July 2018

Control Frameworks For Cryptocurrencies: An Initial Evaluation

DasCoin™
The Currency of Trust

The Z/Yen Group

Control Frameworks For Cryptocurrencies:

An Initial Evaluation

July 2018

Matthew Leitch
Z/Yen Group

Aleksandar Matanović
CEO and Co-Founder, ecd.rs

Foreword

DasCoin is delighted to sponsor this interesting and creative investigation of the risk and control needs of cryptocurrencies.

This Eternal Coin research tackles some of the most basic questions about managing all types of risk around cryptocurrencies, from the perspective of all their stakeholders. Using three different analysis methods it combines conventional control thinking with the ideas of the crypto community, offering suggestions applicable to a wide range of cryptocurrencies operating in many different environments.

The objective is to guide cryptocurrencies to a future where they are mainstream, efficient payment systems, competitively successful, widely available, and safe for users and investors. This will involve innovative technology within a framework of appropriate governance, management, procedural, and programmed controls.

We are pleased to have sponsored this important research and hope its many suggestions help business people, technologists, policy-makers, and regulators in setting up increasingly comprehensive and appropriate control systems for cryptocurrencies.

Michael Mathias
CEO, DasCoin

Contents

Preface

Organisation requires control. Control can range from the simple, “follow me”, to the execution of detailed strategic and tactical plans. And how do I know you’re following me? “Trust me”. Germans are fond of a saying attributed to Lenin, “Vertrauen ist gut, Kontrolle ist besser!“ (“Trust is good, but control is better”). Today’s complex social, technical, political, and legal environment has promoted the use of control frameworks. A control framework provides an explicit structure for the practices and procedures an organisation uses to create value and minimize risk. It’s a blueprint for the controls that will be used for operations, reporting, and compliance.

A ‘control framework’ is an abstract, yet essential, concept. The controls should be geared to the achievement of objectives, not the prevention of performance. The framework should consist of ongoing tasks and activities, not become an end in itself. The framework needs to be something that people in the organisation can use and understand. The framework should provide reasonable, rather than absolute, assurance to senior management and stakeholders that the organisation is on track to achieve its goals.

Systems-based thinking frequently includes mention of control system elements. Control is explored by many organisational theorists as a sub-system or set of sub-systems, but also as a desirable element of its own. The limitations of systems thought and systems constraints on creativity and dynamism are important and reaction against them can be strong. Some research would encourage freedom among the constituent units in the organisation to generate creative conflicts between them. Creativity through control, or creative conflict.

Control needs measurement. Measurement takes place by (1) assessing against a standard or (2) comparing against like objects or (3) comparing against a prediction or model. These three means of measuring – (1) standard-based, (2) comparative, (3) predictive – can be fused, e.g. average the comparisons and one has a standard, or consider a prediction to be just another comparison. A current example of mixed means is the ‘balanced scorecard’ approach of Kaplan and Norton. The three means of measuring are worth retaining independently because (1) is about an absolute measure, (2) is about conditional measure, and (3) focuses on expected outcomes. Measure immediately begs the questions, “by whom?” and “for what end?” For the moment, one may assume the measure is by an uninvolved third party and the end sought is an opinion on the quality of a control system.

What makes this booklet so important is that in the new field of digital and cryptocurrencies we need to extend existing control approaches, such as COSO (Committee of Sponsoring Organizations of the Treadway Commission). We need to be able to answer questions such as "what makes a good currency?" and "how do we know this currency will perform as it is intended to?" This report explores controls by looking at currencies through their lifecycle, looking at their special control needs, and looking from the perspective of numerous stakeholders. Ultimately, a control framework for a cryptocurrency might provide a 'market quality dashboard' with statistics on the performance of the cryptocurrency. Perhaps, in the end, like a Good Pub Guide, we can have a Good Currencies Guide, not based on the speculative gains from holding currencies, but on their productive use in helping the wider economy and society.

Professor Michael Mainelli
Executive Chairman, Z/Yen Group

Executive Summary

Cryptocurrency development has been an exciting area for several years with many new ideas coming forward and yet there is still the potential of a new launch that solves the biggest technical and commercial challenges.

However, to date almost all the 1,500+ cryptocurrencies that have been launched have died away and even Bitcoin has serious technical limitations that have prevented it being a competitive payment system in most situations. Cryptocurrencies have been seriously impacted by technical problems, disagreements, fraud, hacks, competition, regulation, lack of popularity, apathy, and sheer incompetence.

To increase the odds of success, those who aspire to launch a successful cryptocurrency must think through the challenges they may face, make plans, make design choices, and develop capabilities that help them survive. They need control frameworks, practices and procedures to create business value and control risk. While unglamorous, these are intellectually tough to create and must respond to the special characteristics of cryptocurrencies. This report looks at the control needs of cryptocurrencies mainly from the perspective of their creators and regulators. It aims to make recommendations on controls for cryptocurrencies that are not too prescriptive but more helpful than generic control frameworks such as COSO's frameworks for internal control and enterprise risk management (Committee of Sponsoring Organizations of the Treadway Commission 2013, 2017), and variations on them (e.g. Basel Committee on Banking Regulation 1998, Financial Reporting Council 2014).

This complements previous Long Finance work on governance, audit, and standards for smart ledger systems. It also reflects the focus of the Eternal Coin research programme, a global discussion on the nature of money and the concept of value over the long term.

This report provides organised justifications for including particular controls. You will probably find that most of its proposals are ones you have already thought of, or would have. But some will come as a slight surprise and some of the things you might have missed may be important.

The three methods described below are progressively more detailed and go beyond generic frameworks by considering the special characteristics of crypto-currencies and their ecosystems. While it is impossible to be sure that all risk

concerns and all controls have been considered, the methods are systematic explorations designed to expand thinking.

Method A: Control through the cryptocurrency lifecycle, simply lists each of the lifecycle stages of a cryptocurrency and considers its control priorities. The early stages will feel familiar but what about the various ways that a cryptocurrency can mutate or die, later in its life?

Method B: Distinctive characteristics and their control implications, starts by thinking about what is distinctive about cryptocurrencies compared to systems generally, and especially financial systems. What do these distinctive characteristics imply about the control system for a cryptocurrency and its ecosystem? This leads to a high level but useful summary of control requirements and mechanism ideas, structured into layers.

Method C: Stakeholder decision risk and control analysis, starts by identifying the stakeholder groups for a cryptocurrency, along with the main decisions they must take concerning it. These include decisions about system design and operational procedures. It is uncertainty around these decisions that is the basis for risk thinking and a spur for ideas about control.

Some interesting repeated requirements emerge from this more detailed analysis, including ideas for a market quality dashboard, other information services, economic and performance simulation, and some other control ideas.

This work complements past reports from the Long Finance programme:

- “Auditing Mutual Distributed Ledgers (aka Blockchains): A Foray Into Distributed Governance & Forensics” by Michael Mainelli and Matthew Leitch, November 2017.
- “Responsibility Without Power? The Governance Of Mutual Distributed Ledgers (aka Blockchain)” by Simon Mills and Bob McDowall, July 2017.
- “The Missing Links In The Chains? Mutual Distributed Ledgers (aka blockchain) Standards” by Michael Mainelli and Simon Mills, November 2016.
- “The London Token Fundraising Manifesto” published October 2017, with many signatories.

- ‘In Search of the Eternal Coin: A Long Finance View of History’ by Malcolm Cooper, March 2010.

1 Introduction

Cryptocurrencies do not come into being spontaneously. Someone has the idea of creating one and a group of people forms that pushes the idea into reality, perhaps using a legal entity or perhaps not. Within this report, that group of people will be called the initiators.

Those enterprising individuals face more challenges than perhaps they realise when they start out. Of the 1,500+ cryptocurrencies that have been launched to date almost all have faded into oblivion. The odds of success, considered historically, are poor. Cryptocurrencies have been cut down by technical problems, apathy, hacks, fraud, delays, regulation, and simple failure to write correct software as quickly as was hoped. It is a highly competitive field with competition from long established electronic payment systems that are extremely efficient, most of the time.

Even the best known cryptocurrency today, Bitcoin, is far too costly and slow to compete as a payment system and has become predominantly an asset for speculative investment (Carney, 2018).

The initiators of a new cryptocurrency need to think very carefully about how they can survive the hazards of their undertaking. This means thinking about everything that is at all uncertain or outside their complete control – the risks – and devising ways to survive and even thrive. This thinking needs to be comprehensive but focused on what matters most, taking into consideration the special characteristics of cryptocurrencies and the people that get involved with them.

Ideally, initiators should strive to understand the issues from the perspectives of all the main stakeholders, so that the initiators can provide others with the information and assurance they need to make decisions and put their trust in the cryptocurrency and the people behind it.

This report aims to provide a high level view of risk and control for a potential cryptocurrency. It looks at all areas of risk from the point of view of all the main stakeholder groups, and their decisions, but focuses in particular on the perspective of the main initiators of the cryptocurrency and its ecosystem. By doing this it also provides a useful perspective for regulators and anyone else interested in the effectiveness of control for cryptocurrencies and in predicting their long term future. Ultimately, the focus is on long term public interests.

Most readers should find that the report confirms much of their thinking, but may also come across important points they might have overlooked. While it is impossible to guarantee that all risks and controls have been considered, the analysis methods used are designed to give a thorough exploration.

The analysis is not quantified and, for simplicity, not mapped into the usual risk categories of financial services. The categorisation is usually obvious anyway. The risk analysis and controls design methods used focus on the lifecycle of a cryptocurrency, the distinctive characteristics of cryptocurrencies as distinct from other systems, and the main decisions taken by all the main stakeholder groups.

The conclusions include inferences about the characteristics of controls needed and the information needs of stakeholders. They include ideas for the content of a market quality dashboard that addresses the needs of stakeholders, and point to a simulation tool we plan as the next phase of this project.

2 Report Methodology

Three different but complementary methods are used in this report to organise thinking and deduce conclusions about risk and control around a cryptocurrency. These are based on the special characteristics of cryptocurrencies and provide more helpful guidance than a single, generic method.

Method A: Control Through the Cryptocurrency Lifecycle

In this approach, the lifecycle stages of a cryptocurrency from first idea to the final ending of a failed or replaced cryptocurrency are listed. The main control priorities at each stage are identified. This is all from the perspective of the sponsor/designer of the cryptocurrency.

Method B: Distinctive Characteristics And Their Control Implications

To provide more detail and focus on what is special and interesting about control for cryptocurrencies, the next analysis begins by listing the distinctive characteristics of a cryptocurrency as a business/system/process. From these, deductions are made about the control scheme needed. The idea is to highlight the adaptations that would be needed to a generic scheme, with all the usual elements, by focusing on what is different in the case of cryptocurrencies.

Method C: Stakeholder Decision Risk And Control Analysis

To provide something of direct interest to other stakeholders, and to get more detail still, the final analysis begins by listing stakeholder groups and their decisions. Each identified decision is then studied in more detail by listing factors that would be considered (implicitly if not explicitly). Since risk/uncertainty attaches to most if not all of these factors (e.g. how costly will operation be with a particular cryptographic mechanism used?) this constitutes a structured risk

analysis. The next step is to think of the information that would help reduce the uncertainty involved, and other controls that the stakeholder could use to manage risk in relation to those uncertain factors and around that decision. The final step is to summarise the conclusions from this, including the information needs of stakeholders that a cryptocurrency designer might seek to meet.

However, we begin with a review of the factual background particularly relevant to this analysis. This clarifies the variety of cryptocurrencies for which control is needed, and describes the events and other factors that introduce risk.

3 Observations On Cryptocurrency History

This section provides some information about cryptocurrencies that informs the analysis of risk and controls. It covers three types of information:

- Design differences between cryptocurrencies, because these can affect how they behave, who wants to use them, and how vulnerable they are to various potential security and economic problems.
- Life stories of cryptocurrencies, showing how some have succeeded and some have failed.
- The reasons for cryptocurrency prices, success, and failure, including some dramatic events that have occurred.

3.1 Varieties Of Cryptocurrency

This section explains some of the most important ways in which crypto-currencies differ from each other in design.

Development Route

The way cryptocurrencies are developed makes a big difference to the risk involved.

Both the program code and blockchains of some cryptocurrencies have been developed from scratch. Bitcoin is the obvious example of this.

Very often the code has been open source, so a typical route in recent years has been to start with the code of an existing cryptocurrency and modify it, then start a new blockchain.

A further shortcut has been to hard fork an existing cryptocurrency. This involves modifying the program code and managing a split of the blockchain so that, on a planned date, everyone holding cryptocoins in the old cryptocurrency also gets the same number of coins in the new one. The two cryptocurrencies then carry on independently. This way the new cryptocurrency gets a head start with both code and user-base.

Though there seems little economic logic to it, this hard fork method is generally liked by users because they have often profited from having more cryptocoins.

Another route is to develop a token using the infrastructure of another blockchain. The best-known examples are ERC20-compliant tokens generated on the Ethereum network.

Governance

Once launched, a cryptocurrency still needs human decisions on matters such as:

- Parameter values used in the system (e.g. total cryptocoins to produce);
- Program code changes (improvements and fixes for problems); and
- Responses to crises (e.g. a hack, a technical failure).

Collectively these are important to overall control.

The main groups that might have a say are the software developers, the node operators/miners, and the holders of the cryptocurrency.

The approach to governance varies, with some cryptocurrencies being more centrally controlled than others. Involvement with different types of decision may vary. The stakeholders may be directly involved or appoint representatives. Forms of electronic voting are popular.

In the well known decentralised cryptocurrencies the developer community commonly suggests the options but the miners/node operators – through their choices about which software to run – have some power to choose which options are adopted.

Consensus Algorithm

A cryptocurrency's consensus algorithm is the process by which holders of copies of its blockchain keep those copies in agreement. It does not necessarily require them to discuss alternatives and agree, as humans would. Consensus algorithms have many rules that honest nodes must follow and these help protect the blockchain from nodes that fail to follow the rules, provided the dishonest nodes are in a sufficiently small minority.

The consensus algorithm must ensure that transactions are recorded in blocks exactly once, with the same details, and in the same order, that the order reflects the actual time of the transactions (but not necessarily exactly), that the transaction details agree to those originally submitted, and that holders cannot spend more cryptocurrency than they have.

Participants are usually rewarded for their work with newly generated units of the cryptocurrency.

Within consensus algorithms there are many rules but one of the most important features for practical purposes is the method that determines who creates the next block for distribution to others. That method usually involves randomisation and usually makes block formation costly to discourage rewriting blocks. There are many design alternatives for this, but the three best known are as follows:

- Proof-of-Work (PoW) requires competing 'miners' to search for a number that solves a computational problem where luck and speed determine which miner wins that race. If a miner is first to find a solution it creates the next block and broadcasts it to others. PoW is the oldest and still the most widely used. It is used in Bitcoin, Ethereum, Litecoin and many others. Finding a solution is computationally intensive, so miners often use specialist hardware, but it is easy for other participants to check that the solution is correct. On average, the rewards for miners are proportional to the power of their hardware. The power consumption of the growing population of PoW miners has become a concern.

- Proof-of-Stake (PoS) uses holdings of cryptocoins rather like lottery tickets, giving participants chances to be selected (randomly) to create the next block. In different designs the period of holding the cryptocoins might be important, or the cryptocoins might have to be committed in some way. PoS is much more energy-efficient than PoW, but has not yet been accepted as secure and effective by a bigger project. PoS is used by Peercoin and PIVX, for example, but not yet by Bitcoin or Ethereum[1].

- Delegated Proof-of-Stake (DPoS) involves users voting for a set of node operators, with their holding of cryptocoins giving them votes. The node operators then take turns to create the next block according to a schedule that may be shuffled periodically. DPoS is used by EOS and BitShares.

Use Of 'Smart Contracts'

Cryptocurrencies vary in the extent to which the system provides functionality to securely embed agreements in code that will execute when the system

[1] Although Ethereum has been working on plans to move to a form of PoS over time.

recognizes conditions have been met. For example, the language provided by Ethereum to write such contracts is very well developed. In contrast, Bitcoin script is an incomplete language (intentionally with no loops) used only to define transactions, including who needs to sign a transaction.

These coded agreements typically involve transfers of the cryptocurrency. The extent to which these represent all or part of a legal contract is complex. This makes it possible to create interesting financial deals that can then influence the economic behaviour of the cryptocurrency system.

This functionality can also be used to orchestrate decision making by the community of users, making it the basis for potentially important control mechanisms.

Cryptocoin Supply

The supply of cryptocoins is important for economic reasons and there are some interesting variations between cryptocurrencies. One variation concerns when the cryptocoins are created. The three main alternatives are these:

- 'Mineable' cryptocurrencies have cryptocoins created through all or part of their lives. The emission of coins starts with the first participants joining the network. No coins exist prior to that moment.
- 'Pre-mined' cryptocurrencies have all their cryptocoins created before use begins.
- A combined approach with some cryptocoins pre-generated and others created during the life of the cryptocurrency.

Another variation in cryptocoin supply concerns the total that will ever be created. The two main alternatives are these:

- Pre-determined, where everyone knows the amount of coins that will ever be generated and no more than that can be generated (e.g. we all know that there will never be more than 21 million bitcoins).
- Flexible, where the total number of coins to ever be generated is not predetermined and can be adjusted if necessary.

The rate at which new cryptocoins are created during the life of the cryptocurrency is particularly important from an economic point of view. The two main alternatives are these:

- Predetermined supply rate is where the supply rate does not adjust to conditions. It is embedded in the cryptocurrency algorithm from the beginning and is predictable, even if it changes over time. It does not react to market conditions so is unlikely to achieve price stability.
- Flexible supply rate is where the supply rate can be adjusted to conditions to achieve certain goals (e.g. price stability, stable income for miners, parity with an asset the token represents).

Exchange Rate Control

Most cryptocurrencies have market-driven exchange rates with other currencies. However, some have their value linked to some other asset in such a way that their exchange rate is fixed or nearly fixed.

Sometimes, the cryptocoins are backed by a fiat currency, as with USD Tether (USDT), whose designers claim to have every USDT that has ever been issued backed up by the same amount of USD in bank accounts.

Acceptability

Most cryptocurrencies can be used wherever there is someone willing to accept them as payment. However, in some cases the cryptocurrency can only be used to pay for particular goods or services within a particular system, such as an online casino. This resembles credits in an online game. The price of the goods/services within the system gives the cryptocurrency a more defined value.

Single And Multiple Currencies

A blockchain-based cryptocurrency system usually has one native cryptocurrency. However, sometimes two or more different cryptocurrencies (or 'tokens') exist in one system. For example, one can be used only to pay for the services/products offered within the system while the other can be used anywhere, without limitations.

If the value of the two cryptocurrencies is linked in some way, and if one is linked to a service within the system, then this may provide another way to control the exchange rate of both cryptocurrencies.

Permission

Most cryptocurrencies are open to all. Anyone can run a node, anyone can be a miner, anyone can make contributions to the code, and anyone can hold the cryptocoins.

However, some cryptocurrencies restrict who has permission to do those things. The system is then more private.

Anonymity And Privacy

With cryptocurrencies it is common to be able to see the transaction histories of all users. This is unlike typical payment systems, where we expect banks to keep our transactions private. The need to allow all nodes to verify new transactions against transactions already completed means that, usually, everyone needs to be able to see everything.

Even completely legitimate users are at risk from this because criminals can identify wealthy people as targets for theft or robbery, and perhaps understand more about their lifestyles and habits, or identify poor people as targets for tempting but illegal offers. Other reasons for wanting to keep legal transactions and wealth secret include hiding wealth to avoid being asked for gifts and hiding wealth, in a legitimate negotiating tactic.

Bitcoin tackles this problem by requiring no details of users other than the private key of any Bitcoin address they use. Whoever has the private keys has the bitcoins. This means that observers can see transactions in each address but not who owns the addresses. Unlike bank statements, Bitcoin transaction displays are baffling.

This method has been called pseudonymity. The owner's true identity is not revealed, although it is possible to see links between transactions when the same address is used more than once. In practice it is also possible to work out who really owns an address if, for example, they display it on Facebook to receive payments (e.g. donations to charity). Also, most exchanges and similar services can link real identities with Bitcoin addresses. And, of course, every time you pay someone from your address they know it's you and you know it's them.

Bitcoin users are encouraged to create new addresses for every transaction to obscure their activities and mixer services are available for people who want to hide the money trail more effectively. (A mixer service, perhaps accessed on the 'dark web' via Tor, obscures the money trail and a variety of techniques are used by different services.)

Alternative cryptocurrency designs are possible. One variation is in which transaction details are fully visible (as opposed to encrypted or not held at all). Another variation is to give some users more access than others, depending on their level of permissions.

Other designs aim to give users more complete anonymity, while others require full Know-Your-Customer procedures to establish real identities during registration to use the cryptocurrency. Different types of user may have different levels of anonymity.

Future cryptocurrencies may develop to provide a higher level of anonymity and privacy, but not from officials in law enforcement with legal permission to access the information where criteria are met. The approach a cryptocurrency takes to anonymity and privacy is an important factor influencing what types of user are attracted to it.

Mutability Of Transaction History

The typical design for cryptocurrencies is to use a blockchain in such a way that records of transactions cannot be changed once they have been fully confirmed, unless there is agreement by most of the node operators/miners.

Normally, economic incentives discourage miners from taking this step, but in a crisis they may agree to it. This happened with the second largest cryptocurrency – Ethereum. After an incident in which tens of millions of dollars were lost, most miners agreed to recreate the history from the moment prior to attack and erase the transactions connected with the hack. The Ethereum blockchain split and the minority of the miners who didn't support the move created Ethereum Classic as a new currency, although it is really the original Ethereum with the transaction history intact.

However, more routine transaction mutability might be included by design.

This is often a desired feature in private blockchains, especially where the blockchain is replacing an existing database. At some point, data from the current system have to be copied to a new, blockchain-based system. If the history is immutable and merely adding corrective transactions later is not an adequate fix, then it is impossible to correct any erroneous data that existed in the old database or any errors made copying old data to the new blockchain.

It is also possible to have a system where transactions are sometimes summarised so that details can be deleted to save space.

3.2 The Typical Life-Stories

Over 1500 cryptocurrencies have been launched so far, but many have already died or become dormant. Studying the main patterns of life and death of

cryptocurrencies tells us something about what to expect from a new cryptocurrency.

Their life-stories can be divided into four broad types:

Table 1: Life story types

	Did not gain/sustain momentum	Gained/sustained momentum
Launched without promotional effort (mostly before 'ICO' era)	**Falling Away**	**Growing**
Launched with promotional effort (mostly in 'ICO' era)	**Flash in the Pan**	**Flying Start?**

Identifying these from the history of their exchange rates is made more complicated by the tendency for cryptocurrency rates to move together[2], most likely in response to changes in Bitcoin. In particular, most currencies have a high period around 2013 and another around late 2017 but, if these are allowed for, the underlying pattern for the particular currency can be understood.

Falling Away

There were cryptocurrencies that were launched with little attention being paid, never really got started, and quietly disappeared. Also, some launched years ago achieved some distribution but now seem to be losing support.

At the time of writing, this group includes Namecoin, Peercoin, and Feathercoin. Figure 1 shows the exchange rate and transaction volumes for Namecoin, taken from the Bitscreener cryptocurrency information website (and based on the HitBTC exchange in this instance). The charts for the others named above are similar. As with Bitcoin, they enjoyed a high point in 2013, and also rose slightly during 2017, but this second rise was smaller than the first. This is consistent

[2] See https://www.sifrdata.com/cryptocurrency-correlation-matrix/

with the idea that most cryptocurrency prices are influenced by the publicity around Bitcoin, or around cryptocurrencies generally, but these less successfull cryptocurrencies are on a long term downward trend.

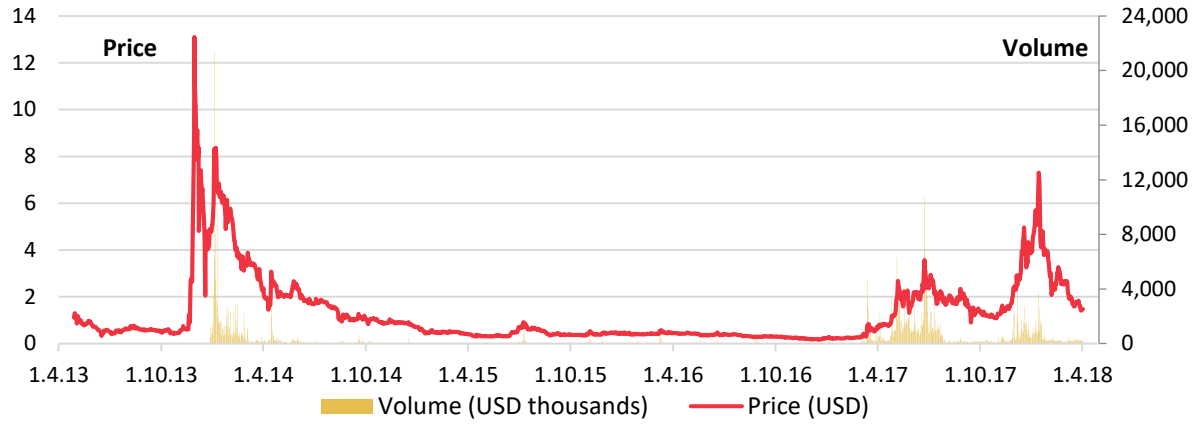

Figure 1: Exchange rate for Namecoin in USD, with volume in USD thousands. Volume data are not available prior to 27 December 2013. (Source: Bitscreener global average and total respectively.)

Growing

In terms of current market value and interest this is the most important group. It contains Bitcoin, Ether, Ripple, Litecoin, and Dash (originally known as DarkCoin). Figure 2 shows the exchange rate and volume for Bitcoin.

There are two high points: a small one at the end of 2013 and a large one at the end of 2017. In between these the price did not fall to its pre-2013 value. Instead, some momentum was sustained allowing another surge later. Other cryptocurrencies in this group show a similar pattern.

The reasons for the rapid rise and fall in price in 2013 are not clear. The FBI's closure of the Silk Road market for contraband had only a tiny effect but the problems at the Mt. Gox exchange may have been more important. The reasons for the halt of the 2017 rise are not yet clear but may be connected with the increased tendency for users to speculate on cryptocurrency prices and the fixed rate of money supply growth.

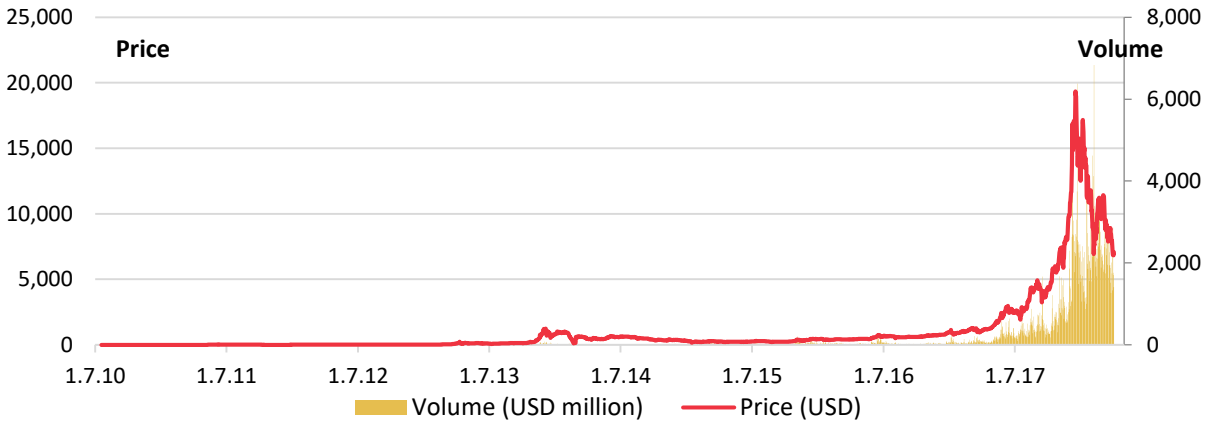

Figure 2: Exchange rate for Bitcoin in USD and volume in USD millions, from mid-2010 onwards. (Source: Investing.com global average and total respectively.)

Flash In The Pan

This group contains cryptocurrencies whose launch involved a sale of tokens, often described as an Initial Coin Offering (ICO), but in reality very different from an Initial Public Offering on a regulated stock exchange. Excluding the effects of the 2013 and late 2017 spikes, they typically achieved their all-time highest price at the time of the initial launch. These include DomRaider, Bancor, Mysterium, and Cofound.it.

Figure 3 shows the exchange rate and volume of DomRaider. DomRaider was initially pre-sold at $0.12 and there must have been people at that stage who thought it worth this much. However, by the time the coins became available and a market value could be calculated from exchange activity enthusiasm had fallen. The price on exchanges was initially between $0.05 and $0.07 and fell gradually, with just the usual 2017 rise and fall to obscure the underlying decline.

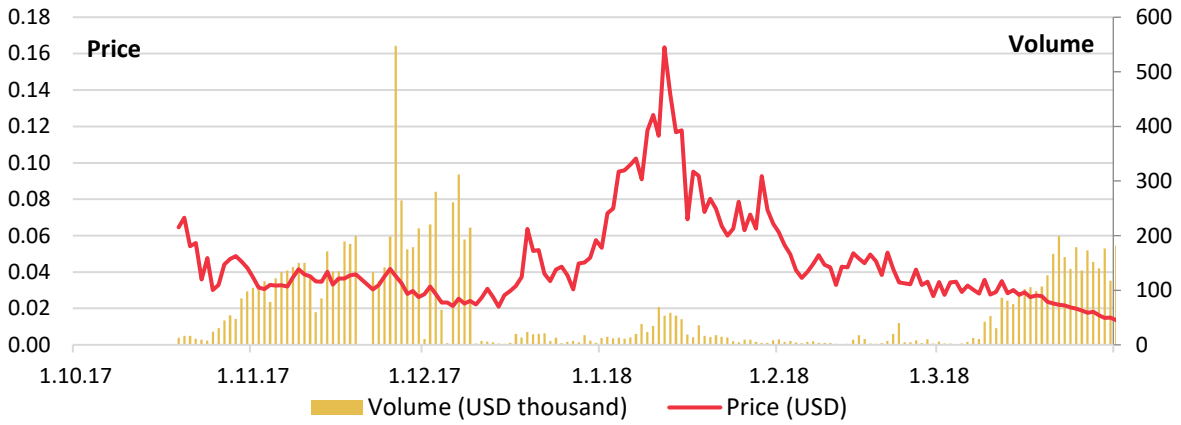

Figure 3: Exchange rate and volume for DomRaider. (Source: Bitscreener global average and total respectively.)

Flying Start?

Most cryptocurrencies using a token for funding are still in their development phase, so it is too early to say if they have sustained momentum or not. However, some cryptocoins have achieved exchange rates higher than their pre-issue sale price, providing a profit for investors who sold at the right time.

This group includes Qtum, NEO, Lisk, and Stratis.

Figure 4 shows the exchange rate and volume for Qtum. This had a price of $0.30 during its token offering and subsequently has traded much higher. Like other cryptocurrencies, it was affected by the 2017 high point.

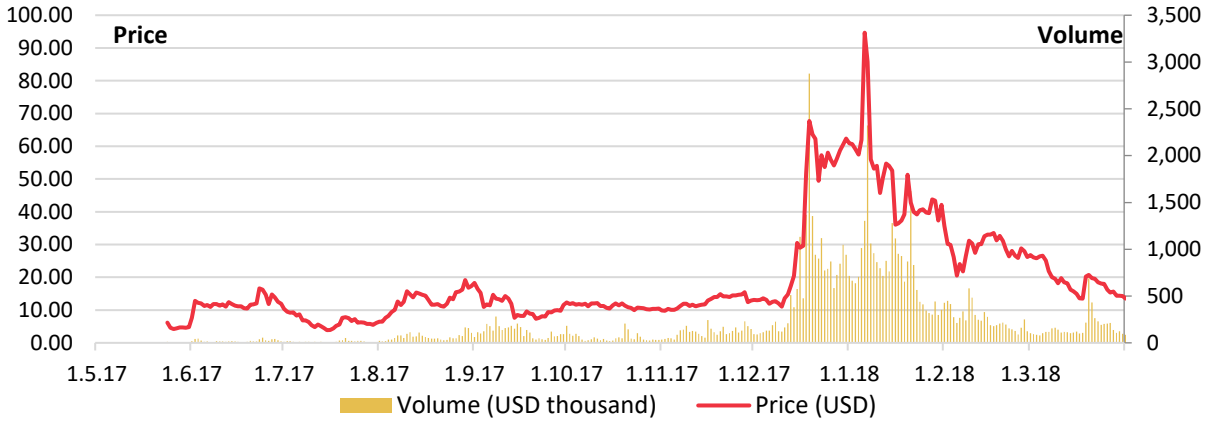

Figure 4: Exchange rate and volume for Qtum. (Source: Bitscreener global average and total respectively.)

3.3 Influences On Cryptocurrency Values And Success

Understanding what has affected the economic performance of past cryptocurrencies helps in understanding their future risks. In addition to shocking events that have occurred there are other factors whose importance and future trajectories are highly uncertain.

Publicity And Herding

Positive Buzz

In recent years the main form of activity seems to have been speculative purchasing and sale of cryptocurrencies, especially Bitcoin (Baek and Elbeck 2015, Bouoiyour et al 2014, Cheah and Fry 2015, Cheung et al 2015). The level of positive publicity around cryptocurrencies and Bitcoin specifically is likely to have been a powerful driver, along with related social media activity (Matta et al 2015).

All holders of cryptocurrencies have a vested interest in talking the price up and this may be one reason why there is a powerful positive buzz. There are also people who make a living by talking about cryptocurrencies, selling tokens, and getting advertising revenue from their YouTube content. When new cryptocurrency projects are selling tokens it is common to point to the price growth of Bitcoin and suggest that the new cryptocoin to be launched will do the same (with a risk warning somewhere in the small print).

This promotional effect spills over into most cryptocurrencies, even minor ones that are heading towards dormancy. The effect is one of the most obvious features of exchange rate charts over the past decade.

Fund Raising Efforts

In addition, cryptocurrencies involving paid-for development activity funded by selling tokens need to generate publicity and sales. This has been done through seminars, advertising, videos, websites, and multi-level marketing schemes. The result is a burst of intense sales activity focused on individuals likely to be persuaded to buy.

When that effort falls away, the cryptocurrency may or may not have enough support to continue operation.

During 2017 there were many such fund raising exercises. Most involved creating tokens on the Ethereum network complaint with the ERC20 standard for tokens. Many tokens could be paid for using Bitcoin or Ether (the main cryptocurrency of Ethereum), so the demand for these was increased.

Use As Currency And For Conversion

Another major driver is the use of the cryptocurrency for payments and for converting cash into electronic money. Sadly, the best known examples of this being done on a large and important scale are criminal.

Crime

The Silk Road marketplace was an online marketplace for the sale of contraband, mostly drugs, which could be purchased with cryptocurrencies.

Another form of crime that appears to be facilitated by cryptocurrencies, and Bitcoin in particular, is ransomware. For example, an employee launches an attachment to an email which then runs software that starts to encrypt the organization's data. The ransom demand is for money, paid in Bitcoin to a specified Bitcoin address, in return for the data being decrypted. As law enforcers have become more skilled at following Bitcoin as it moves between addresses the anonymity of Bitcoin has become doubtful.

Recently, Europol and the Metropolitan Police reported (Corcoran 2018a and 2018b) that criminal activity seemed to be leaving Bitcoin and transferring to Monero, ZCash, and Dash because of their greater efforts to block authorities from tracing money.

Money laundering is another major concern and it has been observed that drug dealers in some areas have sold near to ATMs that receive cash and turn it into Bitcoin. This lessens the dealer's risk of being robbed by other criminals (Corcoran 2017).

Few legitimate goods are advertised with cryptocurrency prices. More often, when cryptocurrencies are accepted as payment, it is on the understanding that the fiat currency price advertised will be converted at the time of paying.

Legitimate Uses

Nevertheless, when a large company announces that it will accept a cryptocurrency (usually Bitcoin) as payment this usually boosts the exchange rate, and when a large company announces that it will stop accepting cryptocurrency that reduces the rate.

However, in future improved cryptocurrencies with greater efficiency and appropriate privacy features can be genuinely competitive as payment systems, making use in legal purchases a factor driving demand.

Purchase of goods and services is not the only use found for cryptocurrencies. Dogecoin, which was started as a bit of a joke, has an enthusiastic community and has been used repeatedly for raising money for charitable causes as well as becoming a currency for tipping. Cryptocurrencies are also used on gambling and gaming sites.

Shocking Events

The upward push created by excited publicity and sales activity is countered from time to time by shocking events that can halt cryptocurrency exchange rate rises.

Arrests

The arrest in 2013 of the people behind the Silk Road market place for contraband goods was an early and well known shocking event. More recently, the exchange BTC-e was closed in July 2017 when the US Department of Justice arrested staff members and seized server equipment.

Such events can have a surprisingly small and short lived effect. Figure 5 shows the immediate effect on Bitcoin prices of the Silk Road arrest and closure.

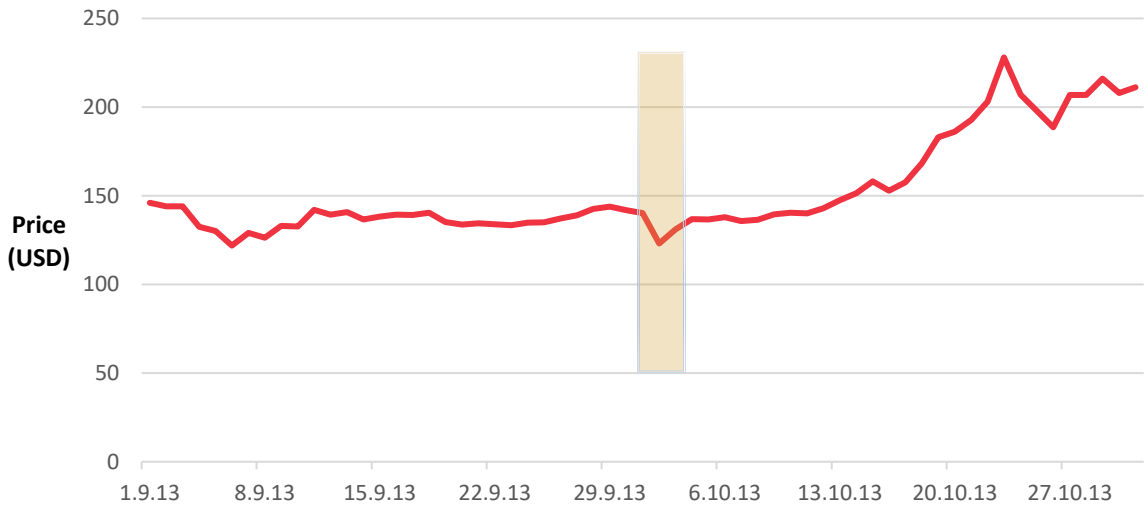

Figure 5: Bitcoin prices in USD for September and October 2013. The effect of the Silk Road crisis is the downward blip starting on 2 October 2013 and over by 5 October 2013. (Source: Investing.com global average.)

Thefts By Hacking

More recently a series of hacks and thefts from cryptocurrency exchanges has occurred. Table 2 lists some of the attacks with approximate values taken from news reports.

Table 2: Hacks on exchanges.

Exchange	Date	Approximate value taken
MtGox	February 2014	850,000 BTC (200,000 BTC was found later)
Bitstamp	January 2015	19,000 BTC
Bitfinex	July 2016	120,000 BTC
Youbit	April and December 2017	4,000 BTC in April, value for December not available.
NiceHash	December 2017	$64 million
Coincheck	January 2018	523 million of NEM coin, then ≅ $500 million
Coinrail	June 2018	Around £28 million.
Bithumb	June 2018	$31 million

These involved conventional attacks on computer security to obtain users' keys rather than cracking the cryptocurrency itself.

The effect of such hacks on cryptocurrency prices tends to be surprisingly brief. Figure 6 shows the effect of the Mt. Gox theft in February 2014. On 7 February the exchange suspended withdrawals of Bitcoin and then on 24 February the exchange closed completely. At the time Mt. Gox was a very important exchange for Bitcoin and the exchange initially blamed the problem on fundamental security problems with Bitcoin itself.

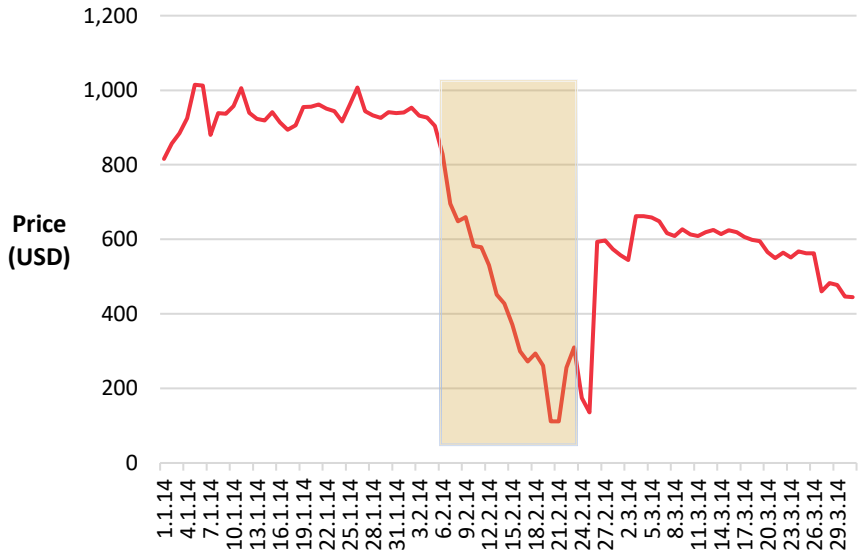

Figure 6: Bitcoin prices in USD during February 2014. The tinted box shows the key period. (Source: Investing.com global average.)

Exchange Failures

Even without thefts, cryptocurrency exchanges tend to be short lived. Moore and Christin (2013) studied 40 Bitcoin exchanges up to January 2013. Of these, 18 had already closed. Their analysis showed that more popular exchanges (with more users and transactions) tended to last longer but were more likely to be hacked.

Regulatory Prohibition

Most recently, China's decision to ban exchanges, financial institutions, and payment processors from handling cryptocurrencies has been a major setback as this was an important territory for cryptocurrencies. When China acted in September 2017, the price of Bitcoin dropped from around USD 5,000 to around

USD 3,000. Cryptocurrencies are also banned in Bangladesh, Equador, Bolivia, and Morocco (Carney 2018).

Restrictions On Advertising

In 2018, Google, Facebook, and Twitter banned advertisements relating to cryptocurrencies, along with advertisements for other unregulated financial products. As these are the most powerful internet advertising platforms, this is likely to have a considerable effect and was received very negatively by those involved with cryptocurrencies.

Hard Forks

When the community that supports a cryptocurrency is unable to agree on the technical solution to a major problem, the community can split into two, each supporting its own copy of the blockchain with its own chosen technical solution. Holders of cryptocoins on the original blockchain now find they are also holders of similar coins in a new one.

The effect on exchange rates depends on the psychology of holders and the extent of support for each of the two blockchains. Typically, one blockchain has vastly more support than the other. Sometimes the hard fork is hardly noticed because its support is so low. Users tend to welcome the idea of getting more coins and prices often rise before a hard fork.

However, if the community is more equally split by the disagreement this can create uncertainty and fear that pushes the exchange rate down before the hard fork.

Discovery And Resolution Of Technical Issues

Technical issues typically concern security or performance. Performance issues tend to grow in importance over time as a blockchain grows and its community grows. Security issues are more often recognized quickly once someone publishes details or an attack occurs. This can cause panic among users.

Most issues involve wallets or other applications. However, issues sometimes involve the cryptocurrency itself. The revelation that Bitcoin transactions were ‘malleable’ (i.e. transaction details could be changed to some extent despite being digitally signed) was significant. Partly to solve this, SegWit (i.e. segregated witness, a technique for separating transaction details and signatures more effectively) was introduced.

SegWit was also an attempt to improve Bitcoin's limited capacity and slow confirmation times by increasing the size of blocks. A further development called the Lightning Network aims to make a much bigger contribution to capacity and speed, but is still in development.

Dishonest Trading

This category includes insider trading, which does not necessarily have a large effect on prices, and market manipulation.

As examples of potential insider trading, people working closely with cryptocurrency exchanges have insider knowledge that they can exploit in the following situations:

- When a decision is made to list a cryptocurrency for the first time but this has not yet been announced. (This is particularly important for the price of newer cryptocurrencies being listed on a major exchange.)
- When a decision is made to cease listing a cryptocurrency on an exchange but this has yet to be announced.
- When a hack has taken place at the exchange but the announcement has yet to be made. (These events cause rapid loss of value so it is very helpful to be able to sell before the hack is announced.)

Market manipulation is exemplified by the 'pump and dump' method, which is more feasible with smaller coins (by total market value). The manipulator pushes the price up by buying the cryptocurrency on various exchanges and using online communication channels to create a positive buzz around it. When the price is higher they can sell and take their profit.

Other Economic Indicators

There have been several academic studies trying to determine the drivers of Bitcoin's exchange rates empirically. Some of these have included economic variables such as interest rates, other exchange rates, and stock market indices in the models used.

However, results are inconsistent and the models tend to be complicated and their results hard to interpret confidently. Macroeconomic variables are relevant or not depending on what other variables were included in the analysis,

what model was used, and probably also depending on when the study was done.

Liquidity

Compared to typical fiat currencies, cryptocurrencies tend to have low liquidity (Greene and McDowall, 2018), and this can be particularly noticeable on individual exchanges. Exchange prices even for Bitcoin show significant differences most of the time due to costs and risks that make arbitrage challenging (Kroeger and Sarka, 2016).

It is likely that liquidity and prices are linked, but there will be other reasons also for the tendency for higher prices to coincide with higher levels of exchange activity.

Design Features

In principle, the design of cryptocurrencies should be crucial to their success. In section 3.1 we reviewed some of the main design differences between cryptocurrencies.

In practice, the connection is not obvious. Reasons for this probably include the gulf in understanding between cryptocurrency users and developers, and the fact that even experts disagree vigorously about what features are desirable.

4 Method A: Control Through The Cryptocurrency Lifecycle

This is the first of three analysis methods used in this report. It focuses on the changes to control priorities through the whole life of a cryptocurrency.

This section looks at controlling the overall undertaking of a cryptocurrency, from the perspective of its initiators. What should they focus on and how do those things change as the cryptocurrency goes through the stages of its lifecycle?

The analysis is simple and high level, but tries to capture crucial changes of priority over time. This form of analysis is different from, but complementary to, the others used in this report.

Key points emerging from this are the importance of very early technical choices, and the importance of thinking ahead to the potential end of the cryptocurrency rather than just letting it end in chaos or apathy. Since most cryptocurrencies launched so far in history have fizzled to nothing, the eventual end within just a few years is more than likely.

The lifecycle used has three main phases, each divided into stages (Figure 7).

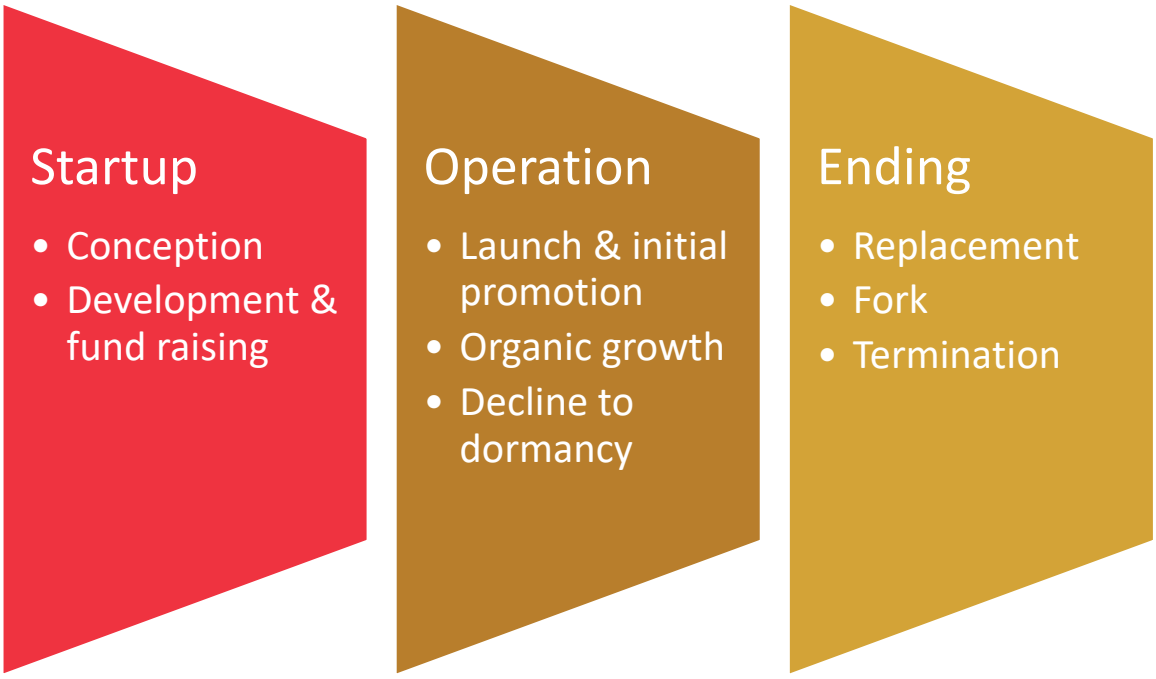

Figure 7: Cryptocurrency lifecycle phases and stages.

For each stage, high level control priorities have been listed (Table 3). This form of analysis helps to highlight stages that tend not to get so much attention, such as those towards the end of life.

Table 3: Control priorities at each lifecycle stage.

Stage	Control priorities
PHASE 1: STARTUP	
Conception	Choose key features for efficiency and to avoid attracting crime. Get the right people involved – people who are control-focused and intolerant of crime.
Development and fund raising	Be honest to investors, if investors are involved. Give investors reasons to trust that their money will be well spent. Get the design details right. Run an effective development project with strong quality assurance.
PHASE 2: OPERATION	
Launch and initial promotion	Effectively promote (encouraging use). Ensure all necessary ecosystem components are functioning adequately by launch day. Issue cryptocoins correctly, especially if exchanging for some other token issued earlier. Control funds received from issue of cryptocoins, if any. Monitor and manage system performance. Respond to any crisis.

Stage	Control priorities
Organic growth	Ensure that any additional ecosystem elements are functioning adequately when launched. Monitor and manage system performance. Control any technical changes. Respond to any crisis.
Decline to dormancy	Choose correctly between continued promotion in order to revitalize the cryptocurrency and managing the end of the cryptocurrency. Promote the cryptocurrency efficiently (perhaps with dwindling resources).
PHASE 3: ENDING	
Hard fork (users have to update their software to keep using the cryptocurrency)	Reliable software that performs as designed. Make any related software changes in a coordinated way. Users and miners/node operators understand their choices. Ensure an adequate developer community exists to maintain the cryptocurrency or cryptocurrencies that exist after the hard fork.
Replacement	Develop an alternative cryptocurrency and offer it in exchange for the cryptocurrency being replaced.
Termination	Withdraw all elements of the cryptocurrency infrastructure with minimal loss to cryptocurrency owners as a direct result. Prevent purchase of the cryptocurrency when it is failing.

5 Method B: Distinctive Characteristics And Their Control Implications

This is the second of the three methods of analysis used in this report. It focuses on the controls required to be in and around the cryptocurrency itself (not the whole programme). It takes the perspective of a person designing the cryptocurrency systems.

The method of analysis is to deduce characteristics of the required control scheme by thinking about what is both important and distinctive about the system, compared to other systems. Making these deductions involves thinking deeply and using experience, knowledge, and some creativity.

The distinctive characteristics are really just the most obvious points one wants to make to describe the system. Here is a paragraph that does that. In the tabular analysis later we break this paragraph into individual components.

A cryptocurrency is a form of money implemented electronically using cryptographic techniques, distributed databases, often operating internationally, usually with the cooperation of many people. Past and existing cryptocurrencies have been attractive to some criminals, among others, and some people interested destruction.

5.1 Inferences From The Distinctive Characteristics

A Form Of Money

Consequently, it is a highly desirable, easily moveable asset (when working properly) and a natural target for crime. People with money in mind tend to become a little more self-reliant and less cooperative with others. Work in finance tends to attract people with a strong money focus. There are also long established patterns of crime involving money, such as counterfeiting.

> *Obviously, controls will be needed to limit access to the money, to block theft and other forms of money crime, and to detect and respond to antisocial behaviour that is moving towards criminal.*

To function as money a cryptocurrency needs to be successful in acquiring and keeping a large group of users, become exchangeable for other currencies on exchanges with adequate liquidity, and maintain a fairly steady exchange rate that does not glide down to zero and stay there.

> *To be successful in this economic role requires a system that is able to adapt to changing usage of the currency and other events. This will control the money supply and, potentially, other parameters, probably automatically. It may also be important to control the level of promotion of the cryptocurrency, particularly in its early years, and this may need more human intervention. Also, the resource efficiency of the system will need to be at least adequate at launch and improve over time to remain competitive with other payment systems, so some mechanisms for achieving this are needed.*

Money has a long history of regulation and is, typically, regulated strictly. Also, money is associated with taxation, with taxes usually being calculated from money amounts and paid with money. A rise in regulation of cryptocurrencies and stricter tax treatment is very likely as authorities respond to the increasing financial significance of cryptocurrencies.

> *Control features of cryptocurrencies will, increasingly, need to meet the specific requirements of regulations and tax laws. For example, anonymity might be prohibited along with features that allow anonymity.*

Implemented Electronically

As an electronic system it is a potential target for cyber-attacks, potentially using significant computer power and sophisticated software, perhaps developed over time by a community of hackers and professional criminals. Social engineering is also likely and, with many distributed users, a serious threat.

> *Security needs to be built into the cryptographic design of the cryptocurrency, into the tools used to manage it, and (if possible) enforced in some way across the computers and networks involved.*

As an electronic payment system a cryptocurrency can, potentially, attain very high velocity (i.e. its coins can be used over-and-over at a high rate). This increases the challenge of controlling its money supply and maintaining a reasonably stable value. A further potential challenge is that some users may automate their transaction decisions to speed them up, even using artificial intelligence techniques whose decisions are opaque to everyone, but still made very quickly.

Having said that, if confirmation times are slow for a cryptocurrency then its velocity may be less than for currencies moved using conventional electronic payment methods between banks.

> *This again underlines the importance of building monetary control into the design of the cryptocurrency and making it automatic and adaptive.*

Electronic implementation means that the payment system should be more resource efficient than notes and coins, but it does not necessarily mean that the cryptocurrency is more resource efficient than electronic payment systems that do not use a blockchain. The notorious inefficiency and electricity consumption of Bitcoin is an illustration of the problem. Inefficient processing and slow confirmations should be predictable long in advance from the basic design of the cryptocurrency and the number of nodes used, and should be something that can easily be monitored over time.

> *Controls to ensure the cryptocurrency is adequately fast and resource efficient should be built into the initial design, with other controls in place to monitor performance over time and trigger further adjustments to maintain efficiency if needed.*

Using Cryptographic Techniques

Particular forms of control are the objective of cryptographic techniques, providing identification, preventing tampering, and keeping information secret for example. The skills needed to develop and implement these for a cryptocurrency are often available and may even be volunteered or subsidised as academic research work. Software libraries and existing blockchain services exist with which a cryptocurrency can be built quite quickly, though innovations will take longer.

> *All this points to heavy use of cryptographic techniques in cryptocurrencies, as one would expect.*

Cryptographic techniques offer the possibility of systems that are hack proof, or at least whose weaknesses can be probabilistically quantified. However, mistakes can be made and even without them a very lucky guess can break security. When that happens confidence in a cryptocurrency is badly damaged. Mistakes may arise from unrealistic assumptions made, often involving human nature or how the stakeholders of a system will change over a long period of time. Systems of ‘smart contracts’ implemented to provide novel features of a

cryptocurrency might have unforeseen implications, especially when deliberately exploited. The same might be true for governance mechanisms designed to ensure fair decision-making by stakeholders that later turn out to allow someone to take complete control.

> *The approach to quality assurance (QA) of proofs and other studies of mechanisms needs to go beyond some of the limited proof techniques used in some past examples and include itemisation and challenge of every assumption, perhaps some element of war gaming, or simulation, in addition to conventional software QA techniques.*

Although cryptographic skills are often in good supply in this field, the systems and their logic are complex and the skills are niche. It is possible for the people designing a cryptocurrency to find that they are increasingly reliant on a small number of people (perhaps just one person) who seems to understand it all but perhaps does not.

> *To combat this, design and proof documents should be written in an accessible style (e.g. plain English to explain the mathematical proofs), with a planned minimum number of people involved, whose understanding is carefully checked and monitored. Exercises like itemising assumptions made in designs and proofs should be done so that anyone with a reasonable understanding of cryptocurrencies and human nature can review them.*

Although the skill to devise cryptographic control mechanisms is a crucial asset, it has limits. Other control mechanisms are needed, backed by a willingness to use them.

> *Teams that devise cryptocurrencies should include an adequate number of people with a good understanding of regulation, economics, and conventional control mechanisms, along with the expected expertise in cryptographic techniques.*

Distributed Databases

More copies of the database mean more copies to store, more copies to be synchronized, more network traffic, and increased costs from duplicated programmed controls (e.g. proof of work – in systems where the number of miners is related to the number of copies).

To keep resource efficiency in a tolerable range it is probably necessary to avoid some of the most resource intensive control mechanisms (e.g. proof of work) and constrain the number of copies.

To be an honest node, the node needs to be running the correct, honest software that follows the rules of the consensus algorithm. More copies of the database require more servers to be secured and patched with the correct, honest software, more security administration people to be guided, and more work in enforcing basic computer security requirements.

As far as possible the security design of the system should be proof against some servers being insecure. The overall security level should not be a function of the weakest link. (This is typical of cryptocurrencies already.) Depending on other design choices, it may also be helpful to build some monitoring of security policies into the node software. A node running on a platform with an easily identifiable security weakness might then be flagged up by the cryptocurrency software.

A fundamental design goal for cryptocurrencies based on blockchains is to minimise the risk of one party gaining control of block formation in such a way that money can be double spent.

An effective mechanism for this is required in all cases.

Mechanisms to distribute software and data across the network of nodes and users are standard features.

These mechanisms also provide an opportunity to monitor security policy adherence across many servers.

Often Operating Internationally

The ability to transfer money internationally, quickly and cheaply, is a good commercial opportunity for cryptocurrencies. However, operating internationally brings a number of challenges. It may be that, if a legal case is begun, it is not clear which country's laws are applicable.

Expert legal advice is needed and may result in requirements for a range of contractual terms to be agreed by participants.

The cryptocurrency needs to comply with the laws of all countries where it is used. Its fundraising will likely also need to comply with the laws of all countries

where money is raised or received. The more countries are involved the tighter the overall set of constraints, with the theoretical possibility of mutually incompatible laws being faced. For example, weak or non-existent Know Your Customer procedures might be acceptable in one country but not in another.

> *Again, expert legal advice is needed and may result in requirements for legal contracts to be agreed, and potentially for the cryptocurrency to be available only in some jurisdictions. Fund raising may also need to be controlled so that only investors in some countries are allowed to participate.*

Cryptocurrency designers thinking about the future and making assumptions about how participants will behave may be influenced by un-noticed cultural assumptions that are not met in some countries. What one person thinks would never happen might be a tradition somewhere else, waiting to be translated into the cryptocurrency world.

> *Again, cryptocurrency design assumptions need to be itemised, properly explained in plain language, and reviewed by a wide range of people.*

Internet infrastructure in some countries might be so slow, or so constrained by national firewalls, that nodes located in those countries cause persistent confirmation delays.

> *This suggests that the ability to restrict the locations of nodes may be needed.*

Usually With The Cooperation Of Many People

One typical characteristic of cryptocurrency communities is a desire for digitally controlled cooperation. The rules are built into, and enforced by, the software system. This applies not only to block formation but possibly also to decisions about parameters of the system, and even to decisions about technical changes to the system. These mechanisms tend to cope best with decisions that are routine and predicted, and are more likely to struggle with very difficult decisions where people try harder to get their way.

> *Although the preference for automatically controlled cooperation is an interesting and attractive feature that should be prominent in the control scheme, the set of governance mechanisms needs the ultimate level of decision-making that can cope with completely unexpected decisions.*

With cryptocurrencies there is usually an initial design phase where central designers have control, after which the set of stakeholders expands.

> *It will usually be much easier to design control into what is initially launched than to persuade people to accept changes later.*

A commercial development team, with a boss and a payroll, may find its workforce more reliable than a group of volunteers. With volunteers, when disagreements arise or people feel things are going badly, their effort and cooperativeness can drop quickly.

Attractive To Some Criminals

Forms of crime to consider include fraud, contraband transactions, extortion payments (including ransomware), money laundering, tax evasion, funding terrorism, getting around international sanctions, and simply stealing cryptocoins. Fighting crime is one of the most important and potentially most costly areas for control of a cryptocurrency. Without it governments may decide that a cryptocurrency is not acceptable and either close it down or deny it access to exchanges and other ecosystem elements it needs.

Features that encourage crime include anonymous account details, giving ownership of coins to whoever has the key, multiple accounts per person with accounts created for every transaction, online services that make it much harder to trace the movement of funds between accounts, other anonymization services, exchanges making it possible to turn cryptocurrencies (e.g. gained from cyber extortion) into fiat currencies, and an international network. Many of these features can be designed out.

> *Features that facilitate crime will probably need to be designed out from the start, with features that restrict or discourage crime being included.*
>
> *The design/development team for a cryptocurrency needs to be dominated by people intolerant of crime.*

Without the right kind of privacy, criminals can identify wealthy people and even identify their transactions, then use that information to target them as victims. The criminals might steal money or use information about legal but embarrassing transactions for blackmail. A practical difficulty that will need clever technical solutions is to distinguish between the privacy that hinders crime by preventing criminals from targeting innocent people and the privacy that allows criminals to hide their activities.

> *Privacy mechanisms need to be designed in that allow legitimate control while blocking snooping for criminal purposes.*

Token fund raising schemes provide opportunities for fraud. Unlike issues of company shares on a recognized and regulated stock exchange, token offerings have been largely unregulated and the tokens usually provide the owner with very little legal power. The investor does not own a piece of a company and usually has no voting rights. The fund raisers could just take the money and not spend it on software development. Selling has sometimes involved multi-level marketing schemes and, where the commissions seem to be much more important than the value of what is being sold, there should be a suspicion of a pyramid scheme (SEC, 2013). The SEC has even set up a chillingly realistic fake ICO site for its fictitious HoweyCoins (SEC, 2018). If you click to buy some you are taken to an educational website.

> *The promotion/fundraising team for a cryptocurrency, if there is one, should be dominated by people intolerant of fraud, including pyramid schemes. The promotion/fundraising approach should be honest and legitimate, and probably should minimise even superficial similarities with methods that now have become tainted by association with fraud or suspected fraud.*

And Attractive To Some People Interested In Destruction

Most of those interested in cryptocurrencies have had straightforward economic reasons, such as speculating on exchanges or trying to create payment services better than those currently offered by established payment systems. Those endeavours, if successful, could have revolutionary effects and could lead to the failure of some organizations currently using more established technology. Despite the potential disruption, most people would probably welcome this as progress for societies overall.

Many interested in cryptocurrencies have had uncontroversial social motives, such as providing affordable electronic payment and banking services to people who otherwise would not be served by banks.

However, some have had political motives that were either controversial or threatening. They have dreamed of undermining governments, fiat currencies, national banks, and the traditional banking system generally, not as an economic strategy but as a political act.

The design/development team for a cryptocurrency should be dominated by people not influenced by this kind of political ambition or by rhetoric motivated by it, particularly around issues like anonymity and taxation.

The controls built into a cryptocurrency influence who chooses to use it. A cryptocurrency with features that support regulation is likely to be unattractive to criminals and also people aiming for political revolution.

The features that support good regulation should be built in from the start as far as possible so that honest users are attracted and dishonest users are put off.

5.2 Summary Of Implications For Control

The implications for controls arising from the reasoning above can be summarised under levels of a control scheme. This is just one possible structure. More detail will come from the later analysis of stakeholders and their decisions.

Organization

- In teams that devise cryptocurrencies, include an adequate number of people with a good understanding of regulation, economics, and conventional control mechanisms, along with the expected expertise in cryptographic techniques.
- Ensure that the design/development team for a cryptocurrency is dominated by people intolerant of crime and not influenced by political ambition or by rhetoric motivated by it, particularly around issues like anonymity and taxation.
- Ensure that the promotion/fundraising team for a cryptocurrency, if there is one, is dominated by people intolerant of fraud, including pyramid schemes.
- Get expert legal advice, which may result in requirements for a range of contractual terms to be agreed by participants.

Procedures

Monitoring Procedures For Commercial Performance And Process Performance

- Monitor and respond to the resource efficiency of the system (in comparison with other payment systems).

Promotional/Fundraising Procedures

- Design an approach to promotion/fundraising that is honest and legitimate, preferably minimising even superficial similarities with methods that now have become tainted by association with fraud or suspected fraud.

Operating Procedures

- Implement controls to detect and respond to money crime and behaviour moving towards crime.
- Control the level of promotion of the cryptocurrency, particularly in its early years, to maintain a steady exchange rate.

Development Procedures

- Within QA of proofs and other studies of mechanisms, include itemisation and challenge of every assumption, and perhaps some element of war gaming, or simulation, in addition to conventional software QA techniques.
- Write design and proof documents in an accessible style, with at least a planned minimum number of people involved, whose understanding is carefully checked and monitored.
- If necessary, control fund raising so that only investors in some countries are allowed to participate.
- Publicise features that support good regulation to attract honest users and put off others.

IT Systems Including The Cryptocurrency

- Try to design control into what is initially launched rather than rely on persuading people to accept changes later.
- Implement controls to limit access to the money, to block theft and other forms of money crime, and to detect antisocial behaviour that is moving towards criminal.
- Right from the start, design out features that facilitate crime, and design in features that restrict or discourage crime.
- Implement privacy mechanisms that allow legitimate control while blocking snooping for criminal purposes.

- Implement features that support good regulation.
- To ensure that the resource efficiency of the system is at least adequate at launch, consider limiting the number of copies of the blockchain and avoiding Proof of Work.
- Control of the money supply and potentially other parameters to maintain a steady exchange rate.
- Implement control features that meet the specific requirements of regulations and tax laws, for the cryptocurrency, exchanges, wallets, and the computers running all these elements of the ecosystem.
- Build security into the cryptographic design of the cryptocurrency, into the tools used to manage it, and enforced as far as possible across the computers and networks involved. Node software should be able to detect and warn of common security weaknesses on typical platforms, providing monitoring across the network of nodes.
- Design the system to be proof against some servers being insecure.
- Design the system to prevent one party gaining control of the formation of blocks.
- If necessary, implement a mechanism to limit use of the cryptocurrency to only some jurisdictions, and/or limit nodes to just some jurisdictions.
- Implement a system of digitally enforced cooperation that is not limited to just a specific list of narrowly defined, predictable situations.

6 Method C: Stakeholder Decision Risk And Control Analysis

This is the third and final analysis method used in this report.

It is within decisions that our uncertainty about the world and especially about the future becomes important. That uncertainty – or rather our limited ability to predict – is the result of our limited knowledge of the world and our limited control of the world. If we know our fate for sure, even if it is a bad one, we face no risk. If we can control our world completely then we also know our fate for sure, even if we do not understand the world.

And so risk can be found by examining our decisions and by then considering how we can learn more, improving our knowledge, and respond in other ways, improving our control.

Those decisions will include strategically important individual choices (taken individually or linked), choices about routine operating procedures and systems, and choices about project and programme plans. The risk consequences of all these decisions are important for overall risk and success.

This section presents an analysis of risk and controls that is structured by the stakeholders in a cryptocurrency and their decisions. (These decisions include those bundled together within planning and design work.) In this way we see risk from the perspective of each stakeholder group, but in a way that also helps the initiators of the cryptocurrency understand what can be done to help other stakeholders manage their risk. This is also helpful for regulators and anyone else who wishes to evaluate a cryptocurrency and its prospects of sustained success.

In our analysis, the decisions by governments and regulators are really about all cryptocurrencies affecting their territory, whereas the decisions by other stakeholders are specific to one cryptocurrency.

This stakeholder and decision perspective is more detailed than the others in this report. It provides more detail about what controls to focus on and, in particular, gives insight into what data should be collected and reported about a cryptocurrency to help stakeholders deal with risk.

This analysis, again, encompasses the whole lifecycle of a cryptocurrency, not just the middle period of normal operations.

6.1 Stakeholder Decisions

Appendix A contains a table that lists all the stakeholder groups used in our analysis (summarised in Figure 8), defines and explains each one, and lists their main decisions relating to a cryptocurrency.

The decisions involved are grouped and defined to give a high level view and minimise tedious repetition. Alongside critical strategic choices there are design tasks such as those for choosing operational procedures, choosing organization structures, developing plans, and coding the details of software designs.

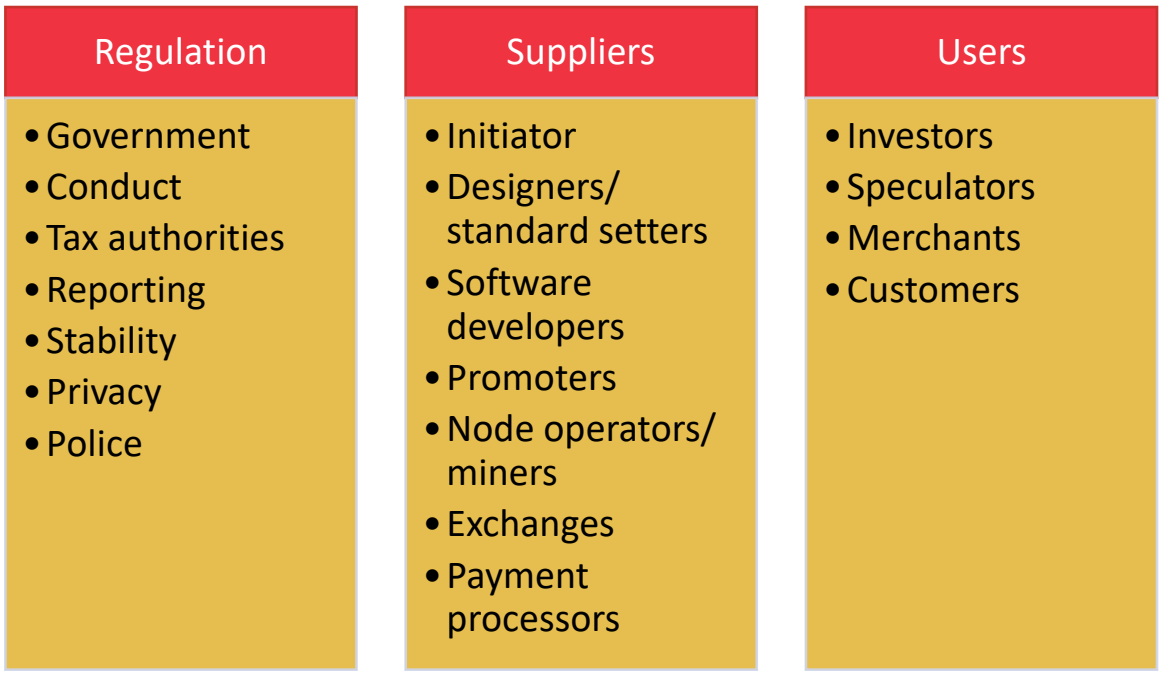

Figure 8: Stakeholders of a cryptocurrency

6.2 Decision And Risk Analysis

Appendix B analyses each of the decision types listed in Appendix A, and cross references to them. This is a substantial piece of work and provides enough detail to be helpful to each stakeholder group, as well as bringing to light ideas that can be helpful to many. The analysis (see Figure 9) works to expand on each stakeholder decision as follows.

The **'Factors Including Those That Are Risky'** column lists factors to be considered in the decision task. This is one way to structure the analysis and others are possible, but these seemed helpful.

Risk attaches to the uncertain current and future values (where applicable) of each of these factors. For compactness, the analysis does not explicitly spell out the 'risks' but the identification of factors in decisions directly implies risks.

The analysis also does not attempt to quantify or rank the significance of uncertainty around each factor. It is implied that all factors worth considering are also associated with uncertainty worth managing. Once information has been obtained to reduce uncertainty around a factor it may or may not be worth implementing additional controls to manage the remaining risk. That will only be clear once the available information has been considered.

The **'Information To Reduce Uncertainty/Risk'** column lists more specific data that might be gathered or taken from a helpful website or research report and that would help a decision-maker assess the factors in the previous column. Because these would reduce uncertainty around factors in the decision, gathering and considering them would help to manage risk and is an important part of risk management.

Finally, the **'Other Key Controls'** column contains controls of two types. (1) There are controls that should be part of the planned courses of action being considered. For example, if making a plan for software development it is usual to list a series of incremental deliveries of value to at least one stakeholder. This structure helps manage risk. Each plan under consideration should have this feature. Not every control is itemised here; just some key controls that are not completely obvious and normal. (2) There are also actions that should be taken when making the decision, such as creating a model or getting someone involved.

Where no specific suggestions are made about decision-making methods then use whatever methods are familiar and appropriate. At its simplest that could be a thorough conversation with a show of hands. However, that might be supported by successive rounds of investigation, listing and mapping of information, and even quantitative modelling and simulation where those involved have the skills. The approach should always include a controlled exploration of alternative events and outcomes, and their implications, reflecting uncertainty and lack of complete control.

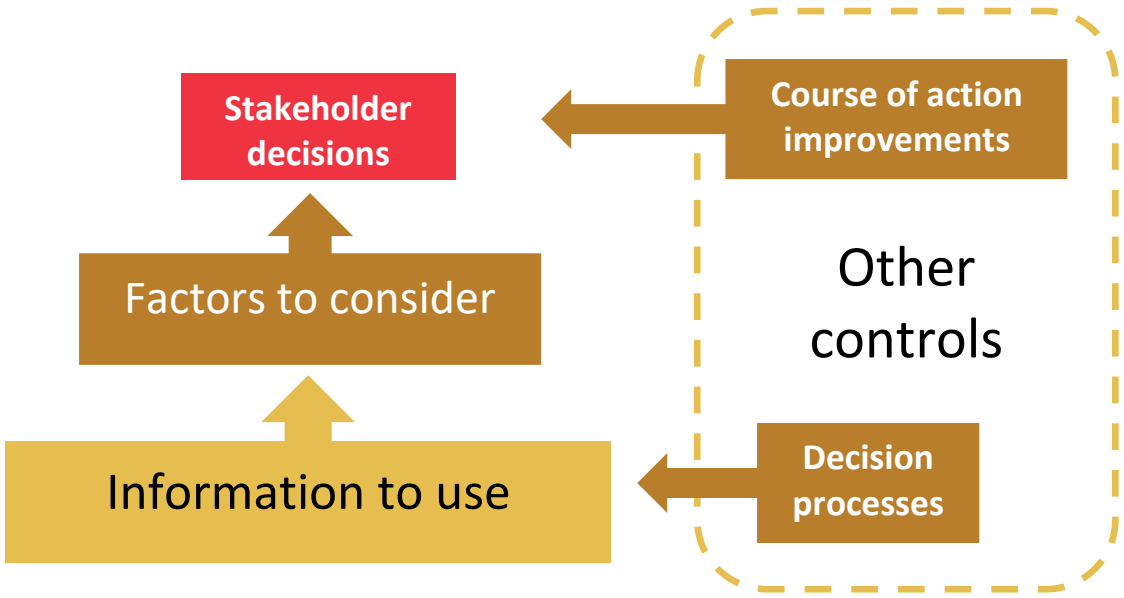

Figure 9: Method C, from stakeholders to information and controls.

6.3 Summary Of Implications For Control

Most of the control ideas in Appendix B are specific to the stakeholders concerned. The table itself is the best summary.

However, there are some items that occur more than once, and sometimes for more than one stakeholder. Many are information needs that might be met by a market quality dashboard providing statistics on the performance of the cryptocurrency or by research (either reports or a website with up to date information). Another recurring control was to use a simulation of cryptocurrency economic performance, which is something we are planning to provide.

Market Quality Dashboard For A Cryptocurrency

All values should be available as a history for download and visualized with appropriate charts.

- Distribution of holdings by size.
- Locations of users and their fiat currency needs.

- Number of cryptocurrency holders who have purchased goods/services with the cryptocurrency.
- Total market value.
- Exchange rates with moving average variability and skew.
- Transaction values and volumes – ideally separating out transactions buying goods/services from other transactions.
- Distribution of transaction values.
- Exchange rate differences between exchanges.
- Liquidity on exchanges.
- Node network monitoring information e.g. number of nodes, confirmation delays, energy consumption.

Many of these items are already provided for Bitcoin. However, there have been problems estimating how much bitcoin is in use rather than just stored for a long period, in finding the distribution of wealth across owners rather than just across accounts, and in estimating the extent to which transactions are paying for goods and services rather than doing something else.

Other Information Services

- Large scale historical research on the lives of past cryptocurrencies and past exchanges.
- More detailed historical analysis of past cryptocurrencies and launch projects. Including: funds raised, development effort needed, exchange rate history, market growth, total market value history, trading volume, any known reasons for failure.
- Fund raising performance of past projects using existing online fund raising services.
- Information about existing and proposed cryptocurrencies and other payment systems and services. Including: speed tests, costs, design features relating to security, design features relating to resource efficiency.
- Review of existing and proposed regulations. Regulatory news feed.

- Information on buying with the cryptocurrency, including: merchants accepting the cryptocurrency, and for what, products/services with prices quoted in the cryptocurrency, current cryptocurrency bargains, and savings from buying with the cryptocurrency.
- Statistics and details of criminal cases showing the harm experienced by citizens.

Simulation

- Economic simulation of the design and its monetary control mechanisms to explore stability in the face of a variety of challenges.
- Simulation of the cryptocurrency to assess prospects for value growth and trading volume.
- Simulation of the cryptocurrency to assess prospects for use as an efficient payment system.

Other Ideas

- Adopt the London Token Fundraising Manifesto.
- In many critical decisions some kind of decision modelling is suggested. Ideally the models will explicitly show uncertainty/risk, and may involve discrete risk events as well as residual uncertainty.

6.4 Economic Control Mechanisms

One crucial group of controls are those built into the cryptocurrency or its ecosystem that could work to give it a relatively stable value. It is important to think about economic controls that might be useful in future and not just those few that have be used in the past with cryptocurrencies. Here are some possibilities.

Providing Market Information

Holders/users of cryptocurrencies base their decisions in part on information about the whole market. It is reassuring to them to know that there are many other users, that they are using the cryptocurrency to buy real goods and services, that there is liquidity on exchanges, that there are merchants that accept the cryptocurrency and even goods and services advertised with stable cryptocurrency prices.

A cryptocurrency with this kind of good, reassuring news to tell could increase its stability by providing that information.

A particular problem in the past is the difficulty of distinguishing between transactions that are payments for real goods and services and transactions that are just moving cryptocurrency between addresses for some other reason.

There may even be ways to encourage users to take a long term view of the cryptocurrency through the way the data are presented.

Responsive Publicity

Cryptocurrency activity and prices seem to be strongly linked to publicity, some of which is generated by companies supporting the cryptocurrency. In theory, it might be possible to increase and decrease that publicity effort in response to price and volume trends to encourage stability.

Supply Control

One potential advantage of fully digital money is the opportunity to have very accurate, almost immediate information about the total money supply. This might allow improved control and decision-making. Some of that might be automated.

A variety of possible mechanisms exist, either adjusting the rate of minting or parameters that encourage users to hold or spend. These might be more responsive than the schemes so far used in most cryptocurrencies.

It would help to have good knowledge of the purpose of transactions (e.g. distinguishing purchases of real goods and services) and to have objectives focused on stability rather than speculation.

Linking To Real Goods And Services

There are already several examples of cryptocurrencies that can, in theory, be exchanged for pre-specified goods or services. For example, they might be exchangeable for a gramme of gold with a cryptocurrency that facilitates trading that gold. Or they might be exchangeable for a burger with a cryptocurrency that has the role of a customer loyalty scheme. Cryptocurrencies might be linked to such fundamental items of value as land (Cooper 2010) and human labour.

Taking this idea further, a catalogue of goods might be offered with prices quoted in the cryptocurrency, linking the cryptocurrency to a large basket of goods.

More generally, the more merchants advertise their goods and services in cryptocurrency prices that remain relatively stable from day to day, the more the cryptocurrency becomes attached to the real utility of the goods and services.

Exchange Mechanisms And Parameters

While cryptocurrency exchange is usually controlled separately from the cryptocurrency itself, this need not be the case and the details of cryptocurrency exchange could have an effect on the stability of prices.

A market maker can provide liquidity when an order-driven exchange contains too few orders to be effective. The market maker's price revision method could have a significant effect on the stability of rates and certainly should not be overly reactive. The difference between buying and selling prices can discourage exchange activity.

Even within an order-driven market there may be scope for subtle choices in the matching algorithm used. The level of fees affects exchange activity, as might any delays in extracting funds from the exchange. There are different ways to calculate the 'market price' for statistical purposes, which may also affect the perceived stability of prices and so affect decision-making.

Sale Of Minted Cryptocoins

With Bitcoin, a miner is, in effect, buying newly minted bitcoins by spending fiat money on computer power and joining a mining pool. In cryptocurrencies where Proof of Stake is used then your holding becomes the source of new cryptocoins. With some other cryptocurrencies it is possible to buy, using fiat currency, a token that can then be used to buy cryptocoins. In principle there is no obvious reason why newly minted cryptocoins should not be sold at an advertised price, which should have a strong effect on exchange rates (Mainelli, Leitch, and Demetis, 2018).

All these mechanisms have the effect of linking the cryptocoins to a price in fiat currency that is an alternative to exchanging the cryptocoins on an exchange.

Financial Instruments And Other Agreements

For established fiat currencies, financial instruments create market mechanisms that affect exchange rates. Interest rate changes are important, for example, and only important because loans exist. Other instruments and deals offered by

cryptocurrency promoters or communities might have hitherto unrecognised value in stabilising exchange rates.

Scale

A cryptocurrency used by more people for more purposes more often is, statistically, more stable, and more liquid. It takes longer for changes to be made by all participants and so may be faster to start reacting to developments but slower to fully react.

Promoting scale might be one of the most important mechanisms for stability, though it is clearly not enough on its own.

7 Conclusions

This research builds on previous Long Finance work on governance, audit, and standards for blockchain-based systems. It adds more detail about risk and control.

The three methods of analysis used provide different ways to develop a sensible control framework, each involving more detail than the one before it, viz. Method A: Control through the cryptocurrency lifecycle, Method B: Distinctive characteristics and their control implications, Method C: Stakeholder decision risk and control analysis,

Although the work is mostly designed to inform those who develop and promote cryptocurrencies, and regulators, the detailed work also has suggestions for many other stakeholder groups. It shows their main decisions, factors they should consider, and possible sources of information as well as other controls they will probably want to adopt.

The proposals highlight the importance of, among other things:

- Providing information to help many stakeholders;
- Exploring the economic as well as technical performance of alternative designs; and
- Considering how alternative designs would perform against a variety of challenging future scenarios;
- Ideally through experiments within simulations.

8 References

Baek, C. and Elbeck, M. (2015). Bitcoins as an investment or speculative vehicle? A first look. *Applied Economics Letters*, 22(1), pp.30-34.

Basle Committee on Banking Regulation (1998). *Framework for Internal Control Systems in Banking Organizations.* Available at: https://www.bis.org/publ/bcbs40.pdf

Bouoiyour, J., Selmi, R., Tiwari, A. (2014). *Is Bitcoin business income or speculative bubble? Unconditional vs. conditional frequency domain analysis.* MPRA.

Carney, M. (2018). *The Future of Money*. Speech given to the inaugural Scottish Economics Conference, Edinburgh University. Available at: https://www.bankofengland.co.uk/speech/2018/mark-carney-speech-to-the-inaugural-scottish-economics-conference

Cheah, E. and Fry, J. (2015). Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin. *Economics Letters*, 130, pp. 32-36.

Cheung, A., Roca, E. and Su, J. (2015). Crypto-currency bubbles: an application of the Phillips–Shi–Yu (2013) methodology on Mt. Gox Bitcoin prices. *Applied Economics*, 47(23), pp.2348-2358.

Committee of Sponsoring Organizations of the Treadway Commission (2013). *Internal Control – Integrated Framework.*

Committee of Sponsoring Organizations of the Treadway Commission (2017). *Enterprise Risk Management—Integrating with Strategy and Performance.*

Cooper, M. (2010). *In Search of the Eternal Coin: A Long Finance View of History.* Long Finance. Available at: http://www.longfinance.net/Publications/In%20Search%20Of%20The%20Eternal%20Coin.pdf

Corcoran, K. (2017). Drug dealers are laundering cash at bitcoin ATMs, London police say. *Business Insider UK*. Available online at: http://uk.businessinsider.com/drug-dealers-laundering-their-money-at-bitcoin-atms-london-police-say-2017-12

Corcoran, K. (2018a). Law enforcement has a massive problem with these 3 cryptocurrencies. *Business Insider UK*. Available online at: http://uk.businessinsider.com/law-enforcement-problems-with-monero-zcash-dash-cryptocurrencies-2018-2

Corcoran, K. (2018b). Here's how police in Europe work together against cryptocurrency crime. *Business Insider UK*. Available online at: http://uk.businessinsider.com/how-european-police-fight-cryptocurrency-crime-2018-2

Financial Reporting Council (2014). *Guidance on Risk Management, Internal Control and Related Financial and Business Reporting.* Available at: https://www.frc.org.uk/getattachment/d672c107-b1fb-4051-84b0-f5b83a1b93f6/Guidance-on-Risk-Management-Internal-Control-and-Related-Reporting.pdf

Greene, R. and McDowall, R. (2018). *Liquidity Or Leakage: Plumbing Problems With Cryptocurrencies.* Long Finance. Available online at: http://www.longfinance.net/DF/Liquidity_Or_Leakage.pdf

Kroeger, A. and Sarkar, A. (2016). *Is Bitcoin Really Frictionless?* Liberty Street Economics blog, Federal Reserve Bank of New York. Available online at: http://libertystreeteconomics.newyorkfed.org/2016/03/is-bitcoin-really-frictionless.html#.VwKEsqQrKUl

Mainelli, M. R., Leitch, M., and Demetis, D. (2018). Economic simulation of cryptocurrencies. *Digitization*, CAPCO Institute. Available online at: https://www.capco.com/Insights/Capco-Institute/Journal-47-Digitization

Mainelli, M.R. and Mills, S. (2016) *The Missing Links In The Chains? Mutual Distributed Ledgers (aka blockchain) Standards.* Long Finance. Available online at: http://www.longfinance.net/1051-the-missing-links-in-the-chains-mutual-distributed-ledger-aka-blockchain-standards.html

Mainelli, M. R. and Leitch, M. (2017). *Auditing Mutual Distributed Ledgers (aka Blockchains): A Foray Into Distributed Governance & Forensics.* Long Finance. Available online at: http://www.zyen.com/1749

Matta, M., Lunesu, I., and Marchesi, M. (2015). Bitcoin Spread Prediction Using Social and Web Search Media. In *UMAP Workshops*.

Mills, S. and McDowall, R. (2017). Responsibility Without Power? The Governance Of Mutual Distributed Ledgers (aka Blockchain). Long Finance. Available online at: http://www.longfinance.net/long-finance-report/1086-responsibility-without-power.html

Moore, T. and Christin, N. (2013). Beware the Middleman: Empirical Analysis of Bitcoin Exchange Risk. In Sadeghi, A. R. (eds) *Financial Cryptography and Data Security. FC 2013. Lecture Notes in Computer Science, vol 7859*. Springer, Berlin, Heidelberg. Also available online at: http://fc13.ifca.ai/proc/1-2.pdf

SEC (2013). Beware of Pyramid Schemes Posing as Multi-Level Marketing Programs. Available online at: https://www.sec.gov/oiea/investor-alerts-bulletins/investor-alerts-ia_pyramidhtm.html

SEC (2018). HoweyCoins ICO website. Available online at: https://www.howeycoins.com/index.html

Z/Yen Group (2017) *The London Token Fundraising Manifesto*. Available online at: http://www.longfinance.net/nstm

Appendix A: Stakeholders, Roles, And Decisions

Stakeholders	Role Description	Decisions
Initiator	• The inspiration and driving force behind a cryptocurrency's creation and launch. • Often the founders of a company backing it. • Might be lead developers or the authors of a white paper launching the design.	• Whether to create a cryptocurrency. Whether to continue. [1[3]] • The basic design features of the cryptocurrency. [2] • How to resource development and promotion effort. [3] • Method of fundraising (e.g. token issue) and detailed terms. [4] • Method of attracting volunteers. [5] • Organization structure to use (entities, locations, reporting/control lines). [6] • Plan for development and launch. [7] • Whether to withdraw at some time post-launch, how, and when. [8]
Designers/standard setters	• The wider group of people involved in designing the cryptocurrency and its eco system, but not necessarily in writing computer code.	• The basic design features of the cryptocurrency. [2] • Detailed designs for the cryptocurrency. [9] • Whether to continue with development. [1]
Volunteer software developers	• People who work on developing the cryptocurrency software or other software for the ecosystem without pay. • A very common situation, especially prior to 2017.	• Whether to get involved at all. [10] • Whether to pull out and abandon the project. [10] • Operating procedures to use.[11] • Software development plan. [12] • Software architecture (choice of languages, libraries, etc and allocation of functionality between components). [13] • Code details. [14]

[3] Numbers in brackets correspond to decision types in Appendix B.

Stakeholders	Role Description	Decisions
Software developers – node/mining software	• People paid to develop software to run a node or do mining in a Proof of Work approach. • A node might be one that just holds a copy of the blockchain, or part of it, and does validation, or it might also do mining.	• Whether to get involved at all. [10] • Whether to pull out and abandon the project. [10] • Operating procedures to use.[11] • Software development plan. [12] • Software architecture (choice of languages, libraries, etc and allocation of functionality between components). [13] • Code details. [14]
Software developers – wallet	• People paid to develop software to run a wallet. • In some cases the wallet might be something that already works for another cryptocurrency so it just needs to be modified to support the new one.	• Whether to get involved at all. [10] • Whether to pull out and abandon the project. [10] • Operating procedures to use.[11] • Software development plan. [12] • Software architecture (choice of languages, libraries, etc and allocation of functionality between components). [13] • Code details. [14]
Promoters (sales, PR, advertising)	• People paid to promote the cryptocurrency for fundraising, to encourage greater use, or both.	• Whether to get involved at all. [15] • Operating procedures to use.[16] • Promotion plan. [17] • Extent and methods of promotion (e.g. MLM, seminars, videos) for fundraising. [18] • Extent and methods of promotion for use of the cryptocurrency. [19]
Miners/node operators	• People who operate nodes and/or do mining. • The role might just hold a copy of the blockchain, or part of it, do just mining (in a Proof of Work design), or do both, or do some other task that involves collating and storing transactions.	• Whether to start mining and/or operating one or more nodes. [20] • Extent of investment in specialist equipment. [20] • If/when to stop mining/operating nodes. [21] • Operating procedures to use.[22]

Stakeholders	Role Description	Decisions
Exchanges	• People who operate a currency exchange.	• Whether to start offering an exchange service for the cryptocurrency at all. [23] • Which currency exchanges to support (i.e. pairs of currencies that will be exchanged). [23] • Method of charging for exchange service, and specific level of charges. [23] • If/when to stop offering exchange services for the cryptocurrency. [24] • Operating procedures to use.[25]
Payment processors	• People whose service is used for electronic payments, either focused on the merchants or customers. • The service for customers typically involves a smartphone app that allows payments by various means (e.g. credit card, debit card, Bitcoin). • The service for merchants typically involves the customer being redirected from the merchant's website to a page where the payment takes place in cryptocoins.	• Whether to start working with the cryptocurrency. [26] • Technically, how to design the page or app, and interface to other systems. [27] • How to hedge and on which exchange(s). [28] • How and when[4] to convert cryptocoins received into fiat currency. [28] • Whether and how to use cryptocurrency funds for additional revenue (e.g. lend, speculate). [28] • Operating procedures to use. [29]
Investors – buying tokens	• People who invest money to fund the development of a cryptocurrency and, potentially, other elements of its ecosystem. • Often done through a token fundraising scheme where electronic tokens are sold that can be exchanged for cryptocoins when the cryptocurrency is launched.	• Whether and how many of the tokens to buy. [30] • Whether and how many of the tokens to sell later. [31]

[4] Should you sell the cryptocoins just received or some others already confirmed? How many confirmations to wait for?

Stakeholders	Role Description	Decisions
Merchants	• People who sell goods and (non-financial) services and might consider accepting payment in the cryptocurrency.	• Whether to accept the cryptocurrency as a payment means and how to do it. [32] • Whether to advertise fixed[5] cryptocurrency prices, and for which products/ services. [33] • How often to revise advertised cryptocurrency prices. [33] • Whether to hold cryptocurrency for exposure to rate changes or exchange for fiat currency as soon as possible. [34] • How and where to store the cryptocoins (e.g. hardware wallet, software wallet, online wallet, exchange). [35]
Customers	• People who buy goods and (non-financial) services and might consider paying using the cryptocurrency.	• Whether to use cryptocurrency as a payment means, and how to do it. [36] • What to buy with cryptocurrency. [36] • Whether to look for and consider advertised cryptocurrency prices for goods/services. [36] • Whether to hold the cryptocurrency for exposure to rate changes. [37] • How and where to store the cryptocoins (e.g. hardware wallet, software wallet, online wallet, exchange). [35]
Holders of the cryptocurrency	• People who hold the cryptocurrency, perhaps as a result of buying tokens and then exchanging them for cryptocoins, or because they bought the cryptocoins hoping they would rise in value.	• How much to hold. [38] • How and where to buy/sell to achieve desired holding. [39] • How and where to store the cryptocoins (e.g. hardware wallet, software wallet, online wallet, exchange). [35]
Governments	• Those politicians and civil servants involved with developing policies and laws related to cryptocurrencies.	• Whether to encourage, discourage, or stay neutral on cryptocurrencies. [40] • What overall approach to take to regulation of cryptocurrencies. [40]
Financial conduct regulators	• Regulators whose main focus is protecting people from corruption in financial services.	• How to allocate regulatory effort over potential problems. [41] • Regulations to impose to safeguard market integrity. [41]

[5] The more usual method so far has been to set fiat currency prices and either quote cryptocurrency prices at the point of payment, or use an API to revise advertised cryptocurrency prices for a fixed fiat equivalent almost in real time.

Stakeholders	Role Description	Decisions
Tax authorities and legislators	• Tax authorities and people involved in making tax laws.	• How to classify cryptocurrencies, possibly depending on what people do with them. [42] • Which tax approaches to use for cryptocurrency transactions (capital gains, trading, gambling, other). [42] • How to enforce tax rules in practice. [42] • Whether to accept cryptocurrency in payment of tax. [43]
Financial reporting regulators/standard makers	• Regulators whose main focus is on reliable financial reporting.	• How to classify cryptocurrency holdings, possibly depending on what is done with them. [44] • Which accounting methods to use (fair value, cost, movements through P&L or not). [44]
Financial stability regulators and legislators	• Regulators whose main focus is financial stability of the financial system, and those involved in making related laws.	• How to apply financial stability principles to cryptocurrencies. [45]
Data privacy regulators and legislators	• Regulators whose main focus is data privacy, and those involved in making related laws.	• How to apply data privacy principles to cryptocurrencies. [46] • Who to consider responsible for privacy. [46] • How to enforce the rules cost effectively. [46]
Police/prosecutors	• Law enforcers, including lawyers who prosecute in court.	• How much to invest in people and equipment to fight crime that involves cryptocurrencies. [47] • Which tools to invest in. [47] • How to allocate resources across the cryptocurrencies. [47] • What types of crime to target (e.g. money laundering, theft, fraud, online extortion including ransomware, terrorist funding, circumventing international sanctions, contraband purchases). [47]

Appendix B: Stakeholder Decisions, Factors, And Controls

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Initiator, Designer/standard setter: [1[6]] Whether to create a cryptocurrency. [1] The ongoing question of whether to continue (during the pre-launch period).	• Competition from other payment systems. • Level of interest in whatever you propose/launch. • Technical feasibility of any new ideas included in the high level design. • Development work needed. • Ability to generate interest/buzz or partner with others who can. • Potential for fundraising or volunteer workforce. • Solvency of any legal entities relied on, in cash and balance sheet terms.	• Historical analysis of past cryptocurrencies. Includes funds raised, development effort needed, exchange rate history, any known reasons for failure. • Information about existing and proposed cryptocurrencies and other payment systems and services. • Assessment of own contacts and reputation. • Feedback from information presentations of ideas, surveys, etc.	• Prefer to go ahead only if a significant area of uncertainty has already been addressed (e.g. innovative design already coded as part of a research programme, existing community looking for a cryptocurrency to back, team of people with previous experience). • Do more analysis, mathematical modelling, prototyping, or other experiments to establish the feasibility of novel design ideas. • For legal entities, financial accounts and financial and cash flow forecasts on a suitably frequent basis. • Reviews of going concern basis.

[6] Numbers in brackets correspond to decision types in Appendix A.

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Initiator, Designer/standard setter: [2] The basic design features of the cryptocurrency.	• Implications of design features for the desirability of the cryptocurrency. • Implications of design features for cost of development. • Implications of design features for cost of operation. • Implications of design features for performance. • Implications of design features for regulatory approval/restriction. • The users/investors likely to be attracted by the design features.	• Performance and cost information on leading payment systems of all kinds. • Historical information about past crimes related to cryptocurrencies and their exchanges. • Review existing and proposed regulations.	• Focus research effort on the most significant areas of uncertainty. • Involve people with good experience and ideas. • Simple mathematical modelling of resource consumption and response times. • Economic simulation of design features. • Side-by-side comparison of cryptocurrency and other payment systems. • Inventory of readily available, working code and features to be created with new code.
Initiator: [3] How to resource development and promotion effort.	• Overall quantity of development work. • Overall cost of paid developers. • Existing pool of volunteers and their capability. • Existing online services supporting fund raising. • Existing contacts for promotion and available potential partners for promotion. • Existing contacts for fund raising and available potential partners for fund raising.	• Historical analysis of past cryptocurrencies. Includes funds raised, development effort needed, exchange rate history, and any known reasons for failure. • Fund raising performance of past projects using existing online fundraising services. • Typical pay required to retain competent developers. • Productivity of volunteers. • Details of potential cryptocurrency promotors. • Details of potential cryptocurrency fund raisers.	• Due diligence review of information about potential partners for promotion or fundraising. • Contractual terms with a code of conduct for partners (e.g. The London Token Fundraising Manifesto).

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Initiator: [4] Method of fundraising (e.g. token issue) and detailed terms.	• Features of the design for the cryptocurrency or its ecosystem that give something different to offer investors. • Amount of money wanted. • The rules in territories that might be sources of funds. • Prospects for fundraising in each potential territory. • The ethics of potential methods and terms. • Ability to control fundraising and ensure legal and ethical constraints are obeyed.	• Review of existing and proposed regulations. • Historical information about similar fundraising efforts, including amounts raised, timing, and related crime and civil cases. • The views of people already in contact who might become investors.	• Modelling to estimate likely funds raised and the implications of upside and downside possibilities.
Initiator: [5] Method of attracting volunteers.	• Time needed. • Prospects for finding capable, committed volunteers. • Confidence in the skill and motivation of volunteers found. • Other publicity advantages and disadvantages of search methods.	• Assess existing contacts. • Observe the reaction to posting a whitepaper on online forums used by the cryptocurrency community.	• Get advice from experienced experts. • Check the track record of volunteers. • Check their personal circumstances to understand who might suddenly become unavailable.

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Initiator: [6] Organization structure to use (entities, locations, reporting/control lines).	• The legal entities that already exist. • The countries where stakeholders are located during fundraising, development, and operation. • The regulations on cryptocurrencies in those countries. • Other legal considerations including personal liability and national tendency to litigate. • Desired leadership/management style/system. • Ability to keep in daily contact with people doing critical activities (for control purposes). • Ability for people working on shared tasks to be in daily contact (for productivity and coordination).	• Review of existing and proposed regulations. • Information about other cryptocurrency projects and their structures.	• Documented entities, rules, relationships, and (usually) contracts. • Get advice from experienced people who have gone through the process or have specialised knowledge of areas like law and tax.
Initiator: [7] Plan for development and launch.	• Work to be done. • Probability distribution(s) of projected time taken by the project. • Probability distribution(s) of projected cost of the project. • Confidence in delivery of the plan. • Value of deliverables if delivered on the schedule and otherwise (earlier is usually better). • Controllability of the project. • Information on progress generated by the project as it proceeds (may be crucial for maintaining support).	• As much early design detail as possible, including design options under consideration. • Historical analysis of past cryptocurrency development and launch projects. Includes any known reasons for failure. • When resources are likely to be available and how they will be located in different organizations (if they are) and naturally form sub-teams.	• Adopt a suitable project/ programme management method. • Identify the most critical uncertainties early and focus on resolving them early if possible. • Develop a plan with incremental delivery of items that are valuable to at least one stakeholder. • Try to minimise dependencies between activities. • Measure progress.

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Initiator: [8] Whether to withdraw at some time post-launch, how, and when.	• Prospects of the cryptocurrency. • Potential gains from selling a going concern, if there is one. • Possible effect on the value of the initiator's holdings of the cryptocurrency, if any. • The existence of others willing to take over, and on what basis. • Solvency of any legal entities relied on, in cash and balance sheet terms.	• Progress of the cryptocurrency since launch. • Exchange liquidity. • Size of initiator's holdings relative to the total cryptocoins issued.	• For legal entities, financial accounts and financial and cash flow forecasts on a suitably frequent basis. • Reviews of going concern basis.
Designer/standard setter: [9] Detailed designs for the cryptocurrency.	• The attractiveness and differentiation of the feature set compared to other cryptocurrencies and payment methods. • Work still required to prove properties of novel ideas (where relevant). • Work still required to implement novel ideas. • Predicted performance of the system under alternative designs. • Economic performance of alternative designs, as money.	• Analysis of the market performance of past cryptocurrencies and the reasons for that. • Surveys of potential users to find out their priorities and views. • Productivity so far. • Typical productivity for proving (where relevant), coding, and testing. • Remaining work items.	• Economic simulation of the design and its monetary control mechanisms to explore stability in the face of a variety of challenges. • Identify alternative mechanisms to use if novel ideas emerge as too difficult or flawed. • Conventional project control, or some controlled form of agile project.

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Volunteer software developer, Software developer: [10] Whether to get involved at all. [10] Whether to pull out and abandon the project.	• Trust in the initiator to be competent and honest with the developer. • Likelihood that the cryptocurrency will be a big, sustained success. • Opportunity to influence the design and/or governance. • Funds raised. • Rewards on offer. • Work needed to complete the development. • Effects on reputation that involvement in the project might have. • Experience that might be gained; things that might be learned. • Value of supporting the philosophy behind the project.	• The design decisions taken so far. • Work required from the developer. • Data on development productivity so far. • Data on the financial situation of the initiator. • Historical analysis of past cryptocurrencies. Includes funds raised, development effort needed, exchange rate history, and any known reasons for failure. • Information about existing and proposed cryptocurrencies and other payment systems and services. • Historical information about the initiator and their reputation.	• An assessment of the developer's own ability. • Prefer to go ahead only if a significant area of uncertainty has already been addressed (e.g. innovative design already coded as part of a research programme, existing community looking for a cryptocurrency to back, team of people with previous experience). • Look for independent confirmation of the financial position of the initiator (e.g. an auditor's report). • Written contract, with legal advice taken.

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Volunteer software developer, Software developer: [11] Operating procedures to use.	• Familiarity to workforce. • Confidence in the quality of the software produced. • Confidence in the security of the software produced. • Efficiency of development. • Control over elapsed time taken. • Cultural appropriateness of methods chosen.	• Review of past methods experience of workforce. • Talk to/survey workforce for their preferences. • Research studies on performance of alternative QA methods.	• Systematic documentation. • Rigorous reviews ('inspections') of requirements, specifications, proofs, and code. • The basic QA items e.g. code standards; a systematic, multi-level testing process including, perhaps, automated static testing. • Prototyping for the user interface and for early testing of cryptographic features. • An agile method of some kind, probably with incremental delivery and rolling planning. • Measurement of performance. • Change & version control; backups. • Secure access to code and data during development. • Management of people & skills.

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Volunteer software developer, Software developer: [12] Software development plan.	• Work to be done. • Probability distribution(s) of projected time taken by the project. • Probability distribution(s) of projected cost of the project. • Confidence in delivery of the plan. • Value of deliverables if delivered on the schedule and otherwise (earlier is usually better). • Controllability of the project. • Information on progress generated by the project as it proceeds (may be crucial for maintaining support).	• As much early design detail as possible including design options. • Historical analysis of past cryptocurrency development projects. Including any known reasons for failure. • When resources are likely to be available and how they are located in different organizations (if they are) and naturally form sub-teams.	• Adopt a suitable project/ programme management method. • Identify the most critical uncertainties early and focus on resolving them early if possible. • Develop a plan with incremental delivery of items that are valuable to at least one stakeholder. • Try to minimise dependencies between activities. • Measure progress.
Volunteer software developer, Software developer: [13] Software architecture (choice of languages, libraries, etc and allocation of functionality between components).	• Development effort for each possible bundle of elements. • Confidence in estimates of development effort. • Cost/freedom from licence issues. • Continued support for the each element by its originator. • Performance in operation (e.g. server load, response times). • Degree of security achievable.	• Elements already available (e.g. programs, objects, services) that the developer wants to use. • People who are familiar with the element. • Background on the developer(s) of each component/language/etc and plans for continued support. • The cryptographic design of the cryptocurrency. • Performance benchmark information for potential elements.	• Detailed security risk analysis and design.
Volunteer software developer, Software developer: [14] Code details.	• Requirements (functional and non-functional). • Efficiency of execution with chosen language/ components/etc. • Maintainability. • Testability at each stage of development.	• Likely future developments. • Security vulnerabilities identified in software components and publicised by the makers and/or monitoring services.	• Inspection of requirements and other development documents. • Coding standards.

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Promoter: [15] Whether to get involved at all.	• Trust in the initiator to be competent and honest with the promoter. • Likelihood that the cryptocurrency will be a big success. • Funds raised so far and still to be raised. • Rewards on offer. • Effects on reputation that involvement in the project might have. • Experience that might be gained; things that might be learned. • Value of supporting the philosophy behind the project.	• The design decisions taken so far. • Work required from the promoter. • Data on the financial situation of the initiator. • Historical analysis of past cryptocurrencies. Includes funds raised, development effort needed, exchange rate history, and any known reasons for failure. • Information about existing and proposed cryptocurrencies and other payment systems and services. • Historical information about the initiator and their reputation.	• An assessment of the promoter's own ability. • Look for independent confirmation of the financial position of the initiator (e.g. an auditor's report). • Written contract, with legal advice taken.
Promoter: [16] Operating procedures to use.	• Familiarity to workforce. • Confidence that inappropriate marketing claims and agreements will not be made. • Efficiency of gaining users/funds. • Control over elapsed time taken. • Cultural appropriateness of methods chosen.	• Review of past methods experience of workforce. • Talk to/survey workforce for their preferences. • Review of past crimes and criminal cases related to promoting cryptocurrencies and mis-selling generally.	• Systematic documentation. • Systematic supervision; pre-release review and approval of published text, video, audio, and scripts (if used). • Training and rehearsal of sales representatives. • Measurement of performance. • Change and version control for promotional literature and sales scripts (if used). • Secure access to user/investor data. • Management of people and skills.

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Promoter: [17] Promotion plan.	• Chosen promotion methods. • Probability distribution(s) of projected time taken by the promotion work. • Probability distribution(s) of projected cost of the promotion work. • Confidence in delivery of the plan. • Value of promotional actions taken if done on the schedule and otherwise. • Controllability of the promotion work. • Information on progress generated by the promotion work as it proceeds (may be crucial for maintaining support).	• Historical analysis of past cryptocurrency launch projects. Including any known reasons for failure. • When resources are available and how they are located in different organizations (if they are) and naturally form sub-teams.	• Adopt a suitable project/ programme management method. • Identify the most critical uncertainties early and focus on resolving them early if possible. • Develop a plan with incremental delivery of items that are valuable to at least one stakeholder. • Try to minimise dependencies between activities. • Measure progress.
Promoter: [18] Extent and methods of promotion (e.g. MLM, seminars, videos) for fundraising.	• Ethical requirements of the initiator. • Regulatory compliance. • Ability to execute in the time available and to raise the required quantity of funds. • Cost of fundraising (e.g. commission payments). • Incentives for promoters.	• Past experience of similar fundraising. • Existing contacts/networks. • Most popular social media for cryptocurrency investors. • Review of past crimes and criminal cases related to promoting cryptocurrencies and mis-selling generally.	• Adhere to the London Token Fundraising Manifesto. • Spreadsheet to calculate costs. • Written scripts for telesales. • Recording of telesales conversations and online chats.
Promoter: [19] Extent and methods of promotion for use of the cryptocurrency.	• Ethical requirements of the initiator. • Regulatory compliance. • Cost effectiveness. • Locations and languages of intended user groups.	• Past experience of similar promotion. • Existing contacts/networks. • Most popular social media for cryptocurrency users.	• Adhere to the London Token Fundraising Manifesto. • Document specific requirements for publicity material, online interactions, and events.

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Miner/node operator: [20] Whether to start mining and/or operating one or more nodes. [20] Extent of investment in specialist equipment.	• Cost of operating a node over time and/or Proof of Work processing – possibly dependent on different hardware/software investments. • Initial purchase cost of hardware and software needed. • Cost of renting the equipment. • Rewards from mining and/or operating a node over time net of costs of a mining pool (if used) – measured in a stable fiat currency. • Predictability of rewards from mining (higher if connecting to a mining pool). • Confidence that rewards from mining and/or operating a node over time will be sustained. • Confidence that cryptocoin rewards can be converted into fiat currency or desired goods/ services. • Competition from other miners/node operators for the available rewards. • Likely longevity of the cryptocurrency and prospects of sustained success. • Contractual commitments required to become a miner/node operator (if any). • The costs, rewards, commitments, and so on of other cryptocurrencies you can operate instead. • Ease of switching to another cryptocoin if necessary.	• Proof mechanisms involved, including the basis of competition with other miners/ node operators. • Enough information about the design of the cryptocurrency to work out the implications for the likely size of the blockchain, amount of network traffic, and computations needed (especially for cryptographic techniques). • Historical analysis of past cryptocurrencies. Includes funds raised, development effort needed, exchange rate history, and any known reasons for failure. • Information about existing and proposed cryptocurrencies and other payment systems and services.	• Prefer cryptocurrencies that do not have features likely to lead to legal prohibition. • Select low energy consumption hardware. • Develop a financial plan. • Measure and monitor costs and rewards over time.

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Miner/node operator: [21] If/when to stop mining/ operating nodes.	• Projected costs and rewards for the future. • The economic value of alternative uses for the same kit (e.g. operating nodes for another cryptocurrency). • Resale value of kit if you stopped using it altogether. • Legal prohibition.	• History of actual costs and rewards. • Total supply of the cryptocoins. • Information on other cryptocurrencies sufficient to evaluate the prospects of profitably mining/operating a node. • News about the cryptocurrency and related regulation.	• Continually look for incremental improvements in performance and costs.
Miner/node operator: [22] Operating procedures to use.	• Familiarity to workforce. • Security of systems used. • Efficiency of mining/node operation. • Cultural appropriateness of methods chosen.	• Review of past methods experience of workforce. • Talk to/survey workforce for their preferences. • Review of past hacks against miners/ node operators, and (especially) mining pools.	• Systematic documentation. • The basic QA items e.g. written procedures, scripting where possible, checklists, supervision. • Measurement of performance. • Change and version control; backups. • Secure access to the systems used. • Management of people and skills.

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Exchange: [23] Whether to start offering an exchange service for the cryptocurrency at all. [23] Which currency exchanges to support (i.e. pairs of currencies that will be exchanged). [23] Method of charging for exchange service, and specific level of charges.	• Prospects of the cryptocurrency measured in users, coins, distribution of holdings, transactions, distribution of transactions, and market value of cryptocoins in issue. • Likely demand for exchange between pairs of currencies. • Prospects for charging high fees (or a high difference between bid and ask prices), which may come from low competition and high variability with lots of speculative trading. • Charging method already implemented on your exchange. • Typical charging method used by competitors. • Potential for good and bad publicity for the exchange by supporting the cryptocoin. • Payments offered by the initiator to list the cryptocoin (more common with smaller cryptocurrencies). • Ease of listing and delisting.	• Locations of users of the cryptocurrency (and so their likely fiat currency needs). • Explanation of the features of the cryptocurrency, its backers, and so on. • Historical analysis of past cryptocurrencies. Includes value growth, trading volume, currencies exchanged with, exchange rate history, and any known reasons for failure.	• Assess prospects for long term operation, value growth and trading volume.
Exchange: [24] If/when to stop offering exchange services for the cryptocurrency.	• Actual level and trend of income from exchange activity. • Cost of supporting the exchange service (perhaps some accounting allocations needed). • Technical issues of the cryptocurrency. • News that might indicate that trading the cryptocurrency has become, or may shortly become, illegal or unethical. • Evidence of illegal activity on your exchange using the cryptocurrency that cannot be selectively blocked.	• Accounting information. • Cryptocurrency and regulatory news feed.	• Some kind of scrutiny of exchange transactions – perhaps automated pattern recognition.

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Exchange: [25] Operating procedures to use.	• Familiarity to workforce. • Efficiency of operations. • Reliability of operations. • Security of operations. • Legal compliance of operations. • Cultural appropriateness of methods chosen. • Similarity to other tokens.	• Review of past methods experience of workforce. • Talk to/survey workforce for their preferences. • Review of past hacks against exchanges and their customers.	• Systematic documentation. • The basic QA items e.g. written procedures, scripting where possible, checklists, supervision. • Measurement of performance. • Change and version control; backups. • Secure access to the systems used. • Management of people and skills.
Payment processor: [26] Whether to start working with the cryptocurrency.	• Prospects of the cryptocurrency measured especially in the number and value of purchase transactions with merchants. • Prospects for charging high fees, which may come from low competition. • Potential for good and bad publicity for your payment service by supporting the cryptocoin. • Ease of supporting and un-supporting the cryptocurrency as a payment method.	• Locations of users of the cryptocurrency. • Explanation of the features of the cryptocurrency, its backers, and so on. • Historical analysis of past cryptocurrencies. Includes value growth, transaction volume, transaction value, exchange rate history, and any known reasons for failure.	• Assess the prospects for long term operation and for growth in payment volume and value.
Payment processor: [27] Technically, how to design the page or app, and interface to other systems.	• Requirements (functional and non-functional), reflecting ease of use, security, reliability, and attractiveness of features. • Efficiency of execution with chosen language/ components/etc. • Maintainability. • Testability at each stage of development.	• Likely future developments. • Security vulnerabilities identified in software components and publicised by the makers and/or monitoring services.	• Inspection of requirements and other development documents. • Coding standards.

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Payment processor: [28] How to hedge and on which exchange(s). [28] How and when to convert cryptocoins received into fiat currency. [28] Whether and how to use cryptocurrency funds for additional revenue (e.g. lend, speculate).	• Time taken at the point of sale if the cryptocurrency is chosen as payment means. • Time needed to exchange for fiat currency. • Short term volatility of the exchange rate. • Fees/cost of exchange(s) under consideration. • Costs of hedging methods. • Effectiveness of hedging methods. • Prospects for gain through holding the cryptocurrency.	• History of exchange rate (including very short term volatility) and transaction values and volumes – ideally separating out transactions buying goods/services. • The design of the cryptocurrency and its actual performance so far, if known, so that confirmation times can be understood. • Information about the liquidity of potential exchanges.	• Put an upper limit on the size of transactions. • Limit time within which payment must be made (e.g. to 15 minutes).
Payment processor: [29] Operating procedures to use.	• Familiarity to workforce. • Efficiency of operations. • Reliability of operations. • Security of operations. • Legal compliance of operations. • Cultural appropriateness of methods chosen. • Similarity to other tokens and payment methods.	• Review of past methods experience of workforce. • Talk to/survey workforce for their preferences. • Review of past hacks against payment processors and their customers.	• Systematic documentation. • The basic QA items e.g. written procedures, scripting where possible, checklists, supervision. • Measurement of performance. • Change and version control; backups. • Secure access to the systems used. • Management of people and skills.

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Investor buying tokens: [30] Whether and how many of the tokens to buy.	• Prospects of the cryptocurrency – use for payments and exchange rate. • Other gains offered e.g. discounts on products/ services. • Pricing scheme for tokens including perhaps bulk discounts and/or discount for early purchase. • Commissions for introducing further buyers of the token. • How the commissions are paid (tokens or fiat currency) and when. • Indications of a potential Ponzi scheme (e.g. shady track record of promoters, focus mostly on the commissions and not on the underlying services). • Desire to support a cause behind the cryptocurrency.	• Explanation of the features of the cryptocurrency, its backers, and so on. • Historical analysis of past crypto-currencies. Including value growth, trading volume, fraud cases, and events that have killed the cryptocurrency.	• Assess prospects for long term operation, value growth and use as an efficient payment system.
Investor buying tokens: [31] Whether and how many of the tokens to sell later.	• Whether transferring tokens is permitted. • Prospects of the cryptocurrency – use and exchange rate. • Other gains possible e.g. discounts on products/ services. • Alternative investment opportunities. • Potential urgent need for fiat currency.	• Explanation of the features of the cryptocurrency, its backers, and so on. • Historical analysis of past cryptocurrencies. Including value growth, trading volume, and events that have killed the cryptocurrency.	• Assess prospects for long term operation, value growth and use as an efficient payment system.

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Merchant: [32] Whether to accept the cryptocurrency as a payment means and how to do it.	• Legal restrictions on accepting cryptocurrency in particular territories. • Prospects for additional sales due to accepting the cryptocurrency (both from the initial marketing effect and from customers looking for ways to spend their cryptocurrency). • Possible incentives offered by cryptocurrency backers to accept the cryptocurrency as payment. • Time needed for the point of sale transaction, potentially including any required confirmation period if a third party payment processor is not used and confirmation is quick. • Time needed to exchange for fiat currency. • Short term volatility of the exchange rate. • Fees/cost of exchange(s) under consideration. • Other transaction costs (e.g. from a service that takes the coins for you) for payment systems under consideration. • Performance of alternative payment systems (costs, speed, security) as experienced by you as a merchant and by customers, analysed by location. • Risk of losing the private key and hence the cryptocurrency. • Risk of having the private key stolen (potentially by an employee or outsider) and hence the cryptocurrency stolen. • Complexity of tax treatment for customers in relevant territories (e.g. UK capital gains tax is very complex to calculate because of tracking the original cost of cryptocoins spent).	• History of exchange rate (including very short term volatility) and transaction values and volumes – ideally separating out transactions buying goods/services. • Terms of other payment systems. • Speed tests of other payment systems. • Details of the design of the cryptocurrency and other payment systems (from which to assess inherent security strengths).	• Limit extent to which the cryptocurrency is accepted e.g. limit to just certain products, certain territories, a limited maximum or minimum purchase value. • Limit time within which payment must be made (e.g. to 15 minutes) to control the time period between a sale being made at an agreed cryptocurrency price and the funds being received in a fiat currency. • Use a third party payment processor who takes the risk, including exchange rate risk.

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Merchant: [33] Whether to advertise fixed cryptocurrency prices, and for which products/ services. [33] How often to revise advertised cryptocurrency prices.	• Short, medium, and long term volatility of the cryptocurrency exchange rate with fiat currencies. • Number of cryptocurrency holders looking for good deals on goods/services. • Opportunity to gain sales by giving people a chance to spend their cryptocoins on something (which advertising cryptocurrency prices would remind them to do). • Possible regulatory constraints (e.g. banning advertising prices in cryptocurrency, or requiring local currency).	• History of cryptocurrency exchange rates, including very short term volatility. • Moving estimate of the number of cryptocurrency holders who have purchased goods/services with the cryptocurrency.	• Monitor sales in cryptocurrency for each product for which the cryptocurrency is accepted as payment, especially where a cryptocurrency price was offered. • Test for an effect from offering a cryptocurrency price. • Set automated limits on cryptocurrency prices to stop large differences in value opening up. • Target cryptocurrency offers at customers known to use the cryptocurrency.
Merchant: [34] Whether to hold cryptocurrency for exposure to rate changes or exchange for fiat currency as soon as possible.	• Consistency with the business strategy for risk management. (Most merchants will not speculate because they are not in that business.) • Short, medium, and long term variability of the cryptocurrency exchange rate. • Prospects for exchanging the cryptocurrency with lower charges at a later date or by reducing the transaction volume. • Capability to speculate effectively and safely, provided by skilled people and large resources relative to the cryptocurrency values involved. • Risk of losing the private key and hence the cryptocurrency. • Risk of having the private key stolen and hence the cryptocurrency stolen.	• History of exchange rates for the cryptocurrency. • History of receipts in the cryptocurrency, if any.	• Treasury risk management policies and procedures. • Suitably qualified people to do the speculation.

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Merchant, Customer, Holder of the cryptocurrency: [35] How and where to store cryptocoins (e.g. hardware wallet, software wallet, online wallet, exchange).	• Risk of loss of the private keys. • Risk of the private keys being discovered and the cryptocoins stolen. • Convenience of use.	• Consider likely number of keys to be used. • Consider the current and likely value of the cryptocoins. • Past performance of different types of wallet and of wallet makers.	
Customer: [36] Whether to use cryptocurrency as a payment means, and how to do it. [36] What to buy with cryptocurrency. [36] Whether to look for and consider advertised cryptocurrency prices for goods/services.	• Availability and convenience (ergonomics, speed) of payment, cost, and security – evaluated for the cryptocurrency and other payment methods. • Range of interesting goods/services that can be paid for using the cryptocurrency (consider merchants, products/services). • Range of interesting goods/services that can only be paid for using the cryptocurrency. • Prospects for finding good deals on interesting products/services when paying with the cryptocurrency using the cryptocurrency price. • Ease of searching for cryptocurrency quoted bargains (knowledge of cryptocurrency prices for goods/services, existence of web services that find bargains). • Risk of losing the private key or having it stolen and hence losing the cryptocurrency.	• Information on products/services with prices quoted in the cryptocurrency. • Information on the merchants accepting the cryptocurrency, and for what. • Information on current cryptocurrency bargains. • Statistics on cryptocurrency related crime. • Terms and performance of alternative payment methods.	• Keep the number of payment methods used low to avoid mistakes due to not paying enough attention.
Customer: [37] Whether to hold the cryptocurrency for exposure to rate changes.	• Understanding of currency trading. • Understanding of, and quality of ongoing information about, the cryptocurrency. • Liquidity of the cryptocurrency on available exchanges. • Other portfolio content.	• History of exchange rate, transaction volume and value, distribution of holdings, distribution of transaction values, moving average variability, skew. • Statistics on cryptocurrency related crime.	• Restrict the size of cryptocurrency holding and, thus, exposure.

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Holders of the cryptocurrency: [38] How much to hold.	• Prospects of making purchases using the cryptocurrency. • Other gains possible from paying with the cryptocurrency e.g. discounts on products/services. • Other earnings from holding the cryptocurrency such as through a Proof of Stake mechanism that pays a form of interest. • Existence of at least one exchange. • Understanding of currency trading. • Understanding of, and quality of ongoing information about, the cryptocurrency. • Prospects of the cryptocurrency exchange rate rising (and so providing profit). • Amount you can afford to risk. • Other portfolio content. • Liquidity of the cryptocurrency on available exchanges. • Exchange costs. • Risk of losing the private key or having it stolen and hence losing the cryptocurrency.	• Explanation of the features of the cryptocurrency, its backers, and so on. • Historical analysis of past cryptocurrencies. Includes value growth, trading volume, crime, and events that have killed the cryptocurrency. • Trends of the cryptocurrency so far, especially recently, on exchange rate, total market value, distribution of coins, transaction volume and value, distribution of transaction value, products/services that can be bought with the cryptocurrency, savings from buying with the cryptocurrency, merchants that accept the cryptocurrency, and number of users, behaviour patterns of holders/traders. • Feed of news items concerning the cryptocurrency and related events. • What other users/speculators/advisors are doing and saying. • Exchange fees/charges.	• Develop and document a strategy for deciding holdings and for buying and selling the cryptocurrency. • Assess prospects for long term operation, value growth and use as an efficient payment system.

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Holders of the cryptocurrency: [39] How and where to buy/ sell to achieve desired holding.	• Fees and prices involved for each method (each exchange, newly minted, mining). • Liquidity on alternative exchanges. • Convenience/speed of each method. • Inconvenience from registration, KYC, and installation procedures needed before each method can be used. • Privacy/security of alternative methods (to reduce risk from criminals). • The financial strength of exchanges (since many have closed down). • If there is an indemnity fund for users of an exchange. • Other factors related to the reliability and reputation of exchanges. • The time needed to withdraw fiat currency from an exchange account[7]. • The physical danger of transacting face to face (e.g. a meeting set up via LocalBitcoin).	• Data on how many active users each exchange has, and measures of liquidity. • Information about the level of security achieved by exchanges (e.g. from statements about security precautions, an audit report). • Details and statistics on cryptocurrency related crime. • Independent assessments of exchanges. • The domicile of an exchange, or even if the domicile is known.	• A systematic method for organized trades, perhaps with an app.

[7] This could be 3 – 7 business days; longer for deposits by wire transfer.

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Government: [40] Whether to encourage, discourage, or stay neutral on cryptocurrencies. [40] What overall approach to take to regulation of cryptocurrencies.	• Potential value to society from useful, efficient services now, electronic payment systems for people not currently able to use banking systems, competitive pressure on existing banks and payment systems, and through future technical and behavioural innovations that might improve mainstream finance too. • Potential effects on choice of location by businesses, perhaps bringing inward investment and new tax payers. • The prospects for harm to citizens from cryptocurrencies (investors cheated or let down by incompetent companies, money laundering, terrorist financing, circumvention of sanctions, contraband sales, fraud, online extortion). • Cooperativeness of cryptocurrency stakeholders (influencing the extent to which self-regulation can be used). • The adequacy or otherwise of existing law. • Pressure to focus on other problems.	• Historical information about past innovations and their challenges. • Total market value of cryptocurrencies and total money supply of each. • Statistics and details of cases showing the actual harm being experienced by citizens now, and trends. • Statistics and details of cases showing problems identifying the perpetrators of crime and problems prosecuting people that common sense says are obviously doing wrong. • Estimates of the number of people involved. • Surveys of their attitudes to regulation.	• Put monitoring in place to report regularly on the development of this area and identify opportunities for worthwhile intervention. • Have representatives of the relevant stakeholders meet regularly.

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Financial conduct regulator: [41] How to allocate regulatory effort over potential problems. [41] Regulations to impose to safeguard market integrity.	• The prospects for harm to citizens from cryptocurrencies analysed by type (investors cheated or let down by incompetent companies, money laundering, terrorist financing, circumvention of sanctions, contraband sales, fraud, online extortion). • Cooperativeness of cryptocurrency stakeholders. • The adequacy or otherwise of existing regulations. • Availability of good ideas for tackling the existing and anticipated problems. • Pressure to focus on other problems.	• Statistics and details of cases showing the actual harm being experienced by citizens now, and trends. • Statistics and details of cases showing problems identifying the perpetrators of crime and problems prosecuting people that common sense says are obviously doing wrong. • Estimates of the number of people involved. • Surveys of their attitudes to regulation.	• Put monitoring in place to report regularly on the development of this area and identify opportunities for worthwhile intervention. • Have representatives of the relevant stakeholders meet regularly.
Tax authority/legislator: [42] How to classify cryptocurrencies, possibly depending on what people do with them. [42] Which tax approaches to use for cryptocurrency transactions (capital gains, trading, gambling, other). [42] How to enforce tax rules in practice.	• Value of taxes that could be collected. • Compliance work created for citizens (e.g. due to matching purchases with sales, or getting market prices whenever the cryptocurrency is exchanged or used as payment). • Collection work created for the tax authority. • The government's overall policy stance on cryptocurrencies (to promote, inhibit, or be neutral). • Potential for exploitation of alternative rules (e.g. grey areas around gambling, actions with no independent records).	• Holdings, transactions, and distribution of holdings and transactions. • Distribution of current tax revenues from cryptocurrency use.	• Make estimates of the financial significance of exploitation of existing rules through evasion and questionable avoidance schemes. • Assess the complexity of record keeping and calculations required of citizens.
Tax authority/legislator: Whether to accept cryptocurrency in payment of tax. [43]	• Volatility of the country's fiat currency and the cryptocurrency. • Number of citizens able to pay electronically by cryptocurrency but not other electronic means.	• Exchange rate histories against a basket of major currencies for the nation's fiat currency and for the cryptocurrency. • Survey of access to electronic payment systems.	

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Financial reporting regulator/ standard maker: [44] How to classify cryptocurrency holdings, possibly depending on what is done with them. [44] Which accounting methods to use (fair value, cost, movements through P&L or not).	• Importance of cryptocurrencies for accounting purposes. • Ease of establishing a reliable market value for cryptocurrencies at a particular time. • Availability of existing guidance that can be applied with little or no modification. • Scope for creative accounting. • Prudence considerations (i.e. not wanting to allow recognition of very uncertain gains).	• History of distribution of holdings by size. • History of distribution of transactions by size. • History of variability of exchange rates. • History of differences between exchanges. • History of liquidity on exchanges.	
Financial stability regulators and legislators: [45] How to apply financial stability principles to cryptocurrencies[8].	• Distribution of holdings by size. • Distribution of transactions by size. • Operational risk associated with cryptocurrencies generally and types of cryptocurrency. • Market risk associated with cryptocurrencies generally and types of cryptocurrency. • Potential for contagion between cryptocurrencies and between cryptocurrencies and other assets. • Prospects for greater stability with better money supply control and other control mechanisms for cryptocurrencies.	• Price histories of cryptocurrencies. • Historical research on the lives of past cryptocurrencies and past exchanges.	• Regular monitoring process. • Segmentation of cryptocurrencies by geography and design features. • Produce risk assessment guidance. • Simulate alternative cryptocurrency designs.

[8] For example, ban cryptocurrency holdings, set ratios for capital requirements, or give risk modelling advice.

Decisions	Factors Including Those That Are Risky	Information To Reduce Uncertainty/Risk	Other Key Controls
Data privacy regulator/ legislator: [46] How to apply data privacy principles to cryptocurrencies. [46] Who to consider responsible for privacy. [46] How to enforce the rules cost effectively.	• What personal data are held (on the blockchain, at an exchange, on an online wallet system). • Which legal entities are controlling each computer storing data. • Which countries the data copies are held in. • How effectively data are anonymised, if anonymization is used as a control. • Ease of identifying every node in relevant territories.	• Design details of the cryptocurrency. • Node network monitoring information. • Design details of exchanges. • Research on trying to identify users from supposedly anonymous data (e.g. public key strings cross referenced across social media). • De-anonymising tools available.	• Document control expectations for each ecosystem element, e.g. currency, exchange, payment system.
Police/prosecutor: [47] How much to invest in people and equipment to fight crime that involves cryptocurrencies. [47] Which tools to invest in. [47] How to allocate resources across the cryptocurrencies. [47] What types of crime to target (e.g. money laundering, theft, fraud, online extortion including ransomware, terrorist funding, circumventing international sanctions, contraband purchases).	• Scale and consequences of cryptocurrency-related crime types. • Other types of crime, particularly cybercrime, competing for resources. • Developing methods of crime. • Degree of organization. • The law. • Levels of public and political concern. • Success rates for investigating and prosecuting crime types. • Discoveries from cases (e.g. interpretations, criteria, evidential weight). • Extent to which each cryptocurrency is attractive to criminals.	• Reported crime levels and crime surveys. • Intelligence gathering. • Surveys of public concern. • Other performance metrics. • Design features of each cryptocurrency. • Level of cooperation provided by cryptocurrency initiators, exchange operators, and others in the ecosystem. • Tools offered to law enforcement by software companies.	• Regular monitoring process. • Guidance to police officers through supervision, training, and written updates. • Prosecutors compiling written guidance based on the results of cases and other factors.

Principal Authors

Matthew Leitch

Matthew Leitch specialises in internal control and risk management. He has worked alongside Michael Mainelli in innovative operational risk management work and is often called upon by clients to help find new solutions to tough problems. His background includes writing, psychology, mathematics, software development, audit, and accountancy. He spent 7 years as a controls specialist with PricewaterhouseCoopers, where he pioneered new methods for designing internal control systems for large scale business and financial processes, through projects for internationally known clients. Matthew is a visiting lecturer and supervisor at the University of Southampton's Business School and a member of its Centre for Risk Research. He is also a member of a risk management standards committee at the British Standard Institution and the author of two books on risk and risk management.

Aleksandar Matanović

In 2007, Aleksandar Matanović co-founded a Serbian e-gold exchange. In 2012, after learning about Bitcoin, he co-founded www.ecd.rs, a Serbian bitcoin exchange, and became its CEO. His company also operates a network of cryptocurrency ATMs, has developed a cryptocurrency payment application for merchants, and initiated the founding of the Serbian Bitcoin Association. In 2016, Aleksandar graduated with an MSc in Digital Currencies at the University of Nicosia, making him one of the first graduates of this pioneering course. Aleksandar is a regular speaker at blockchain and cryptocurrency industry events. He aims to spread awareness and promote safe and responsible use of cryptocurrencies and blockchain technology. He strongly believes that blockchain and cryptocurrencies will change the world and tries to be an active participant in that revolution.

The Eternal Coin programme aims to initiate a global discussion on the nature of money and the concept of value. It takes a long-term and inter-generational approach and is an educative programme teaching the theory and mechanics of currencies. The Eternal Coin encompasses discussion on the composition of currencies which might, for example, enable sustainability. Ultimately, Eternal Coin aims to provide an online tool or 'playpen' which will enable communities to design, create and transact with their own currency, whatever form that may take.
www.eternalcoin.com

DasCoin™

Our vision is to lay down a global bedrock of trust that unlocks prosperity for everyone. By eliminating the problems of traditional money and adapting trust to the digital age, we are creating a better system for holding and exchanging value.

We are focused on delivering solutions that increase empowerment, enhance control and expand freedom. We believe the pursuit of these qualities will lead to a better, fairer, more prosperous future for all involved. We are constantly innovating as we create, maintain and evolve the world's most secure digital currency.
www.dascoin.com

LONG FINANCE

"When would we know our financial system is working?" is the question underlying Long Finance's goal to improve society's understanding and use of finance over the long term. Long Finance aims to:

- expand frontiers - developing methodologies to solve financial system problems;
- change systems - provide evidence-based examples of how financing methods work and don't work;
- deliver services - including conferences and training using collaborative tools;
- build communities - through meetings, networking and events.

www.longfinance.net

Yen

Z/Yen is the City of London's leading commercial think-tank, founded to promote societal advance through better finance and technology. Z/Yen 'asks, solves, and acts' on strategy, finance, systems, marketing and intelligence projects in a wide variety of fields. Z/Yen manages the Long Finance initiative.

Z/Yen Group Limited
41 Lothbury, London EC2R 7HG, United Kingdom
+44 (20) 7562-9562 (telephone)
hub@zyen.com (email)
www.zyen.com