDoS attacks have been launched on a wide range of services in the cryptocurrency ecosystem. Examples include cryptocurrency-based gambling sites and mining pools (Vasek, et al., 2014). However, previous studies in the literature have shown that exchanges have been targeted by DDoS attacks far more than on any other cryptocurrency service, especially in recent years.

DDoS attacks are usually reported on an exchange’s Twitter feed, as this is one of the few ways to learn, from an external perspective, whether a DDoS incident has occurred. Scraping of the historical tweets of the current largest 30 cryptocurrency exchanges, (by bitcoin traded volume; ranked by coinmarketcap.com), shows that these DDoS-related attacks remain a problem. Figure 1.7 shows the increase of tweets reporting DDoS-related incidents. We built a timeline of each exchange’s tweet history which included the word ‘DDoS’ and then manually selected those referring to an attempted attack.

**FIGURE 1.7 TWITTER REPORTED DDoS INCIDENTS ACROSS THE 30 LARGEST GLOBAL CRYPTOCURRENCY EXCHANGES.**

There are several studies in the literature examining cryptocurrency exchange DDoS attacks. Most existing work focuses on DDoS attacks of the now-defunct Mt. Gox exchange, since, shortly after filing for bankruptcy in early 2014, a detailed trade history of transactions was made public.

28 Data taken from coinmarketcap.com on 20 November 2017.
Vasek, et al., 2014, examine the prevalence and impact of DDoS attacks on various cryptocurrency services, such as exchanges, mining pools, and online wallets. Using social-media/forum posts mentioning DDoS attacks between May 2011–Oct 2013, (142 DDoS attacks on 40 Bitcoin services in total), they found that cryptocurrency exchanges were the most targeted cryptocurrency service, (41% of all occurrences). In further examinations of Mt. Gox DDoS attacks, it has been observed that several attacks follow shortly after a fall from a new peak in an exchange rate, which is ‘consistent with the modus operandi of blocking exchanges in order to slow down a panicked sell-off’ (Vasek, et al., 2014). In the (slight) majority of cases, a decrease in transaction volume in the week following a DDoS, compared to the week prior, is observed.

(Feder, et al., 2016) used Mt. Gox leaked trading data spanning Apr 2011–Nov 2013, in combination with online sources reporting DDoS attacks at the time, to compare the impact of DDoS attacks against other types of shocks such as self-inflicted technical outages and pressure from regulators.29 They found evidence that DDoS attacks had more serious effects than other types of shocks. In days following a DDoS attack, the skewness and kurtosis of trading volume fell by 56% and 28% respectively.30 In other words, the distribution of daily transaction volume shifts, so that fewer extremely large transactions take place after shocks occur.

### 1.12.1 Case Study

To illustrate the disruptive effect of DDoS attacks, we examine an attack, occurring on 7 May 2017, which targeted a well-known cryptocurrency exchange called Kraken. The attack had a dramatic effect on the liquidity and traded price of ether: the (average) traded price of ETH/USD fell from $88.7 to $45.8 within an hour, a 47% drop before the event was reported publicly by Kraken. The attack was confirmed by their Twitter feed which reported the incident at 22:57 (UTC): ‘Site under heavy DDoS. We are working to mitigate the attack.’

Figure 1.8 shows the average traded price and total traded volume of ETH/USD aggregated to 10-minute windows.

**FIGURE 1.8 KRAKEN DDoS EVENT – ETH/USD TRADE PRICE PLOTTED WITH ACCOMPANYING VOLUME. PRIOR TO THE DDoS ANNOUNCEMENT BY KRAKEN, THERE IS A SPIKE IN TRADE VOLUME AND A SHARP CRASH IN THE ETH/USD PRICE.**

---

29 bitcointalk.org, Reddit's bitcoin sub-forum and public announcements by Mt. Gox.
30 Skewness is a measure of a distribution's lack of symmetry (where 0 represents a perfect symmetry). Kurtosis is the degree of excess peakedness of a distribution, where a positive number represents the excess from Gaussian.
While it is difficult to truly know the motivation for such a DDoS attack, analysis of the price impact, as shown in Figure 1.9, on different traded currency pairs on Kraken before, during, and after the DDoS attack, appears to link suspicious trading activity to the ETH/USD pair in particular. Bitcoin-based pairs were almost unaffected during the attack and other non-USD based ether pairs moved in a more reactive and lagged manner.

**FIGURE 1.9 KRAKEN PRICE IMPACT DURING THE DDoS EVENT. ETH KRAKEN TRADED PAIRS ARE AFFECTED BY A DRAMATIC DROP IN PRICE, WHEREAS BTC PAIRS SHOW A MUCH SMALLER REACTION AND QUICKLY RETURN TO PRE-DDoS LEVELS.**

![Graph showing price impact during DDoS event](image)

### 1.13 Hacks and Exploitations

The types of manipulation we now consider are hacks of cryptocurrency exchanges and exploitations of both smart contracts and cryptocurrency protocols themselves. It should be noted that we have been careful in certain areas of this section to use the term _exploit_ rather than _hack_. We use exploitation to refer to taking advantage of unintended design flaws in a smart contract or cryptocurrency protocol, and hacks more generally as gaining unauthorized access to a private system or network. The reason for this separation of terms is as follows. Smart contracts are meant to outline their terms within their code completely. The question then arises, does executing a smart contract in a format allowed by its code, but unintended by its original author, constitute hacking? This is a point of much debate and is the motivation for us to refer to exploitation rather than hacking in these cases.

In this section, we cover three different targets of hacks and exploitations – exchanges, smart contracts, and protocols – providing examples of historical occurrences in each case. It should also be mentioned that, although DDoS attacks, (see section 1.12), are potentially important components of a hack, we exclude DDoS attacks since, by their nature, they do not involve a compromise of security – their aim is to slow or disrupt a target exchange rather than gain access to user wallets.

#### 1.13.1 Exchange Hacks

The 2017 surge in cryptocurrencies prices has made exchanges popular targets for criminals since they handle and store large amount of cryptocurrency (Hileman and Rauchs, 2017). In general, cyber hacks present a considerable risk for exchanges, highlighted by the fact that in 2013 it was found that 45% of...
Almost all cryptocurrency exchanges require users to transfer their cryptocurrency into the exchange’s ownership before the user can trade them through their exchange account. To do this, the cryptocurrencies are transferred to the exchange’s blockchain wallet by the user. Therefore, exchanges are tasked with protecting large amounts of cryptocurrency owned by their users. As large amounts are being stored in one location, this makes exchanges highly lucrative targets for hackers.

If an attacker can find some way to take control of an exchange’s servers, or any other valid approach, they may be able to transfer the cryptocurrencies owned by users of that exchange into their ownership. In some cases, withdrawal may not be a viable option, but attackers can still profit by, prior to the attack, accumulating a large quantity of a specific cryptocurrency that has low trade volume and a small order book. The attackers then use compromised accounts to submit large numbers of buy orders at an unreasonably high price (e.g. 10,000x the last traded price) and make a huge profit by matching these orders with their own sell orders using the cryptocurrency they previously purchased at a much cheaper price.

Historically, cryptocurrency exchange hacks have been allowed to occur for numerous reasons which include incompetence/naivety, inside jobs, or purely because of the sophistication of the attack (some speculate that some attacks are being carried out by government-backed operations). In Table 1.1, we examine the 6 largest exchange hacks which have occurred in the short history of cryptocurrency. The size of each attack is assessed by calculating the USD-equivalent value of the stolen tokens at the prevailing market rate at the time of the attack.

### TABLE 1.1 LARGEST REPORTED CRYPTOCURRENCY EXCHANGE HACKS SINCE 2011.

<table>
<thead>
<tr>
<th>Rank</th>
<th>Exchange</th>
<th>Date</th>
<th>Approx. Amount Stolen</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Coincheck</td>
<td>Jan 2018</td>
<td>~$500 Million</td>
</tr>
<tr>
<td>2</td>
<td>Mt. Gox</td>
<td>Feb 2014</td>
<td>~$460 Million</td>
</tr>
<tr>
<td>3</td>
<td>BitGrail</td>
<td>Feb 2018</td>
<td>~$187 Million</td>
</tr>
<tr>
<td>4</td>
<td>Bitfinex</td>
<td>Aug 2016</td>
<td>~$77 Million</td>
</tr>
<tr>
<td>5</td>
<td>Zaif</td>
<td>Sep 2018</td>
<td>~$60 Million</td>
</tr>
<tr>
<td>6</td>
<td>NiceHash</td>
<td>Dec 2017</td>
<td>~$60 Million</td>
</tr>
</tbody>
</table>

32 Often, exchanges enforce higher security controls (e.g. two-factor authentication, IP whitelisting, email confirmation), or size limits on withdrawals. By default, API keys, which allow users to trade programmatically with funds/tokens from their account, do not have withdrawal permission enabled. This can mean that in many cases, even if a user’s account is compromised, withdrawal is not possible.


34 Cointelegraph, (23rd Aug 2018), Kaspersky Lab: North Korea Hacks Cryptocurrency Exchange With ‘First’ macOS Malware, see https://bit.ly/2Jf0sGL.
To date, the largest reported cryptocurrency exchange hack occurred in January 2018 when nearly $500M of NEM coins were stolen from the exchange Coincheck. It is not known how the attack was accomplished. Coincheck claimed it was not an inside job but admitted that its own sloppy security practices were to blame for the breach.³⁵ Rather than storing its customers’ assets in offline wallets, the assets were stored in hot wallets that were connected to the internet. Coincheck also reportedly failed to protect the wallets with standard multi-signature security protocols.

Interestingly, because blockchain transactions for NEM are all public, Coincheck were able to identify and publish the 11 wallet addresses where all the 523 million stolen coins ended up. All the funds seem to have been funnelled through one address which can be viewed within the NEM block explorer.³⁶ Since the attack, 6 of the 11 wallets have begun moving small amounts (between 1 and 10,000 NEM) and the other 5 moving larger amounts (300,000 to 20 million NEM). In response to the attack, the NEM development team created a new tagging system designed to alert crypto exchanges when an account has been tagged for stolen funds, thus making it difficult for the hacker(s) to convert them into other cryptocurrencies or fiat.³⁷

One of the highest profile hacks within the cryptocurrency ecosystem remains that of the exchange Mt. Gox, which at the time handled the majority of global bitcoin trading volume. The hack culminated in Mt. Gox’s collapse in 2014, with a total of over 600,000 bitcoins being stolen (valued then at ~$460 million). From subsequently released Mt. Gox logs it appears that, starting in 2011, the number of bitcoins Mt. Gox thought they held was overstated; it is believed a hacker was slowly syphoning off bitcoins over this period. It is still not known how the hacker was able to access the bitcoins.

In (Gandal, et al., 2018), researchers claim to have discovered suspicious trading activity occurring between February and November 2013 on Mt. Gox. The activity was deemed suspicious due to irregularities in how the trades were logged in the Mt. Gox database when compared to other trading activity. This activity had a significant impact on the bitcoin price. The price rose on 80% of days where suspicious activity was detected. In comparison, it only rose on 55% of days where suspicious activity was not detected. The authors believed that this activity was the cause of the price rise experienced by bitcoin during this time – a period where bitcoin experienced what many describe as a price bubble going from $150 to above $1000 in two months. The subsequent price decline seen in 2014 – described as the bubble bursting – was likely to have been caused by the uncertainty surrounding the collapse of Mt. Gox. The motivation of this suspicious trading activity is not known and not necessarily the work of a hacker. It has been speculated that this activity was conducted by someone internal to Mt. Gox attempting to recover funds previously lost to a hacker.

Recently, a Russian national was arrested on suspicion of laundering a considerable number of bitcoins. The bitcoins appear to be sourced from a number of different exchange thefts that occurred over the period 2011–2014, including a previous Mt. Gox hack. It should be noted the person arrested was the alleged

³⁵ Fortune, (31st Jan 2018), How to steal $500 Million in Cryptocurrency, see https://bit.ly/2O5h0C3.
³⁶ The wallet address is NC4C6PSUW5CLTDTSXAGJDQJGZNESKFK5MCN77OG and can be viewed at http://explorer.nemchina.com/#/s_account?account=NC4C6PSUW5CLTDTSXAGJDQJGZNESKFK5MCN77OG.
money launderer and not the original hacker. Interested readers can find an information visualization of how bitcoins linked with particular attacks have since moved around the Bitcoin ecosystem online.\(^{38}\)

The Italian exchange BitGrail was hacked in early February 2018, with an alleged 17 million Nano tokens stolen, representing approximately $187 million in value at the time. There remains some confusion over the attack and whether the blame lies with BitGrail funder Francesco Firano, the Nano development team or the hackers.\(^{39}\) Nano blockchain data appear to indicate that the hackers may have initiated the unauthorized attack weeks before it was reported as a hack, which prompted some accusations of an inside job.\(^{40}\) However, these accusations prompted Firano to respond by claiming the timestamps of the transactions on the NEM blockchain explorer are inaccurate: ‘they [the public] don’t have the complete data (it is only available to us and law enforcement authorities). And secondly, we cannot rely on the official explorer developed and managed by the Nano dev (proved flawed), which is, to this day, the only way to determine the date of the transactions.’

In August of 2016, the cryptocurrency exchange Bitfinex reported a loss of over $77 million dollars’ worth of bitcoin. An initial investigation by the exchange failed to reveal the cause of the alleged hack. Then, in October of the same year, the FBI began an investigation after a Bitfinex user reported that over a million dollars’ worth of bitcoin was removed from his account during the attack. Despite the FBI’s involvement, no further information has been revealed to the press to date.\(^{42}\) However, more questions around Bitfinex arose in June 2018, when researchers at University of Texas discovered that entities associated with Bitfinex or traders with Bitfinex accounts may have artificially ballooned the price of bitcoin to record-breaking heights in 2017 (Griffin and Shams, 2018).

In September 2018, Japanese exchange Zaif (operated by the Tech Bureau) was hacked resulting in a reported loss of 6.7 billion yen (~$60 million). The security breach was first noticed at around 17:00 on 14 September 2018, upon which time the firm suspended asset withdrawals and deposits. Hackers had gained access to the exchange’s hot wallets, even after the Financial Services Agency (FSA) had issued a business improvement order in March 2018 focused on anti-money laundering and security. An investigation found that 5,966 bitcoins had been taken, together with Bitcoin cash and MonaCoin, although the exact number stolen of the latter two coins is unknown. The scale of this hack was around 3x larger than Zaif’s own asset reserve, forcing the exchange to look for bailout options. A listed Japanese firm named Fisco agreed to invest $44.5 million for a major share of Zaif.\(^{43}\)

Slovenian-based cryptocurrency mining pool NiceHash, which also functions as a marketplace, was hacked on the 6 December 2017 for ~4,700 bitcoin. It was revealed an employee’s computer was compromised, allowing the hackers to access the NiceHash marketplace. Bitcoin was then siphoned off from the firm’s account and directed to another wallet address where the hackers subsequently emptied all funds from that wallet as of 23 December 2017.\(^{44}\) NiceHash had promised users that their funds would

---

39 Investopedia, (6 July 2018), The Largest Cryptocurrency Hacks So Far This Year, see: https://bit.ly/2SkEq9H.
44 This target wallet address can be viewed at: www.blockchain.com/btc/address/1EnJHhq8Jq8vDuZA5ahVh6H4f6jh1mB4rq.
be reimbursed, with payments occurring on a monthly basis. According to local media, as of 15 October 2018, the firm has paid back ~60% of the losses, less than a year on since the attack occurred.45

Exchange hacks are very detrimental for the cryptocurrency ecosystem, especially given the systemic importance of exchanges. As well as generating wide-reaching news articles, hacks can have considerable indirect effects on cryptocurrency markets; not only are individual victims affected by having their funds stolen, news of a hack can cause market prices to plunge. Depending on the scale of an individual attack, the impact can spread to the entire cryptocurrency market via contagion with uncertainty and fear driving prices down.

Figure 1.10 gives a visual representation of the most notable exchange hacks since 2011. The size of each bubble in the plot indicates the amount stolen, and its position on the y-axis measures the subsequent 5-day change in market price (in percentage terms).

**FIGURE 1.10 HISTORICAL TIMELINE OF NOTABLE EXCHANGE HACKS. THE SIZE OF EACH BUBBLE INDICATES THE (USD-EQUIVALENT) AMOUNT STOLEN. THE POSITION ON THE Y-AXIS INDICATES THE APPROXIMATE CHANGE IN THE GLOBAL BTC/USD PRICE.**46

![Image of Figure 1.10](image)

1.13.2 Smart Contract Exploits

Traditional legal contracts, which may outline the terms of a specific agreement, are usually enforceable by law. Smart contracts, on the other hand, are agreements written in code and enforced by the ecosystem in which they run. Interested parties can interact with a smart contract – hosted on a particular blockchain – by executing predefined functions for that smart contract.

46 The day of each hack was taken, where possible, as the first public report of the incident – either by the exchange itself or a notable cryptocurrency news site such as coindesk.com. Daily data for the global BTC/USD price was obtained from https://www.coindesk.com/price/.
Creation of verifiably secure smart contracts poses a number of challenges, which potentially opens such contracts up to exploitation. Firstly, in an attempt to be transparent, smart contract writers are encouraged to publish human readable versions of their code. This allows anyone to view its intentions (you may want to see what a software plans to do with your money before you send it). However, it also allows those attempting to use the software for nefarious purposes to search for vulnerabilities. Secondly, once a smart contract has been deployed and it has started to be used, it cannot easily be changed because it is embedded within the blockchain. Finally, although there are attempts to outline good practices, there are limited guidelines for what makes good smart contract code.47

An example of such an exploit involves some of the earliest software built on the Ethereum ecosystem, viz. the Decentralized Autonomous Organization (DAO). The DAO was intended to be a decentralized (i.e. crowd-run) venture capital fund. To be properly decentralized, with no one party in control, actions the DAO could take were written in its programming code. It was intended that participants would vote to take certain actions allowed by the code – e.g. potentially allocating funds to different projects vying for funding.

The DAO received funds (intended for later allocation) through one of the earliest token sales on the Ethereum ecosystem. Funds were sent to the system by those wishing to participate, and in return, they received a share of anticipated profits and the ability to vote on decisions. The software stored the funds that it had received. By the time that the funding phase ended on 28 May, approximately 12 million ether, (valued then in total at approximately $150,000,000), was contributed by over 10,000 participating Ethereum addresses.48

Before any funding could be allocated, an attack managed to drain considerable funds, preventing further progress of the project. On Friday, 17 June, the first public report of the attack appeared as a post by a concerned user on Reddit.49 An attacker, using a known but yet to be fixed vulnerability in the DAO’s code, was slowly draining funds from the DAO. Approximately 3.6 million ether were stolen by the attacker, which was around 1/3 of the total amount held by the DAO. The market price of ether reacted quickly to news of the attack, dropping from $20 to $13. Those selling were worried the vulnerability demonstrated the potential insecurity of the Ethereum network. Furthermore, if the ether taken in the attack were to be sold, it would undoubtedly reduce the price significantly.

Luckily (for those who had funds in the DAO) as an unintended consequence of how the DAO was designed, the stolen funds could not be accessed by the attacker for 28 days. This gave the development team and community a chance to attempt to make changes to retrieve the stolen funds. After much debate, a hard fork was introduced to the Ethereum network which returned the funds stolen to an account accessible to original DAO investors; meaning they could claim back their original investment. A by-product of this change resulted in a version of the Ethereum blockchain called ‘Ethereum Classic’ which did not have this change implemented.

Over a year after the DAO exploit, the SEC published a report on whether the DAO – given its design – violated federal securities law. They ultimately determined not to pursue action against the creators

48 The cryptocurrency is actually termed ether and the blockchain is termed Ethereum, however Ethereum is sometimes used to describe both protocol and cryptocurrency.
49 Reddit, (17 Jun 2016), I think The DAO is getting drained right now, Ethereum, see https://bit.ly/2D8fZrX.
of the DAO, but used the report to reiterate the need for compliance with suitable laws, stating ‘the automation of certain functions through this technology, “smart contracts”, or computer code does not remove conduct from the purview of the U.S federal securities law’.\textsuperscript{50} Those interested in further details on the DAO, how it was attacked and the resulting conflict of beliefs in the community are encouraged to read Mehar, et al., 2017.

1.13.3 Protocol Exploitation

The last type of exploit we examine is known as protocol exploitation. Protocol refers to the underlying rules of a cryptocurrency’s software which govern its processes. A protocol exploit is possible when an exploitable attack vector is found in the mechanism by which a particular cryptocurrency operates.

One famous and early example of a protocol exploit is the Bitcoin protocol attack of August 2010, which worked by finding and exploiting an integer overflow bug which could not detect when a Bitcoin transaction output summed to over 184 billion bitcoins.\textsuperscript{51} The bug meant that the Bitcoin network assumed there was only a very small amount of bitcoin in the transaction, and so accepted it (as part of block #74638). Fortunately, the issue was noticed and discussed publicly, and within hours a fix was deployed which, upon acceptance, saw the transaction removed from the future version of the blockchain. More detail can be found in a bitcointalk.org thread.\textsuperscript{52}

1.14 FLASH CRASHES

This section investigates flash crashes and their link to market manipulation and fraud. We provide examples of historical flash crashes and focus on a detailed investigation of the Ethereum flash crash of 21 June 2017 on the cryptocurrency exchange GDAX.

A flash crash can be defined as an extreme price fluctuation on the minute/subminute time scale – that is, a very large negative price movement followed almost immediately by an equally large price recovery. Cryptocurrency markets exhibit large daily volatility on a regular basis, underpinned by an immature infrastructure and frequent speculation. For this reason, large positive or negative returns are more common in cryptocurrency markets than traditional markets.

To ensure a fair comparison of flash crashes (extreme events) across different assets with vastly differing volatility dynamics, we impose a restriction to be considered where the price fluctuation must have breached three standard deviations from the mean, (i.e. the three-sigma rule). The definition of a flash crash should therefore depend on which market is being analysed and consider the following characteristics:

- The duration of the flash crash.
- The relative deviation from the mean return.
- The market’s role in the wider economy (conventional or digital).

\textsuperscript{51} In computer programming, an integer overflow occurs when an arithmetic operation attempts to create a numeric value that is outside of the range that can be represented with a given number of bits – either larger than the maximum or lower than the minimum representable value.
\textsuperscript{52} Bitcointalk (15 Aug 2010), Strange block 74638, see https://bit.ly/2O6NrA9.
To help contextualize market differences, we visualize the daily returns of each asset as listed in Figure 1.11 to demonstrate the differences between traditional and digital assets. The chart shows ether has much fatter tails, and often shows movements of a magnitude which are considered as flash crashes in traditional markets, than the DJIA or Gold Futures, thus justifying the need to contextualize the severity of a flash crash event on a market-by-market basis.

**FIGURE 1.11 A COMPARISON OF DAILY RETURNS FROM ETH/USD, THE DOW JONES INDUSTRIAL AVERAGE AND COMEX GOLD FUTURES. ETHEREUM HAS MUCH FATTER TAILS (I.E. A HIGHER STANDARD DEVIATION) THAN THE DJIA OR COMEX MEANING THE SEVERITY OF A MARKET MOVEMENT NEEDS TO BE MUCH LARGER IN MAGNITUDE TO JUSTIFY THE TERM ‘FLASH CRASH’.

Most academic work surrounding flash crashes has focused on the 6 May 2010 crash on the DJIA. This is due to its importance in the world economy as it briefly wiped over $1 trillion in value from the US economy, affecting global firms from pension funds to state-owned businesses.

There is much debate on the exact cause of the 6 May 2010 flash crash. Kirilenko, et al., (2011) examined trade data at the time of the event and ruled out the role of High Frequency Trading (HFT) in causing the crash, given HFT trading patterns did not change either before or during the crash. Madhavan (2011) suggest that the fragmentation of markets over several different exchanges creates a thinning effect of the limit order book and so makes liquidity shocks more prominent. Increased occurrences of liquidity shocks in turn increase the likelihood of flash crashes.

Traders who use market orders to fill their trades are liquidity takers and referred to as ‘informed’ as they are assumed to know something about the impending direction of the market, as this form of trading means you want to buy/sell immediately at the best ask/bid, (see Section 1.15 for more details on trading the limit order book). The order flow of informed traders is often called ‘toxic flow’ and in the literature, measures of order book toxicity have been explored as a leading indicator of flash crashes.53

Easley, et al., (1996) build a model around the concept of informed and uninformed traders by modelling their activity as an information arrival process. They propose a metric termed the Probability of Informed Trading (PIN), which is formulated as the ratio of orders occurring from informed traders against the total order flow.

---

53 Toxic to the uninformed trader (i.e. the market maker who places orders with limit orders).
This concept is taken further by Easley, et al., (1996), who create an adaptive metric that is supposedly more useful and not as difficult to estimate, called Volume Synchronized Probability of Informed Trading (VPIN), which is a common proxy of order book toxicity. An important part of VPIN is that the measure is calculated in volume time rather than trade time, meaning VPIN is linked to the time it takes to fill a set volume quantity. Easley et al. suggest that it is intuitive to compare periods of equal volume, (or information content in this context), which addresses trade frequency clustering, having the effect of smoothing out information bursts. Aslan, et al., (2011) suggest that VPIN is an effective leading volatility indicator and demonstrate this with analysis of the 6 May 2010 DJIA flash crash. However, Jonathan Heusser applied the technique to the 2013 bitcoin crash and found it to yield weaker results, (although the parameters were not optimized), leaving open the question: Is toxicity a useful factor in analysing cryptocurrency markets?54

In traditional markets, flash crashes may be induced by fraud and manipulation techniques such as spoofing, (see Section 1.15: order book based manipulations), as was the case in DJIA 2010.55 However, aside from spoofing, market participants in cryptocurrency markets can, potentially, place very large market orders which may consume the order book and trigger stop-loss orders and margin calls. This will deepen the sell-off, possibly setting off a free-fall in prices. Once the price has fallen by an appropriate level the manipulators buy back into the market and, having sold high and bought at a lower price, they can profit from the manipulation. This form of manipulation can be accomplished in cryptocurrency markets more easily than it can in traditional markets, due to the large skew of ownership towards early adopters, (e.g. 1000 people own 40% of bitcoin, where they can organize between themselves a coordinated trade), or simply high-net-worth individuals, (as the market cap of cryptocurrencies was relatively low at the time).56

Some theories as to the real motive behind the Ethereum flash crash of 2017 on GDAX revolve around a fat-fingered (errored) trade which had nothing to do with market manipulation, whereas others propose that someone deliberately placed a large market order intended to put pressure on an already fragile cryptocurrency market.57 It is still an open question as to whether the crash was a malicious attack or simply a mistake. Detailed literature focusing on flash crashes in cryptocurrency is all but non-existent; however, in general, flash crashes are caused by fragmented markets, low liquidity and a rapid increase in sell-side volume, which are all factors often present in cryptocurrency markets.

Many flash crashes have been observed in conventional markets in the past – most notably on 6 May 2010 when a $4.1 billion trade was placed on the New York Stock Exchange (NYSE) which resulted in the Dow Jones Industrial Average (DJIA) losing ~1000 points and then recovering within the space of 15 minutes. Other markets such as the S&P500 and Nasdaq also experienced similar price volatility as a result.

The 2010 flash crash on the E-mini S&P 500 futures contract was traced back to Navinder Singh Sarao, a trader who had used spoofing algorithms to modify $200 million worth of trades, approximately 19,000 times, moments before the flash crash.

55 FT (10 Nov 2016) ‘Flash crash’ trader Navinder Sarao pleads guilty to spoofing.
There are many more examples of crashes in the cryptocurrency markets such as 10 April 2013 bitcoin crash, when a large trade volume lag at the Mt. Gox exchange sent the market plummeting over 60% within the day.\(^{58}\) However, this cannot be defined as a flash crash as the event occurred over a number of hours, which does not constitute a ‘very rapid’ decline in price within the scope of cryptocurrency markets. Table 1.2 summarizes the most notable recent flash crashes.

### TABLE 1.2 RECENT NOTABLE FLASH CRASHES.

<table>
<thead>
<tr>
<th>Date</th>
<th>Market</th>
<th>Peak-to-Trough (Magnitude)</th>
<th>Peak-to-Trough (Duration)</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 May 2010</td>
<td>DJIA</td>
<td>9%</td>
<td>~4 minutes</td>
<td>Market manipulation</td>
</tr>
<tr>
<td>26 June 2017</td>
<td>Gold Futures</td>
<td>1.6%</td>
<td>~8 seconds</td>
<td>$2bn market order</td>
</tr>
<tr>
<td>22 June 2017</td>
<td>Ether</td>
<td>99.97%</td>
<td>~1.5 seconds</td>
<td>Million-dollar market order</td>
</tr>
</tbody>
</table>

It can be seen from Table 1.2 that the duration and peak-to-trough magnitude of each flash crash are very different, especially when comparing conventional markets (DJIA, Gold) to cryptocurrency markets (ether). A ‘deep’ volatile fall (as stated in the definition of a flash crash) depends on what market is encountering the event. The 1.6% move in the price of Gold Futures within 60 seconds\(^{59}\) in 2017 constitutes a contextually deep crash as this market is one of the most liquid in the world, whereas a change of 1.6% in cryptocurrency markets would not be classified as a crash but simply market noise. Crashes in cryptocurrency markets can be much deeper – for example ether’s flash crash lost 99.97% of its value within seconds of a large market sell order being placed, before the price recovered. This magnitude of movement is unheard of in conventional markets.

#### 1.14.1 GDAX-ETH/USD Flash Crash

On 21 June 2017, a $12.5 million market sell order was placed on the GDAX exchange at 12:30pm Pacific Time (PT), which triggered a flash crash on ETHUSD.\(^{60}\) This massive order, (~14.5% of the GDAX 21-day average daily volume), which accounted for 39,300 ETH, removed a large chunk of liquidity from the order book, incurring a 29.4% price move, from $317.81 to $224.48, immediately.

The movement resulted in approximately 800 stop-loss orders and margin-funding liquidations. The volume of sell orders, (from stop-loss activation and margin calls), overwhelmed the market’s available liquidity, causing further extreme downward movement. The price of ETH fell momentarily to $0.10, accounting for a 99.97% loss from trading prices seconds before.\(^{61}\)

This event occurred over a period of approximately 10 seconds where the price went from $317.81 to $0.10 and recovered back to $302. Figure 1.12 shows the price movement over the period.

---

Interestingly, we can see bids in the order book starting at 10 cents and asks at $74 in the GDAX final update on their blog. The spread quoted at $73.9 at the time of this snapshot exhibits an extreme market inefficiency which automated traders subsequently traded away, recovering the price to $302. However, it can be seen that there were approximately 24,000 ETH filled at 15 cents and under, for a total price of around $2600; if these fills were from a single user they would have made nearly $7.8 million from the flash crash.

After an investigation by GDAX, it was decided that all profitable trades during the time of the flash crash would be honoured. GDAX went a step further with an official announcement on their blog, stating:

For customers who had buy orders filled — we are honoring all executed orders and no trades will be reversed. For affected customers who had margin calls or stop loss orders executed – we are crediting you using company funds.

This unusual act restored faith in GDAX’s reputation as one of the most trusted cryptocurrency exchanges – they were not required to refund customers because no system errors were uncovered. The exchange stated their reasons for these actions were that they:

...view this as an opportunity to demonstrate our long-term commitment to our customers and belief in the future of this industry.

The total cost to GDAX because of the flash crash is still unknown.

Although the ETHUSD flash crash of 2017 has seen no legal action, its ties to a possible market manipulation are clear. Price movements of this extreme magnitude cause many to speculate whether any wrongdoing was the central cause of such an event, (e.g. the large market order was intended to crash the market), or whether the event was caused by a large trade amount being entered accidently. The reason is still unknown to this day, although the cause is well documented (as in the above case study).

---

63 Trade fills can be found through GDAX’s API and can be found at: https://api.gdax.com/products/eth-usd/trades?after=6326581&limit=18.
Conventional markets deal with unstable trading using systems such as circuit breakers, which would freeze trading should a market move by a large percentage in a very short period of time. GDAX stated that they were looking into how these measures could be integrated, although at the time of writing no action had been taken.⁶⁴

This event on GDAX clearly highlights the effectiveness of regulation in conventional markets, which suggests that, if measures proposed after the 2010 flash crash on the DJIA had been implemented on GDAX, the flash crash on ETHUSD in 2017 would probably have been avoided. However, the onus is on the leading exchanges such as GDAX to develop market-stabilization systems to prevent such an event recurring.

1.15 ORDER BOOK-BASED MANIPULATIONS

The next two approaches that we examine are based on manipulation of the order book. In a typical market, there are a wide array of participants, each with their own motivations and behaviour. ‘Quote stuffing’ and ‘Order spoofing’ are two order book manipulations, using limit orders, which are designed to provide the manipulator with an unfair advantage. Both are quite sophisticated manipulations developed from traditional financial markets and intend to distort or influence the true price of a currency pair.

1.15.1 Quote Stuffing

Quote stuffing is an algorithmic trading strategy which involves rapidly placing and cancelling limit orders. During a quote stuffing event, high quote volatility is observed over a very short period where short-lived quote updates often follow specific patterns. One variation we focus on here creates new best bid or best ask prices, which are quickly cancelled. There are a number of reasons why this form of quote stuffing may be engaged in, as outlined in Tse, et al. (2012). Quote stuffing creates a false mid-price – the mid-price is the average of the current best bid and ask prices and is often used by algorithmic traders and traditional traders in benchmarking the trade execution and market price of an asset; manipulation of the mid-price can give an impression of rising or falling prices, and may manipulate others into trading if they are looking for mid-price related signals. Furthermore, quote stuffing may generate high volumes of inconsequential market data updates, potentially slowing and confusing the responses of other competing algorithms and traders, (in a similar way to a DDoS attack slowing a website server); this is especially important for high-frequency trading, where speed is a critical factor.

It should be noted that quote stuffing has also been observed in traditional markets, as identified by Tse, et al. (2012). Exchange standards and sophistication (8.2.4) within cryptocurrency markets may be a contributory factor to quote stuffing. Many cryptocurrency exchanges may not have the analytical systems set up to catch its occurrence. Furthermore, they may not see it as a priority to do so when other manipulations have a more dramatic effect.

To illustrate the effect of quote stuffing, we examined some order book BTC/ EUR data from a prominent cryptocurrency exchange over a 10-week period in 2017. By recording real-time market updates which are broadcast publicly from their servers, we were able to reconstruct the historical state of the BTC/ EUR order book and track placed and cancelled orders. Using the approach as described in Bogoev and

Karam (2016), we identified periods of quote stuffing using the \( D\)-ratio. The \( D\)-ratio is a ratio between the start-to-end change and the sum of all incremental changes observed in a particular window of order book updates. More specifically, the in-bid \( D\)-ratio (for detecting stuffing occurring on the bid side of the order book) is defined as:

\[
D = \frac{\sum_{i=1}^{t} |B_i - B_{i-1}|}{\sum_{i=2}^{t} |A_i - A_{i-1}|}
\]

where the numerator is the absolute sum of the incremental changes in best bid price during a period considered, divided by the absolute change in best bid prices from start to end of the window. The denominator is the same, but for the ask price. Essentially, the formula measures whether there is a lot of temporary movement in best bid prices without much overall movement, compared to the ask price. Appropriate approaches exist in Bogoev and Karam (2016) to detect in-ask stuffing, and stuffing on both sides of the book, but a full description is omitted here for brevity.

In our research, we calculate the \( D\)-ratio for each time window (chosen as 10-seconds) over the entire dataset. The windows are then ordered based on their \( D\)-ratio, creating a distribution of observed \( D\)-ratios. The methodology aims to capture windows of data that contain characteristics associated with quote stuffing events: repeated and small changes in best bid or ask, which are rapidly reversed, combined with little actual change in best bid or ask between the start and end of the window. The higher the \( D\)-ratio, the higher the likelihood a specific type of quote stuffing is taking place. Unfortunately, it is difficult to define in simple terms how frequently quote stuffing occurs since a \( D\)-ratio ‘cut-off’, defining what is and is not quote stuffing is somewhat arbitrary and therefore is chosen as a percentile of the \( D\)-ratio distribution.

As such, we opt to show one example time window that exhibits a high \( D\)-ratio as an example. Figure 1.13 (a) shows an example of a 10-second window containing bid-stuffing, and (b) gives a lower-frequency (10-minute) picture surrounding the identified quote stuffing event. It is observed that fleeting orders are being placed to alter the best bid, before being cancelled almost instantaneously. The ask price during this event is relatively static.

**FIGURE 1.13 BTC/EUR (A) 10-SECOND SNAPSHOT (B) 10-MINUTE SNAPSHOT BEST BIDS.**
1.15.2 Order Spoofing

Order spoofing is another type of order book manipulation where limit orders are placed into the limit order book to deceive other market participants, such as normal traders and algorithmic trading bots, into believing that there is more demand or supply. Usually, these ‘spoof’ orders are comparatively large in quantity to create the impression of a large imbalance. However, what separates spoof orders from standard large limit orders is that the entity placing the orders intends to cancel them before they can be executed against. After a spoof order is placed, if successful, the market moves, based on its belief that the imbalance is real. This allows the entity placing the spoof order to manipulate the price; potentially to execute a trade on the opposite side of the book. Figure 1.14 gives a demonstration of the process undertaken.

FIGURE 1.14 ILLUSTRATIVE EXAMPLE OF ORDER SPOOFING PROCESS

Numerous examples occur where a large buy or sell limit order is placed, discussed on social media and then removed. Trader IDs, which would need to be supplied by the exchanges, would shed further proof that an individual event can be classified as ‘order spoofing’, and on whether the participating trader is filling orders on the other side of the book.
Existing literature investigating order spoofing occurring in any financial market is relatively sparse. However, it has been documented that many targeted financial assets have certain shared attributes, including higher return volatility, lower market capitalizations, and lower price level (Jung Lee, et al., 2013). All these attributes are common among cryptocurrencies, and those that do not have a low (unit) price level, have had this in the past. As such, the distribution of cryptocurrency ownership is skewed (Moore and Christin, 2013). Early investors have the potential to own large percentages of the total amounts available. As with quote stuffing, low exchange standards and sophistication (Section 1.9.4) may also enable this manipulation, as it may not be a priority to catch.

1.16 STABLECOINS AND TETHER

A **stablecoin** is a type of price-stable cryptocurrency whose price is pegged to an asset, such as gold or a fiat currency. The majority of existing stablecoins use some form of collateralization; however, others are emerging that use algorithms which expand or contract the issuance scheme depending on the traded price of the coin. Fiat-collateralized stablecoins require a certain amount of collateral to be deposited against which (stable)coins are issued, typically using a 1:1 ratio. Although this is a relatively straightforward currency issuance process, it requires a central party, acting as a custodian, who guarantees the issuance and redeemability of the stablecoin.

Unlike other cryptocurrencies, a stablecoin is designed to have little risk of suddenly changing in value. It is engineered explicitly not to provide any return. The idea is that if you bought $2,500 worth of stablecoins a year ago, you would have roughly $2,500 today. There is a demand for stablecoins from both exchanges and investors as they both provide an effective hedge against cryptocurrency volatility as well as facilitating dollar-like transactions without a banking connection, something many crypto-exchanges have difficulty obtaining or keeping (Griffin and Shams, 2018).

The story of stablecoin use and adoption to date is primarily one about Tether. **Tether** (denoted USDT), is currently the 8th largest crypto globally and largest stablecoin in existence. In fact, Tether accounts for more crypto transaction volume than USD. Even with the emergence of some new entrants, it still accounts for approximately 98–99% of all stablecoin trading volume.

As Tether explain on their website: “**Tether converts cash into digital currency, to anchor or ‘tether’ the value of the coin to the price of national currencies like the US dollar, the Euro, and the Yen.**” As such, the price of one USDT is pegged to $1, and so a current market capitalization of $2 billion indicates approximately 2 billion USDT tokens in circulation. This quantity can also be verified from blockchain transactions. New USDT tokens are issued from one Tether wallet address on the Omni Layer (formerly Mastercoin), a platform that enables the creation of new assets on the Bitcoin blockchain. Every Omni transaction, and therefore every Tether transaction, is recorded in a Bitcoin transaction sharing the same

---

65 For example, see https://basis.io or https://carbon.money.
69 The wallet address is 3MbYQMMmSkC3AgWkj9FMoS5LsPTW1zBTwXL, and a full history of issuances can be viewed at www.omniexplorer.info/address/3MbYQMMmSkC3AgWkj9FMoS5LsPTW1zBTwXL.
transaction hash.\textsuperscript{70} New tokens are purportedly issued upon new USD deposits and, since Tether claims to be fully-collateralized, this implies that Tether holds collateral of $2 billion in its bank accounts.

On paper, Tether proves to be an extremely successful example of a stablecoin project; however, its history has been plagued with controversy. To better understand these issues and shed light on the allegations of misconduct and suspicious activity, we first examine Tether’s history. Following this, we examine some of the criticism put forward, including new research published in June 2018, which finds evidence of Tether being used for cryptocurrency price manipulation. Finally, we highlight the important role Tether plays in cryptocurrency market prices and discuss the ramifications of hypothetical wrongdoing.

1.16.1 Tether Historical Timeline

Table 1.3 provides a summary of important events in Tether and Bitfinex’s history between 2012–2018, including key legal announcements and Tether market capitalisation milestones.

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>IFinex, the eventual parent company of Tether (and Bitfinex) is founded in Hong Kong.</td>
</tr>
<tr>
<td>2013</td>
<td>Bitfinex is incorporated. Phil Potter runs the company alongside CEO Jan Ludovicus van der Velde and CFO Giancarlo Devasini.</td>
</tr>
<tr>
<td>2014</td>
<td>Jul Realcoin is announced, built on top of Bitcoin with a protocol called Mastercoin (now called Omnicoin).</td>
</tr>
<tr>
<td></td>
<td>Sep Bitfinex operators (Potter and Devasini) set up Tether Ltd. in the British Virgin Islands but tell the public that Bitfinex and Tether are separate.</td>
</tr>
<tr>
<td></td>
<td>Nov Realcoin rebrands to Tether and announces several partners including Bitfinex.</td>
</tr>
<tr>
<td>2015</td>
<td>Feb Tether begins trading under the symbol USDT, but currency circulation remains relatively low.</td>
</tr>
<tr>
<td>2016</td>
<td>May Tether market capitalization rises to $7 million.</td>
</tr>
<tr>
<td>2017</td>
<td>Feb Tether market capitalization hits $25 million.</td>
</tr>
<tr>
<td></td>
<td>Mar Wells Fargo ends its banking relationship with Tether, issuing a statement that ‘all international wires to Tether have been blocked . . . As such, we do not expect the supply of tethers to increases substantially until these constraints have been lifted’. (continued)</td>
</tr>
</tbody>
</table>

\textsuperscript{70} Tether Whitepaper (Jun 2016) Tether: Fiat currencies on the Bitcoin blockchain, see https://bit.ly/2EIroAh.
\textsuperscript{72} Medium (22 Aug 2018) Is the Price of Bitcoin Based on Anything at All?, see https://bit.ly/2yHhcTl.
\textsuperscript{73} Amy Castor (17 Jan 2019) The curious case of Tether a complete timeline of events, see https://bit.ly/2NbOj7E.
<table>
<thead>
<tr>
<th>Month</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr</td>
<td>Tether market capitalization reaches $50 million. Bitfinex files a lawsuit against Wells Fargo for interrupting its banking transfers (eventually withdrawn in 2017). A pseudonymous character Bitfinex’ed appears online, accusing Bitfinex of creating Tether out of thin air to pay off debts.</td>
</tr>
<tr>
<td>May</td>
<td>Bitfinex and Tether hire Friedman LLP to complete an external audit.</td>
</tr>
<tr>
<td>Sep</td>
<td>Tether market capitalization expands exponentially to $440 million. Tether Ltd. publishes a memo from Friedman LLP affirming that Tether is fully backed. However, this does not constitute an official audit.</td>
</tr>
<tr>
<td>Nov</td>
<td>Bitfinex and Tether are shown to be run by the same individuals via leaked documents dubbed the ‘Paradise Papers’. Tether is hacked and 31 million USDT are moved from the Tether treasury wallet and sent to an unauthorized Bitcoin address – a hard fork is initiated to prevent those funds from being spent.</td>
</tr>
<tr>
<td>Dec</td>
<td>The Commodity Futures Trading Commission (CFTC) send subpoenas to Bitfinex and Tether, but the actual documents are not made public. (To date, no charges have been filed).</td>
</tr>
<tr>
<td>2018 Jan</td>
<td>Tether parts ways with auditor Friedman LLP, blaming the accounting firm’s overcomplicated procedures for what is a ‘relatively simple balance sheet of Tether’. Bloomberg reports on the CTFC subpoena of Tether and Bitfinex. Tether issues more than $850 million tether, more than any previous month.</td>
</tr>
<tr>
<td>Jun</td>
<td>Tether releases a report it had commissioned from law firm Freeh Sporkin and Sullivan (FFS) attesting that ‘Tether’s unencumbered assets exceed the balance of fully-backed USD Tethers in circulation as of June 1st, 2018’.</td>
</tr>
<tr>
<td>Aug</td>
<td>Tether market capitalization hits $3 billion.</td>
</tr>
<tr>
<td>Oct</td>
<td>Bitfinex temporarily suspends all cash deposits four days after reports claiming the exchange is banking at HSBC under the name ‘Global Trading Solutions’ amid Tether insolvency woes. Bitfinex publishes three wallet addresses (BTC, ETH, and EOS) to prove the exchange is still solvent. (continued)</td>
</tr>
</tbody>
</table>
Oct  Rumours claiming Tether is insolvent sees its pegging slip to $0.92, and $0.85 on Kraken.

Tether appears to be holding reserves at Bahamas’ Deltec Bank.

Tether ‘redeemed a significant amount of USDT’ and burns 500 million USDT representing these redemptions. The remaining 446 million USDT is held in treasury for ‘preparatory measures for future USDT issuances’.

Nov  Tether provides an attestation letter from Deltec confirming its banking partner and showing proof of ~$1.8 billion which fully backs Tether, although the letter has an incomprehensible signature.

Bloomberg report US federal prosecutors have ‘homed in on suspicions that a tangled web involving Bitcoin, Tether, and crypto exchange Bitfinex might have been used to illegally move process’.

Tether announces that customers can redeem USDT for USD again.

Dec  Tether has issued over 1 billion USDT in 2018.

### 1.16.2 Tether Controversy and Criticism

Key events in Tether’s history have raised concerns over its conduct. The fact that Bitfinex and Tether are run and operated by the same individuals immediately produces potential conflicts of interest: Tether and Bitfinex are issuers of a cryptocurrency on their own and other platforms, with a direct stake in its performance. A recent report commissioned by the NY Attorney General points out that running these multiple lines of business would be ‘restricted or carefully monitored in a traditional trading environment’, a safeguard which is currently not present in cryptocurrency markets.74

Many sceptics have questioned the reality of the US dollar peg and the token’s redeemability. Some other have even accused Tether of cryptocurrency price manipulation. We now examine each of these claims in turn.

There has been very little transparency provided by either Bitfinex or Tether regarding the preservation of Tether’s US dollar peg. Only days after Tether announced it had dissolved its relationship with auditors Friedman LLP in December 2017, it issued $600 million worth of tokens, raising its market capitalization by nearly half. Some, particularly in the blogosphere and press, have expressed scepticism that Bitfinex/Tether really have this kind of collateral.75,76 Nonetheless, cryptocurrency exchanges and investors have largely rejected such concerns, and widely use Tether in transactions.

The September 2017 memo from Friedman LLP and the June 2018 commissioned report of Freeh Sporkin and Sullivan (FSS) go some way in demonstrating Tether is fully collateralized, but both fall short of a full audit. For example, FSS’s report includes important caveats stating that ‘FSS makes no representation

75 See https://twitter.com/bitfinexed and https://medium.com/@bitfinexed.
regarding the sufficiency of the information provided to FSS’ and ‘FSS is not an accounting firm and did not perform the above review and confirmations using Generally Accepted Accounting Principles’.77

Some concede that the information provided in the reports may accurately confirm that Tether reserves matched that of circulating USDT on the date of examination. However, they raise different concerns regarding the way in which the funds were raised, and highlight the importance of the order of transactions. Without disclosing the order of transactions, it is theoretically possible for Tether to issue new tokens out of thin air, use these tokens to buy other cryptocurrency, sell that cryptocurrency, and used the proceeds to create its reserves. In February 2018, the blogger Bitfinex’ed illustrates a scenario where Tether first issues several million Tether to buy other cryptocurrencies on Tether-supported exchanges, transfers these to other exchanges such as GDAX, liquidates the cryptocurrency and then funnels the (now fiat), currency back to Tether-owned bank accounts. Bitfinex’ed backs up this scenario with suspicious trading activity on Bitfinex and GDAX, saying ‘when GDAX goes down, the volume on Bitfinex dries up dramatically . . . until GDAX comes back online’. They summarize: ‘[Bitfinex] Pump on Tether exchanges while simultaneously having large sell orders on GDAX/Bitstamp/Gemini and then immediately transfer the funds back to their main account’.78

Figure 1.15, constructed using Tether historical transactions recorded on the Omni Protocol, highlights the dramatically increasing rate at which new Tether was issued throughout 2017 and 2018. The figure also shows that very little Tether has ever been removed entirely. Tether are often moved to the Tether treasury wallet and kept as ‘preparatory measures for future USDT’ and thus not redeemed completely.79 In September 2018, there had only ever been one Tether redemption transaction (30 million tokens were redeemed on 31 January 2018). This means that, on a net basis, Tether should have taken in more deposits than withdrawals. This said, on 24 October, Tether did destroy 500 million USDT from the Tether treasury wallet after a growing accumulation throughout 2018.

**FIGURE 1.15 TETHER ISSUANCE PLOTTED AGAINST BTCUSD PRICE AS QUOTED ON COINMARKETCAP.COM. TETHER CAN ISSUE TOKENS BUT HOLD THEM IN A TREASURY WALLET; THESE TOKENS ARE CONSIDERED NOT IN CIRCULATION AND EXCLUDED FROM ITS MARKET CAPITALIZATION.**

---

78 Medium (8 Feb 2018), @Bitfinexed, Bitfinex and Tether is unauditable: Why they will never do a real audit, see https://bit.ly/2PkSFN9.
In December 2017, Bloomberg published an article wherein Oguz Serdar, a USDT user who relied on cryptocurrency to pay contractors, claimed that in early November he tried to cash out $1 million of Tether through Tether Ltd., but was refused and ‘instead recommended in an email that he try to sell on one of the exchange partners it lists on its website’.\(^80\) Tether defended this decision, explaining that Serdar was flagged as suspicious and that they were not permitted to do business with him until he completed their KYC process. Within Tether’s terms of service, it is stated: ‘Tether must and does at all times reserve the right to refuse to issue or redeem Tether tokens’.\(^81\)

In June 2018, John Griffin and Aman Shams published their research examining the timing of Tether purchases following market downturns. They were able to establish that entities associated with Bitfinex were successfully using Tether to purchase bitcoin when prices were falling and reverse the trend of the market. These effects were only present after negative bitcoin returns and periods following the circulation of new Tether.

They asserted that 50% of bitcoin’s and 64% of other top cryptocurrencies’ price rises were due to well-timed, heavy Tether transactions. Patterns they found in publicly available trading data supported the hypothesis that Tether is used to support and manipulate cryptocurrency prices. The authors also mention that negative end-of-month price pressure on bitcoin only during months with large Tether issuance supports a month-end need for dollar reserves related to Tether.

Without the existence of USD/BTC and other fiat-to-crypto trading pairs, the price of Tether would be an entirely self-referential process, with the price of Tether always equal to itself. As these markets do exist on banked exchanges, Tether’s global market price is expected to move away from one dollar given a change in the price of bitcoin (or any other cryptocurrency) in fiat markets, without an accompanying one in Tether markets. When Tether is consistently reported to be worth a dollar, implicitly, the price of bitcoin in Tether on unbanked exchanges is the same as the price of bitcoin in dollars on banked exchanges. However, there is no obvious mechanism for keeping the two values at parity.

Professor Rosa Abrantes-Metz finds this parity something extremely puzzling, because there is no reason for their prices to stay matched. Tether does not have a built-in (i.e. blockchain-encoded) stability mechanism and so, ‘If things trade freely, the only way to keep parity is for someone to actively intervene in the markets’, but who, or how, is unknown.\(^82\)

Generally, USD and Tether trade on different exchanges and are therefore not visibly connected. Kraken is among very few markets worldwide that let investors trade USD for Tether and vice versa. In effect, Kraken should play a large role in establishing Tether’s price.

In June 2018, Bloomberg published an investigation claiming the normal economics of supply and demand do not always appear to apply for USD/USDT. ‘Counter to basic trade economics, large and frequent trade volumes appeared to have less influence on price than small trade volumes’—a clear indicator of market manipulation.

\(^80\) Bloomberg (5 Dec 2017), There’s an $814 Million Mystery Near the Heart of the Biggest Bitcoin Exchange, see https://bit.ly/2PmkogB.
The distribution of Tether trade volumes showed an unusual pattern with the third most common Tether trade size 13,076.389 Tethers, an oddly specific number. Former Federal Reserve bank examiner Mark Williams’s theory is that this could be a sign of wash trading as the software would look for orders with a unique size and trade against that. Williams explains ‘Many of the trade amounts are frequently occurring to the fifth decimal point, a unique identifier which increases the probability it is being generated by the same person or entity’.83,84

1.16.3 Tether’s Significance in Cryptocurrency Global Markets

Tether is a systemically important part of the cryptocurrency ecosystem. The global published price of a cryptocurrency, e.g. bitcoin is generally a volume-weighted average of its price on all the markets on which it is traded. Since three times as much bitcoin trading takes place in Tether than in USD, this means that the published price is based three times as much on Tether trades as on dollar trades.

However, this volume-weighted method also applies to the quoted price of Tether itself. Just like any other coin or token, Tether’s global price is a weighted average of all the available markets by volume. Since virtually all Tether trading occurs in markets where it is traded against bitcoin and other cryptocurrencies, the only way to arrive at a dollar price is by dividing its price in cryptocurrency by the price of that cryptocurrency in dollars. Similarly, the dollar prices of most cryptocurrencies are themselves derived from trades with other cryptocurrencies, primarily Tether. ‘The price of crypto is derived largely from trades in Tether, the price of which is derived largely from trades in crypto, the price of which is derived largely from trades in Tether.’ This has large implications for cryptocurrency price discovery.85

As Wang Chu Wei, a researcher at the University of Queensland explains, ‘If Tether was in fact able to issue tokens not backed by fiat reserves then effectively, they would be printing USD in the cryptocurrency ecosystem . . . . If that was the case, Tether Limited’s role/power would not be dissimilar to that of a central bank; i.e. the ability to increase money supply and boost asset prices.’86

In a worse-case scenario where Tether collapses, the ramifications for cryptocurrencies are concerning. Before Tether tokens began flooding the market at the start of 2017, bitcoin was priced at less than $1,000. Professor Sarit Markovich, who researches cryptocurrency at Northwestern University, has stated that ‘If there’s a panic in the market, we’re going to go to the same price we had before and we’re going to see it across all cryptos.’

1.17 SUMMARY AND CONCLUSIONS

The purpose of this chapter was to provide the reader with a non-exhaustive survey of manipulations which have often occurred, or are alleged to have occurred, in cryptocurrency markets. We began with a general introduction to cryptocurrencies, the nature of their transactions, and the cryptocurrency exchanges upon which large volumes of cryptocurrency are traded. Section 1.9 then gave an idea of why manipulations are prominent in cryptocurrencies. Throughout the remainder of the chapter, we attempted to link back to these reasons. Often it is clear that one reason alone is not sufficient to motivate/facilitate

84 Wash trading involves taking both sides of a transaction for the express purpose of feeding misleading information to the market.
manipulation and we, therefore, rely on a combination of reasons to explain them. In the subsequent subsections, we surveyed a variety of manipulations ranging from social-based manipulations to more technical and complex ones.

Although the first manipulation, a pump and dump event, occurs within traditional financial markets, we focused our investigation on a cryptocurrency-adapted version. This modification involves groups on social media coordinating buying pressure for a particular cryptocurrency; we included a case study with a real example of a coordinated pump and dump event in 2017, and analysed the event’s effect on both the price and trading volume.

Next, we discussed a manipulation – inflated trading volume – allegedly employed by Chinese trading exchanges in an effort to give themselves an elevated image to different interested parties, and we saw that its eventual prevention in January 2017 caused an astonishing reduction in trading volume. The rapid series of regulatory-influenced events, which prompted such a change, emphasises that cryptocurrency markets are an extremely fast-evolving environment; opportunities to profit from different legitimate strategies come and go, as do the opportunities for manipulation. The work here has documented some of the most relevant instances of manipulation at the time of writing, but further down the line – even a year or two – numerous manipulations may or may not continue to occur; especially with increased regulatory scrutiny.

Our next two manipulations, exchange DDoS attacks and hacks, which are illegal wherever undertaken, tend to be deployed in the cryptocurrency markets rather than more traditional financial markets, due to what the manipulators deem as an unrivalled risk–return payoff: the potential return in cryptocurrency far outweighs the chance of being caught, in part because of the high level of anonymity in cryptocurrency markets.

The next manipulation, flash crashes, was the only one that may not always be intentional. Although flash crashes may be the result of manipulations such as a carefully executed DDoS attack, they can also be accidental. The fragmentation of trading across many venues and the low liquidity seen on a number of smaller exchanges, cultivates an environment where large sell orders may trigger stop losses which further propagate downwards price movement.

Section 1.15 looked at two order book-based manipulations, quote stuffing and order spoofing, which are examples of strategies which have been recorded a number of times in equities, commodities, and other more established markets, repurposed and deployed in cryptocurrency markets.

We finished our survey off with a slightly different, but important, section on the role of stablecoins, and more specifically the controversy concerning Tether, the largest stablecoin. At the time of writing, no allegation of misconduct by Tether or related parties has been substantiated. However, closer examination does highlight the importance Tether has on the cryptocurrency market in general.

After our discussion of the vast array of manipulations within cryptocurrencies, two questions may be raised:

1. What is the impact of the manipulations covered on normal cryptocurrency market participants?
2. Why does participation within cryptocurrency markets continue to grow while manipulations such as these are occurring so freely?

In addressing the impacts (1) it is best to consider each manipulation separately:

- The documented near-instantaneous pump and dump groups appear primarily to redistribute money between those actively participating. Those that buy can quickly flip the targeted asset at a mark-up to later participants in the group, who end up buying at a premium and losing out. To other market participants, the price spike may at most become a nuisance when examining, or training models on, historical data.

- The inflated trading volume was well documented and discounted by the majority of market participants who were well aware of who was engaging in it; many reporting websites refused to report on trading volumes of the culprit exchanges.

- As documented above, exchange DDoS attacks have the potential to cause large short-term price deviations. A successfully executed DDoS attack has the potential to cause stop-losses to execute at below true market prices and also cause margin traders to be forced from their positions.

- Hacks arguably have the largest potential impact of the manipulations covered. If market participants are over-invested in one exchange, (e.g. if a market participant has all their cryptocurrency stored with one trading exchange), or one particular cryptocurrency, they are at risk of losing funds through the failure of that exchange or cryptocurrency.

- Order spoofing may scare traders, (and trading bots) into making rash, wronglyinformed decisions; however, once it is understood what order spoofing is and that it occurs commonly in cryptocurrency markets, it can increasingly be ignored. Quote stuffing may only manipulate other similar trading bots, and due to the speed in which it occurs, manual traders may be completely unaware of and unaffected by the effects of it.

Although certainly not without impact, the number of participants engaging in manipulative strategies are insubstantial compared to those following legitimate short, medium, and long-term trading and investment strategies.

We now look at addressing the second question raised (2). Indeed, despite the presence of the manipulations we document here, the enthusiasm of participants to remain in the markets, and for new traders and investors to enter, has only grown in recent times. We hypothesize that this is because of the potentially meteoric returns cryptocurrency markets can offer: people are happy to overlook the potential risks of manipulations. In 2017, the values of the two largest cryptocurrencies (by market capitalization), bitcoin and ether’s, grew approximately 1,411% and 8,500% respectively. These price rises can be paired with a sizeable increase in mainstream interest, including a growing body of inexperienced market participants with little understanding of the blockchain protocol underlying the cryptocurrencies which they trade, and of the exchange trading and direct peer-to-peer markets for cryptocurrencies. It is expected that with the recent boom in interest, further regulatory scrutiny will follow. In 2018, market prices reversed and by October 2018 the market capitalization had fallen to approximately $200 billion but cryptocurrencies look set to stay.
In 2018, the New York State Office of the Attorney General (OAG) sent letters to 13 cryptocurrency exchanges to gather data for a 40-page report eventually published in September 2018. Within the report, several key shortcomings of exchanges were cited including a lack of ability to combat market abuse real-time and prevent wash trading. They also highlighted that conflicts are rampant, with exchanges engaging in several business lines and that there was no ‘rhyme or reason’ to the listing of new currencies on their platforms. In other words, creators of worthless cryptocurrencies can simply bribe exchanges to feature their coin.

Many exchanges were quick to respond to the report. Coinbase’s Mike Lempres (their CPO), was largely welcoming of the report but disagreed with some aspects; in particular, that Coinbase (GDAX) were engaging in proprietary trading. Kraken, one of four exchanges that refused to provide information for the report, explained that since they do not operate in New York they were not obligated to participate. However, the OAG noted that “In announcing the company’s decision not to participate, Kraken declared that market manipulation ‘doesn’t matter to most crypto traders’ even while admitting that ‘scams are rampant’ in the industry.” Based on the investigation, the OAG referred Binance, Gate.io, and Kraken to the Department of Financial Services (NYDFS) for potential violation of New York’s virtual currency regulations. At the time of writing, no formal charges have been brought against any exchange.

Practically all the problems the OAG listed can be linked to the discussion in 8.2 explaining why fraud and manipulation are rife in cryptocurrency markets, and the report’s conclusion points toward a clear need for increased regulation. However, regulators wishing to remove manipulative practices like those documented here need to be careful when doing so, not to alter the wider characteristics that make cryptocurrency markets a unique and attractive environment to the many legitimate traders and investors.

Furthermore, as mentioned in Section 1.8, cryptocurrencies are cross-listed assets (i.e. identical products which can be traded in multiple locations) and so, although many ‘banked’ exchanges such as Coinbase will maintain traditional banking relationships and comply with local KYC and AML requirements, they will be linked to unbanked exchanges where it is easier to manipulate the market. This makes effective regulation difficult and is one of the reasons the SEC continues to reject cryptocurrency ETF proposals.
### CHAPTER 1: TEST YOUR KNOWLEDGE

The following questions are designed to ensure that you have a complete understanding of the information presented in the chapter (assignment). They are included as an additional tool to enhance your learning experience and do not need to be submitted in order to receive CPE credit.

We recommend that you answer each question and then compare your response to the suggested solutions on the following page(s) before answering the final exam questions related to this chapter (assignment).

<table>
<thead>
<tr>
<th>1.</th>
<th>Which of the following relies on techniques from cryptography for security, which allow them to function without a centralized authority, such as a central bank:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A. a digital currency</td>
</tr>
<tr>
<td></td>
<td>B. a virtual currency</td>
</tr>
<tr>
<td></td>
<td>C. a fiat currency</td>
</tr>
<tr>
<td></td>
<td>D. a cryptocurrency</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.</th>
<th>The rise of cryptocurrencies was led by the introduction of which of the following in 2008:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A. Bitcoin</td>
</tr>
<tr>
<td></td>
<td>B. Ethereum</td>
</tr>
<tr>
<td></td>
<td>C. Litecoin</td>
</tr>
<tr>
<td></td>
<td>D. Ripple</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3.</th>
<th>Which of the following is correct regarding public blockchains:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A. public blockchains tend to be small</td>
</tr>
<tr>
<td></td>
<td>B. public blockchains never utilize tokens</td>
</tr>
<tr>
<td></td>
<td>C. public blockchains are open for anyone to participate at any level</td>
</tr>
<tr>
<td></td>
<td>D. the core code of public blockchains may or may not be open source</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>4.</td>
<td><strong>Which of the following is not correct regarding the impact of blockchains:</strong></td>
</tr>
<tr>
<td></td>
<td><strong>A.</strong> blockchains allow for slow business and banking processes to be completed in days rather than weeks</td>
</tr>
<tr>
<td></td>
<td><strong>B.</strong> blockchains are considered the “fifth evolution” of computing</td>
</tr>
<tr>
<td></td>
<td><strong>C.</strong> blockchains can create trust in digital data</td>
</tr>
<tr>
<td></td>
<td><strong>D.</strong> blockchains allow for the creation and maintenance of things like property rights and identity to be conducted online</td>
</tr>
<tr>
<td>5.</td>
<td><strong>Which of the following is correct regarding hashing:</strong></td>
</tr>
<tr>
<td></td>
<td><strong>A.</strong> hashing was the recent discovery that led to blockchains</td>
</tr>
<tr>
<td></td>
<td><strong>B.</strong> hashing creates a two-way mathematical algorithm that is difficult to decrypt</td>
</tr>
<tr>
<td></td>
<td><strong>C.</strong> hashing requires the use of bit strings, which are typically 256 characters long</td>
</tr>
<tr>
<td></td>
<td><strong>D.</strong> hashes are the digital equivalent of a fingerprint</td>
</tr>
<tr>
<td>6.</td>
<td><strong>For which of the following purposes have blockchains been utilized:</strong></td>
</tr>
<tr>
<td></td>
<td><strong>A.</strong> paying employees in other countries</td>
</tr>
<tr>
<td></td>
<td><strong>B.</strong> trading public company stock</td>
</tr>
<tr>
<td></td>
<td><strong>C.</strong> currency exchanges</td>
</tr>
<tr>
<td></td>
<td><strong>D.</strong> all of the above</td>
</tr>
<tr>
<td>7.</td>
<td><strong>There is no single agreed upon definition of a cryptoasset.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>A.</strong> true</td>
</tr>
<tr>
<td></td>
<td><strong>B.</strong> false</td>
</tr>
<tr>
<td>8.</td>
<td><strong>The Ethereum blockchain was the first fully functional distributed ledger technology (DLT) used.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>A.</strong> true</td>
</tr>
<tr>
<td></td>
<td><strong>B.</strong> false</td>
</tr>
<tr>
<td>9.</td>
<td><strong>The market price and traded volume of the 2000+ crypto tokens currently listed on exchanges combine to form an asset class with a market capitalization of $1 billion.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>A.</strong> true</td>
</tr>
<tr>
<td></td>
<td><strong>B.</strong> false</td>
</tr>
</tbody>
</table>
10. Which of the following is correct regarding Mt. Gox:
   A. Mt. Gox is one of the most successful cryptocurrencies available today
   B. Mt. Gox was initially launched as an online poker website
   C. Mt. Gox failed due to the loss of bitcoins by an unknown entity over a prolonged period of time
   D. the failure of Mt. Gox proved that crypto exchanges were not lucrative

11. Limit orders are those orders which indicate a price and quantity at which a trader is willing to buy or sell an asset while a market order does not specify a price.
   A. true
   B. false

12. All cryptocurrency exchanges are required to enforce Know-Your-Customer (KYC) and Anti-Money-Laundering (AML) procedures.
   A. true
   B. false

13. Twitter is the most common mobile chat platform that crypto pump and dump groups are formed on, due to its high level of anonymity and encryption.
   A. true
   B. false

14. Which of the following is a manipulation that previously had a big impact on the perception of the global cryptocurrency trading ecosystem, but no longer occurs:
   A. an inflated trading volume scheme
   B. a pump and dump
   C. a DDoS attack
   D. an exchange hack

15. DDoS attacks are usually reported on an exchange’s Twitter feed.
   A. true
   B. false
16. Exploitation refers to gaining unauthorized access to a private system or network.
   A. true
   B. false

<table>
<thead>
<tr>
<th>17.</th>
<th>Which of the following is correct regarding smart contracts:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A. smart contracts are hosted on blockchains</td>
</tr>
<tr>
<td></td>
<td>B. smart contract writers are encouraged to also release a human readable version of their code</td>
</tr>
<tr>
<td></td>
<td>C. there are limited guidelines as to what makes for good smart contract code</td>
</tr>
<tr>
<td></td>
<td>D. all of the above</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>18.</th>
<th>All of the following are correct regarding the Decentralized Autonomous Organization (DAO) except:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A. the DAO is the software that makes bitcoin function</td>
</tr>
<tr>
<td></td>
<td>B. the DAO had funds drained through an attack before any funding could be allocated</td>
</tr>
<tr>
<td></td>
<td>C. due to the way in which the DAO was designed, stolen funds could not be accessed by the attacker for 28 days</td>
</tr>
<tr>
<td></td>
<td>D. the original DAO investors were able to retrieve the funds stolen from them</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>19.</th>
<th>In 2010, Bitcoin suffered a famous example of a protocol exploit.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A. true</td>
</tr>
<tr>
<td></td>
<td>B. false</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>20.</th>
<th>The definition of a flash crash should depend on which market is being analyzed and consider which of the following characteristics:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A. the market's role in the wider economy</td>
</tr>
<tr>
<td></td>
<td>B. the duration of the crash</td>
</tr>
<tr>
<td></td>
<td>C. the relative deviation from the mean return</td>
</tr>
<tr>
<td></td>
<td>D. all of the above</td>
</tr>
</tbody>
</table>
21. **Which of the following is correct regarding the 2010 DJIA flash crash:**
   - A. the flash crash wiped out over $100 billion from the U.S. economy
   - B. a $4.1 million trade triggered the 2010 crash
   - C. the DJIA lost roughly 1,000 points and then recovered within the space of 15 minutes
   - D. all of the above are correct

22. **Which of the following **cannot** be defined as a flash crash:**
   - A. the 2010 DJIA crash
   - B. the 2013 bitcoin crash
   - C. the 2017 gold futures crash
   - D. the 2017 Ether crash

23. **Quote stuffing and order spoofing are examples of order book manipulations.**
   - A. true
   - B. false
# CHAPTER 1: SOLUTIONS AND SUGGESTED RESPONSES

Below are the solutions and suggested responses for the questions on the previous page(s). If you choose an incorrect answer, you should review the pages as indicated for each question to ensure comprehension of the material.

1.  
   A. Incorrect. Digital currencies are electronic representations of value that include a broad range of common payment systems, such as gift cards, air miles, and mobile coupons.  
   
   B. Incorrect. Some, but not all, virtual currencies may use techniques from cryptography. However, this selection is not the best answer.  
   
   C. Incorrect. Fiat currencies are government backed currencies, like the U.S. dollar.  
   
   D. **CORRECT**. Cryptocurrencies are a type of virtual currency (and therefore a digital currency) that relies on techniques from cryptography for security, which allow them to function without a centralized authority, such as a central bank, government, or private company.  
   
   *(See page 1 of the course material.)*

2.  
   A. **CORRECT**. The rise of cryptocurrencies was led by the introduction of Bitcoin in 2008, which was one of the first to use a blockchain to record transactions without the use of a trusted central authority.  
   
   B. Incorrect. Ethereum is another cryptocurrency, but not the one which led to the popular use of cryptocurrency in 2008.  
   
   C. Incorrect. Litecoin was not the cryptocurrency which became popular in 2008.  
   
   D. Incorrect. The rise of cryptocurrencies did not begin with the advent of Ripple.  
   
   *(See page 1 of the course material.)*

3.  
   A. Incorrect. Public blockchains tend to be large distributed networks, while private blockchains tend to be much smaller.  
   
   B. Incorrect. Public blockchains, such as Bitcoin, run through a native token.  
   
   C. **CORRECT**. Public blockchains are open for anyone to participate at any level.  
   
   D. Incorrect. The core code of a public blockchain is open-source code, while the core code of a permissioned blockchain may or may not be open source.  
   
   *(See page 2 of the course material.)*
4. **A.** CORRECT. Blockchains allow for slow business and banking processes to be done nearly instantaneously.

**B.** Incorrect. Blockchains are considered to be the “fifth evolution” of computing, allowing for the full confidence in digital data.

**C.** Incorrect. Blockchains allow for the creation of trustworthy digital data because once information has been written into a blockchain database, it is almost impossible to remove or change it.

**D.** Incorrect. Because Blockchains allow for the creation of permanent and reliable digital data, areas that have remained analog, such as property rights and identity, can now be created and maintained online.

*(See page 3 of the course material.)*

5. **A.** Incorrect. While blockchains are a recent innovation, hashing was invented over 30 years ago.

**B.** Incorrect. Hashing creates a one-way function that cannot be decrypted.

**C.** Incorrect. Bit strings are usually only 32 characters long, not 256.

**D.** CORRECT. A hash can be seen as a digital fingerprint of data that is used to lock it in place within the blockchain.

*(See page 4 of the course material.)*

6. **A.** Incorrect. Blockchains are utilized for the purpose of paying employees in other countries, but this is not the only selection that is correct.

**B.** Incorrect. The trading of stock in public companies is an area that blockchains are commonly used for. However, this is not the only selection that is correct.

**C.** Incorrect. Currency exchanges frequently utilize blockchains, but this is not the only correct selection.

**D.** CORRECT. Most current blockchain applications exist for the purpose of moving money or other forms of value quickly and cheaply. Blockchains are used to pay employees in other countries, trading public company stock, and exchanging one currency for another.

*(See page 6 of the course material.)*

7. **A.** CORRECT. There is no single agreed definition of a cryptoasset, but in general they are cryptographically secured digital representations of value or contractual rights which can be stored, transferred, or traded electronically.

**B.** Incorrect. Although there is a general agreement on what cryptoassets are, there is no single agreed upon definition.

*(See page 7 of the course material.)*
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| **8.** | **A.** Incorrect. Ethereum was not the first fully functional DLT.  
**B.** **CORRECT**. The Bitcoin blockchain was the first fully functional DLT, used and maintained by a network of communicating nodes which run the client software.  
(See page 7 of the course material.) |
| **9.** | **A.** Incorrect. The actual market capitalization is significantly higher than $1 billion.  
**B.** **CORRECT**. The market price and traded volume of the 2000+ crypto tokens currently listed on exchanges combine to form an asset class with a market capitalization (market price multiplied by the number of existing currency units) of $121 billion.  
(See page 9 of the course material.) |
| **10.** | **A.** Incorrect. Mt. Gox is not a cryptocurrency, but rather a crypto exchange where people could trade bitcoins.  
**B.** Incorrect. Mt. Gox was originally designed in 2007 as an exchange for fantasy trading cards.  
**C.** **CORRECT**. Due to several technical issues throughout its existence, bitcoins were being removed over a prolonged period by an unknown entity. The loss of bitcoins caused Mt. Gox to collapse in 2013 and file for bankruptcy in 2014.  
**D.** Incorrect. Despite Mt. Gox's failure, replacements quickly emerged as running a crypto exchange had been proven to be a lucrative business.  
(See page 9 of the course material.) |
| **11.** | **A.** **CORRECT**. Unlike market orders, limit orders are orders that indicate a price and quantity at which a trader is willing to buy or sell an asset, and these are recorded in the order book.  
**B.** Incorrect. A market order does not specify a price, only a quantity and direction. However, a limit order does indicate a price.  
(See page 10 of the course material.) |
| **12.** | **A.** Incorrect. Unlike cryptocurrency exchanges, many traditional financial exchanges are required to enforce Know-Your-Customer (KYC) and Anti-Money-Laundering (AML) procedures, which include the detailed records of traders using their exchanges.  
**B.** **CORRECT**. Some cryptocurrency exchanges do enforce KYC and AML procedures; however, some do not.  
(See page 12 of the course material.) |
13.  
A. Incorrect. Telegraph, not Twitter, is the mobile chat platform preferred by perpetrators of crypto pump and dump schemes.  
B. **CORRECT**. Telegram is the most common mobile chat platform that groups are formed on, due to its high level of anonymity and encryption. This, coupled with the relative anonymity of markets, means it is difficult to identify perpetrators.  

*(See page 15 of the course material.)*

14.  
A. **CORRECT**. Although inflated trading volume schemes no longer occur, they previously had a big impact on the perception of the global cryptocurrency trading ecosystem, but no longer occurs.  
B. Incorrect. A pump and dump occurs when an entity accumulates a large amount of a target asset and subsequently promotes its purchase as an opportunity for substantial future return. While others enter, the original position is unwound and when the promotion stops, the price then crashes.  
C. Incorrect. Exchange DDos attacks are an attempt by an attacker to overwhelm a network target with a large volume of incoming messages. These types of manipulations still occur.  
D. Incorrect. Exchange hacks occur when attackers try to take control of an exchange’s server.  

*(See pages 16 to 17 of the course material.)*

15.  
A. **CORRECT**. DDoS attacks are usually reported on an exchange’s Twitter feed, as this is one of the few ways to learn, from an external perspective, whether a DDoS incident has occurred.  
B. Incorrect. DDos attacks are, in fact, usually reported on an exchange’s Twitter feed.  

*(See page 20 of the course material.)*

16.  
A. Incorrect. Exploitation refers to taking advantage of unintended design flaws in a smart contract or cryptocurrency protocol.  
B. **CORRECT**. Hacking, not exploitation, means gaining unauthorized access to a private system or network.  

*(See page 22 of the course material.)*
### Chapter 1: Fraud and Manipulation within Cryptocurrency Markets

#### 17. Smart Contracts

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A.</strong> Incorrect. Smart contracts are agreements written in code and enforced by the ecosystem in which they run. They are hosted on a blockchain, but this is not the only answer that is correct.</td>
<td></td>
</tr>
<tr>
<td><strong>B.</strong> Incorrect. In an attempt to be transparent, smart contract writers are encouraged to publish human readable versions of their code. However, this is not the only selection that is correct.</td>
<td></td>
</tr>
<tr>
<td><strong>C.</strong> Incorrect. Although there are attempts to outline good practices, there are limited guidelines for what makes good smart contract code. However, this is not the only correct selection provided.</td>
<td></td>
</tr>
<tr>
<td><strong>D.</strong> CORRECT. Smart contracts reside on blockchains, they have few guidelines for what makes for good smart contract code, and the writers of the code are encouraged to publish a human readable version.</td>
<td></td>
</tr>
</tbody>
</table>

*(See page 26 of the course material.)*

#### 18. The DAO

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A.</strong> CORRECT. The DAO was intended to be a decentralized venture capital fund.</td>
<td></td>
</tr>
<tr>
<td><strong>B.</strong> Incorrect. Before any funding could be allocated, an attack managed to drain considerable funds, preventing further progress on the project.</td>
<td></td>
</tr>
<tr>
<td><strong>C.</strong> Incorrect. As an unintended consequence of how the DAO was designed, the stolen funds could not be accessed by the attacker for 28 days.</td>
<td></td>
</tr>
<tr>
<td><strong>D.</strong> Incorrect. A hard fork was introduced to the Ethereum network which returned the funds stolen to an account accessible to original DAO investors.</td>
<td></td>
</tr>
</tbody>
</table>

*(See page 27 of the course material.)*

#### 19. Protocol Exploit

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A.</strong> CORRECT. One famous and early example of a protocol exploit is the Bitcoin protocol attack of August 2010, which worked by finding and exploiting an integer overflow bug which could not detect when a Bitcoin transaction output summed to over 184 billion bitcoins.</td>
<td></td>
</tr>
<tr>
<td><strong>B.</strong> Incorrect. In August 2010, Bitcoin suffered a protocol exploit.</td>
<td></td>
</tr>
</tbody>
</table>

*(See page 28 of the course material.)*

#### 20. Flash Crash

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A.</strong> Incorrect. The market's role in the wider economy should be considered when defining a flash crash, but this is not the only selection that is correct.</td>
<td></td>
</tr>
<tr>
<td><strong>B.</strong> Incorrect. The definition of a flash crash should consider the duration of the crash. However, this is not the only correct selection.</td>
<td></td>
</tr>
<tr>
<td><strong>C.</strong> Incorrect. The relative deviation from the mean return should be considered when defining a flash crash, but this is not the only selection that is correct.</td>
<td></td>
</tr>
<tr>
<td><strong>D.</strong> CORRECT. The definition of a flash crash should depend on which market is being analyzed and consider the duration of the flash crash, the relative deviation from the mean return, and the market's role in the wider economy.</td>
<td></td>
</tr>
</tbody>
</table>

*(See page 28 of the course material.)*
B. Incorrect. The trade that triggered the flash crash was in the amount of $4.1 billion.  
C. **CORRECT.** After the $4.1 billion trade was placed, the DJIA lost roughly 1,000 points and then recovered within the space of 15 minutes.  
D. Incorrect. Only one of the selections provided is correct.  

(See page 29 of the course material.)

22. | A. Incorrect. The 2010 DJIA is an example of a flash crash.  
B. **CORRECT.** The 2013 bitcoin crash cannot be defined as a flash crash because it occurred over a number of hours.  
C. Incorrect. The 2017 gold futures crash is an example of a flash crash as its duration from peak to trough was roughly 8 seconds.  
D. Incorrect. The 2017 Ether crash would be defined as a flash crash.  

(See page 31 of the course material.)

23. | A. **CORRECT.** Quote stuffing and order spoofing are two order book manipulations, using limit orders, which are designed to provide the manipulator with an unfair advantage.  
B. Incorrect. Quote stuffing and order spoofing are quite sophisticated order book manipulations developed from traditional financial markets and intend to distort or influence the true price of a currency pair.  

(See page 33 of the course material.)
**Benchmarking:** The practice of comparing business processes and performance metrics to industry bests and best practices from other companies.

**Blockchains:** A system in which a record of transactions made in bitcoin or another cryptocurrency are maintained across several computers that are linked in a peer-to-peer network.

**Cryptoassets:** Cryptographically secured digital representations of value or contractual rights that use some type of distributed ledger technology (DLT) and can be transferred, stored or traded electronically.

**Crypto exchanges:** A business that allows customers to trade cryptocurrencies or digital currencies for other assets, such as conventional fiat money or other digital currencies.

**Digital currency:** A form of currency that is available only in digital or electronic form, and not in physical form.

**Exchange DDoS attacks:** A Distributed Denial of Service (DDoS) attack is a non-intrusive internet attack made to take down the targeted website or slow it down by flooding the network, server or application with fake traffic.

**High-frequency trading:** A method of trading that uses powerful computer programs to transact a large number of orders in fractions of a second. Typically, the traders with the fastest execution speeds are more profitable than traders with slower execution speeds.

**Initial Coin Offerings (ICO):** A type of funding using cryptocurrencies. It is often a form of crowdfunding, however a private ICO which does not seek public investment is also possible. In an ICO, a quantity of cryptocurrency is sold in the form of “tokens” (“coins”) to speculators or investors, in exchange for legal tender or other (generally established and more stable) cryptocurrencies

**Market manipulation:** A type of market abuse where there is a deliberate attempt to interfere with the free and fair operation of the market and create artificial, false or misleading appearances with respect to the price of, or market for, a product, security, commodity or currency.

**Money laundering:** Money laundering is the illegal process of concealing the origins of money obtained illegally by passing it through a complex sequence of banking transfers or commercial transactions. The overall scheme of this process returns the “clean” money to the launderer in an obscure and indirect way.

**Order spoofing:** Spoofing is an illegal form of market manipulation in which a trader places a large order to buy or sell a financial asset, such as a stock, bond or futures contract, with no intention of executing. By doing so, the trader—or “the spoofer”—creates an artificial impression of high demand for the asset.

**Pump-and-dump:** Denoting the fraudulent practice of encouraging investors to buy shares in a company in order to inflate the price artificially, and then selling one’s own shares while the price is high.
Quote stuffing: The practice of quickly entering and then withdrawing large orders in an attempt to flood the market with quotes, causing competitors to lose time in processing them.

Stablecoins: A new class of cryptocurrencies that attempts to offer price stability and are backed by a reserve asset.

Stop-loss orders: An order placed with a broker to buy or sell a security when it reaches a certain price.

Virtual currencies: A form of digital currency that represents monetary value in electronic form and mostly remains outside of regulatory purview.
INDEX

A
anonymity 12, 15, 20, 43, 49, 56
Anti-Money-Laundering (AML) 12, 18, 45, 49, 55

B
barriers to entry 15, 20
benchmarking 33
bitcoin 1, 7, 9, 10, 16, 18, 19, 20, 21, 24, 25, 28, 30, 31, 41, 42, 44, 50, 51, 58
blockchain 1, 7, 9, 10, 12, 17, 22, 23, 24, 25, 26, 27, 28, 36, 37, 41, 44, 45, 53, 57
blockchain applications 5, 6, 7
Byzantine general’s problem 5

C
Canada 24
Chain 3
chief executive officers (CEO) 17, 18, 37
China 17, 18
cold storage 14
Commodity Futures Trading Commission (CFTC) 38
conflicts of interest 39
constraints 37
cryptoassets 7, 8
cryptocurrency exchange 6
cryptocurrency markets 11, 13, 14, 15, 19, 20, 26, 28, 30, 31, 33, 39, 42, 43, 44, 45
crypto exchanges 10, 12, 14, 24, 49
cryptography 2
crypto tokens 8, 9, 48, 55

D
Decentralized Autonomous Organization (DAO) 27, 28, 50, 57
digital currencies 1
Distributed Denial-of-Service attack (DDoS) 11, 13, 19, 20, 21, 22, 33, 43, 44, 49, 56
Distributed Ledger Technology (DLT) 7
Dow-Jones Industrial Average Index (DJIA) 29, 30, 31, 33, 51, 58
D-ratio 34

E
economics 41
dddos 2
Ethereum ecosystem 27
Ethereum flash crash 28, 30
exchange DDoS attacks 20, 43, 44
exchange hacks 23, 26
exchanges 2
exchange standards 17, 36

F
Federal Bureau of Investigation (FBI) 25
federated nodes 5
fees 9, 17, 18
Financial Services Authority (FSA) 25
flash crashes 11, 28, 29, 30, 31, 43
full nodes 2, 3, 4, 5
fund settlements 3
futures 30, 51, 58

H
hacks 11, 13, 17, 22, 23, 24, 26, 43, 56
hedge funds 9
high-frequency trading 33
Hong Kong 37

I
Initial Coin Offerings (ICO) 7, 8
innovation 7
inside information 14
interest 10, 39, 44
international travel security applications 6

J
Japan 24
<table>
<thead>
<tr>
<th>K</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td>Know-Your-Customer (KYC)</td>
<td>12, 18, 41, 45, 49, 55</td>
</tr>
<tr>
<td>Korea 23</td>
<td>sanctions 11</td>
</tr>
<tr>
<td>Kraken 21, 22, 39, 41, 42, 45</td>
<td>Secure Hash Algorithm 4</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>L</td>
<td></td>
</tr>
<tr>
<td>limit orders 10, 29, 33, 35, 58</td>
<td>self-driving cars 6</td>
</tr>
<tr>
<td>liquidity 10, 17, 21, 29, 30, 31, 43</td>
<td>sell orders 10, 15, 17, 19, 23, 31, 40, 43</td>
</tr>
<tr>
<td></td>
<td>smart contract 22, 26, 27, 50, 57</td>
</tr>
<tr>
<td>M</td>
<td>spoofing 11, 30, 33, 35, 36, 43, 44, 58</td>
</tr>
<tr>
<td>margin trading 18</td>
<td>stablecoins 36, 43</td>
</tr>
<tr>
<td>market manipulation 10, 14, 28, 30, 32, 41, 45</td>
<td>Standard and Poor’s Index (S&amp;P) 30</td>
</tr>
<tr>
<td>market orders 15, 29, 30</td>
<td>stop-loss orders 30, 31</td>
</tr>
<tr>
<td>misconduct 37, 43</td>
<td>surveillance 14</td>
</tr>
<tr>
<td>money laundering 25</td>
<td></td>
</tr>
<tr>
<td>money wires 3</td>
<td></td>
</tr>
<tr>
<td>monitoring 13</td>
<td></td>
</tr>
<tr>
<td>Mt. Gox 9, 20, 21, 24, 25, 31, 49, 55</td>
<td>Tether 11, 36, 37, 38, 39, 40, 41, 42, 43</td>
</tr>
<tr>
<td></td>
<td>trading data 21, 41</td>
</tr>
<tr>
<td></td>
<td>trading volumes 18, 44</td>
</tr>
<tr>
<td></td>
<td>trust layer 3, 6</td>
</tr>
<tr>
<td></td>
<td>Twitter 13, 15, 20, 21, 49, 56</td>
</tr>
<tr>
<td>N</td>
<td></td>
</tr>
<tr>
<td>NiceHash 25, 26</td>
<td></td>
</tr>
<tr>
<td>O</td>
<td></td>
</tr>
<tr>
<td>open-source code 2</td>
<td></td>
</tr>
<tr>
<td>options 25</td>
<td></td>
</tr>
<tr>
<td>order book manipulations 33, 58</td>
<td></td>
</tr>
<tr>
<td>order spoofing 35, 36, 43, 44</td>
<td></td>
</tr>
<tr>
<td>P</td>
<td></td>
</tr>
<tr>
<td>pegging 39</td>
<td></td>
</tr>
<tr>
<td>protocol exploitation 28</td>
<td></td>
</tr>
<tr>
<td>pump-and-dump 15</td>
<td></td>
</tr>
<tr>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>quote stuffing 11, 14, 33, 34, 36, 43</td>
<td></td>
</tr>
<tr>
<td>R</td>
<td></td>
</tr>
<tr>
<td>regulation 11, 12, 17, 20, 23, 33, 45</td>
<td></td>
</tr>
<tr>
<td>S</td>
<td></td>
</tr>
<tr>
<td>safety systems 6</td>
<td></td>
</tr>
<tr>
<td>sanctions 11</td>
<td></td>
</tr>
<tr>
<td>Securities and Exchange Commission (SEC) 14, 27, 45</td>
<td></td>
</tr>
<tr>
<td>self-driving cars 6</td>
<td></td>
</tr>
<tr>
<td>sell orders 10, 15, 17, 19, 23, 31, 40, 43</td>
<td></td>
</tr>
<tr>
<td>smart contract 22, 26, 27, 50, 57</td>
<td></td>
</tr>
<tr>
<td>spoofing 11, 30, 33, 35, 36, 43, 44, 58</td>
<td></td>
</tr>
<tr>
<td>stablecoins 36, 43</td>
<td></td>
</tr>
<tr>
<td>Standard and Poor’s Index (S&amp;P) 30</td>
<td></td>
</tr>
<tr>
<td>stop-loss orders 30, 31</td>
<td></td>
</tr>
<tr>
<td>surveillance 14</td>
<td></td>
</tr>
<tr>
<td>T</td>
<td></td>
</tr>
<tr>
<td>Tether 11, 36, 37, 38, 39, 40, 41, 42, 43</td>
<td></td>
</tr>
<tr>
<td>trading data 21, 41</td>
<td></td>
</tr>
<tr>
<td>trading volumes 18, 44</td>
<td></td>
</tr>
<tr>
<td>trust layer 3, 6</td>
<td></td>
</tr>
<tr>
<td>Twitter 13, 15, 20, 21, 49, 56</td>
<td></td>
</tr>
<tr>
<td>U</td>
<td></td>
</tr>
<tr>
<td>United States of America (USA) 8, 13, 29, 36, 39</td>
<td></td>
</tr>
<tr>
<td>U.S. Department of Homeland Security 6</td>
<td></td>
</tr>
<tr>
<td>V</td>
<td></td>
</tr>
<tr>
<td>virtual currencies 53</td>
<td></td>
</tr>
<tr>
<td>virtual private networks (VPN) 13</td>
<td></td>
</tr>
<tr>
<td>W</td>
<td></td>
</tr>
<tr>
<td>Wells Fargo 37, 38</td>
<td></td>
</tr>
<tr>
<td>Z</td>
<td></td>
</tr>
<tr>
<td>zombie computers 19</td>
<td></td>
</tr>
</tbody>
</table>