CrowdCoin

White Paper

The one-stop platform for the world of cryptocurrency

Version 2.0.0
Nov 17th 2018

Creating an environment for crypto-investors, users and residents of the cryptocurrency world to come together and invest, innovate and educate as part of a tangible movement for change

Disclaimer

The purpose of this White Paper is to present CrowdCoin, its technology, business model and the CRC coins to potential coins holders. The information set out below may not be exhaustive and does not imply any elements of a contractual relationship. Its sole purpose is to provide relevant and reasonable information to potential coin holders in order for them to determine whether to undertake a thorough analysis of the company with the intent of acquiring CRC coins.

This White Paper does not constitute an offer to sell or a solicitation of an offer to buy a security in any jurisdiction in which it is unlawful to make such an offer or solicitation.

Certain statements, estimates and financial information contained herein constitute forward-looking statements or information. Such forward-looking statements or information concern, known and unknown risks and uncertainties, which may cause actual events or results to differ materially from the estimates or the results implied or expressed in such forward-looking statements. This English-language White Paper is the primary official source of information about the CRC coin. The information contained herein may be translated into other languages from time to time or may be used in the course of written or verbal communications with existing and prospective community members, partners, etc.

In the course of a translation or communication like this, some of the information contained in this paper may be lost, corrupted or misrepresented. The accuracy of such alternative communications cannot be guaranteed. In the event of any conflicts or inconsistencies between such translations and communications and this official English-language White Paper, the provisions of the original English-language document shall prevail.

Table of Contents

Introduction

Although cryptocurrencies have existed since the mid-1990s, it took until 2009 and the success of Bitcoin for the concept to be taken seriously by the general public. Bitcoin finds itself at the head of a recent surge in popularity – due in no small measure to the attention of investors. This has caused the price of the cryptocurrency to rise enormously, but not before starting many conversations about the viability of a digital currency across the financial world.

This conversation has been marked by a difficulty in assigning a financial value to these newly created cryptocurrencies. This has caused the trading public to treat these coins more like stocks than like real money – investing in them for the short-term viability, and then selling them on as the commodity, not using these altcoins as a means of payment for other commodities. This is in some part due to the fact that most cryptocurrencies are pegged to large, more successful coins that have a fiat value. This requires users to trade their coins for *other* altcoins that must then be sold on in order to convert them into cash.

Because of the intensely convoluted system that has sprung up in the wake the Bitcoin success story, CrowdCoin aims to provide a comprehensive platform for investors and enthusiasts that not only simplifies the complex chain of trading, while providing bespoke investment services to community members but educates the community at large. This will move the cryptocurrency community towards a sustainable, responsible future and introduces a profound change for good in a financial ecosystem that has been renowned primarily for its volatility. This paper aims to set out the goals of the CrowdCoin platform, as well as a look into the *masternode* technology that will power it.

In the spirit of the community of which the CrowdCoin ideals form an integral part, we are a crowd-sourced initiative. This means that we will draw on the expertise of the many, not the few and use the ideas of the people who use our platform to drive it forward and make CrowdCoin the greatest success that it can possibly be. By doing this, we can bring our platform to its maximum potential.

Product Development Initial Phases

The CrowdCoin platform has a concrete roadmap for success, laid out here. Before CrowdCoin can achieve these goals, however, real funding is required in order to help implement these changes. The first step in the CrowdCoin journey is to continue to work on implementing a truly world-class and community-defining platform for users. Once this platform is operational, further development of the masternode and blockchain systems (derived from the proven and successful DASH model) can take place. Once the masternode system is working efficiently, development can turn back towards refining the platform, as well as providing ancillary services that CrowdCoin seeks to provide.

This sensible, sustainable and methodical approach to cryptocurrency is backed by recent international responses to investment and concerns from governments about investing in cryptocurrency. With some concern that China's recent clampdown on mining operations will cause Bitcoin to become unsustainable, it is time that the responsible crypto-community at large took concrete steps to prove the viability and responsibility to users to prevent nervous regulators from clamping down.

Our roadmap to achieving the sustainable future of digital currency, in which goods and services can be paid for entirely in cryptocurrency, is as follows:

Phase 0: Creation of the CrowdCoin network, minting, and setup

Phase 0 has now concluded. It encompassed the setup of the network, the blockchain and the minting of the coins and tokens. We have also established the secure servers, the creation of the online explorer as well as the launch of the basic edition of our CrowdCoin website.

It also included the creation of the easy-to-install script, explorer upload. We have added CrowdCoin to mining pools, as well as Social Media channels: YouTube, Facebook, Twitter, Discord and BitCoin Talk, as well as the start of a dedicated CrowdCoin Subreddit.

We have also now been listed on Cryptopia and Stock.exchange, which has allowed us to begin trading in earnest. More exchange listings will follow, even though the wider work within Phase 0 has now concluded. We have also now had our Masternode listed on masternode.online.

Phase 1: Masternode Management System

The MMS system, which forms part of our revised Phase One activities, will allow users to get their funds matched and maintained by a third party (predominantly by the CrowdCoin platform itself). This allows for a hassle-free journey through the CrowdCoin experience and will provide an excellent opportunity for users who are not part of the wider crypto-community to invest and learn about the world of investment while ensuring that they maintain profitability and control of their MN systems.

The Masternode Management System functions by having the user send coins to the central CrowdCoin service. Your coins are then combined with collateral sent in by other MMS users, creating new Masternodes at a fraction of the standard collateral required to do so.

As an example, if you were to buy into Dash, you would be required to use 1000000 coins(1M) are a collateral in order to operate your own Masternode. Using the CrowdCoin management service means that you will not need to purchase 1000000 coins as originally required, as your coins will be paired with those of other users to reach the 1000000 coin mark collaboratively. This provides an affordable way to operate what is effectively your own MN without the need for costly transactions at the beginning.

The revenue from your share of the service is sent directly back to the wallet from which the transaction originated. This requires that users send their coins directly from their wallets, *not* from exchanges, as this will mean that all proceeds are returned to the exchange from which the transaction originated (This requirement will be removed once the new CrowdWallet has gone live). As we cannot guarantee the actions of a third-party, CrowdCoin request that all transactions to their MMS system originate from private wallets, so that you have maximum control over the revenue earned by your coins, as sending proceeds back to the exchanges means that we are unable to guarantee that you will receive your full income back from them.

All coins in our MMS system are monitored 24 hours a day for maximum security. You can monitor your investments in real time to ensure that your coins are creating maximum value. Should you wish, at any time, to remove your coins from the MMS programme, then it will be possible to do so without any loss of revenue on your part at natural ends of the contract you have subscribed for. As the MMS system will function in 3 and 6-month contracts, removal of the coin will occur at the end of the contract.

Use of the MMS service will incur a small fee on the part of the user, from which CrowdCoin and the platform will fund further improvements to their services. The fees will come from both the original amount deposited, and then be calculated on the total value of the returns gained through the use of the system. The deposit fee will be charged up-front, while the revenue fees will be taken while its generated. The MMS is as well accessible from mobile using the mobile version of the website. It maintains full desktop functionality while being optimized for mobile use.

Phase 2: CrowdWallet

The new CrowdWallet provided by the platform represents perhaps the strongest demonstration of our intentions yet. By designating the key sector of the user experience as our second goal for the future, the platform is demonstrating

The CrowdWallet will also feature much of the community functionality that originally featured within this roadmap. Contained within it will be a live news aggregator, information and news on CrowdCoin and other social elements that will be used to draw investors together and provide a sense of community for the coin. The CrowdWallet aims to be an all-encompassing user experience in its own right, which will negate the need for users to have to spend time using different applications and sites, as all the functionality and ancillary services that they require will be provided within it.

Furthermore, use of the CrowdWallet will allow real-time information tracking and control of the Masternodes, as well as the ability to subscribe to our Masternode Management

System without the need to complete complex forms. Users can simply select the service they require and control it simply and easily.

There will also be much more functionalities for users to chat directly via instant messenger in order to support coin transactions between them, meaning that the CrowdWallet will also be able to function as an independent marketplace in its own right. Internal transactions from within the wallet will occur without fees (subject to terms and conditions).

The update revenues will also allow for Proof Of Stake functionality, granting users a share of revenue from POS directly into their wallets.

Phase 3: Secure Custody Functionality

As the world of cryptocurrency is a fast-moving environment, it is important for CrowdCoin to help our users to remain in line with major security developments. To this end, we are pleased to announce that our coin will offer Secure Custody functionality, designed to add maximum security for your digital assets and ensure that you retain your coins safely and properly in the form of securing the product as absolutely as possible. This is also an important step towards the acquisition of traditional investors who have, until this point, stayed away due to security concerns.

Cold Custody is a service in which we take alive, 'hot' coins from the user's wallets and store them safely and securely in multiple physical locations, in order to ensure maximum security for large deposits. While wallets are in cold storage, they cannot be used but will be provided with an additional layer of security against loss. This is the safest way to prevent any potential loss of coins through malicious action. We keep the assets on your behalf, generating advanced security protocols to ensure that your property remains safe and available without risking a loss through any untoward activity.

In short, Its the placement of private security keys into a secure physical location, allowing them to receive, but *not* to send until they have been retrieved from their physical location and had their 'hot' function restored. Our exact processes are necessarily confidential, but CrowdCoin is extremely proud of the rigorous and secure protocols that we have put in place, making CrowdCoin an extremely safe storage option when compared to the wider crypto markets.

While this functionality may seem esoteric for many users, it is an important development for the platform not only in terms of security and safety for users who have purchased or mined a high number of coins but it also demonstrates a crossover from a purely digital currency to something more tangible – an important step for any serious cryptocurrency looking to gain wider acceptance in opposition to traditional fiat currency.

Ultimately, the Secure Custody service is not meant simply as a simple way to store coins, it is the single safest way to ensure that a stock of currency can be stored long-term without the traditional pitfalls of crypto storage. By taking them out of circulation and placing them into a physically secure location, they will be safe from cyber attacks, and when stored properly, will be safe to physical attacks as well, meaning that your coins can be stored without concern.

Phase 4: Fund Management Listings

In order to successfully operate any financial organization, it is necessary to understand the wider market in which we operate. To this end, CrowdCoin will compile listings on available investments funds that operate in the cryptocurrency space, based on their past investment performance. Our aggregated ranking system, while obviously no guarantee of future results, but will help prospective investors to understand who, and what is the best-suited service available that can help them to invest their money in a manner best suited to them

Every fund offers a different investment experience and portfolio, and our Fund Management Listing, which comprises Phase 4 of our development plan, will help users to compare the different options available for them and their money at a crucial time in the story of cryptocurrency.

CrowdCoin cannot be held responsible for the performance of Funds listed, but will seek to help users understand the best way to proceed with their portfolio options. We will do this by presenting users with a list, based entirely on previous performance (according to predefined parameters) allowing users to continue at their own risk.

Our ranking structures will contain information about past results, effectively making us a comparison stop based on liquidity, time frame, investment type, sector, the minimum required investment and other relevant information.

Phase 5: Expand Platform to Offer Crypto Exchange Services

In conjunction with our existing news aggregation service, and use of real-time data, we will be able to display prices, volumes and order books of various exchanges, meaning that CrowdCoin users will be able to get an accurate market overview of the various major exchanges from our site.

Phase 6: OTC Cryptocurrency Exchange

We will allow users to escrow funds while performing OTC transactions, and operating off-chain, (via bank direct transfer or via cash) transactions allowing users to buy and a sell cryptocurrency directly to other users using CrowdOTC as escrow mechanism.

Phase *: Side Projects

While proceeding in the achievement of the previously mentioned phased we'll keep on every possible way to support and provide more value for the entire blockchain and crypto community promoting and getting involved in open sources projects project that could be beneficial for our users as well.

Market Environment and Platform Dynamics

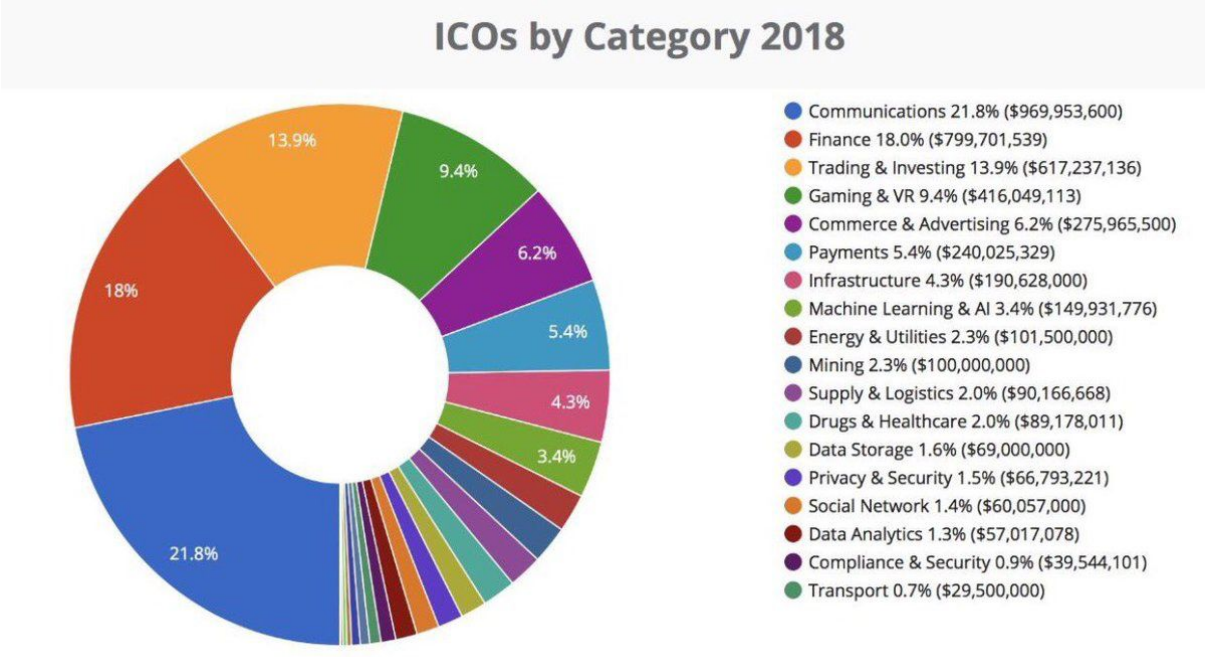
Market Environment

After a period of turbulence, the market for cryptocurrency is finally showing signs of stability, in no small part thanks to almost 18 months of sustained investment. There is sufficient evidence to prove that most investors react positively to speculative, wild suggestions at ICOs, rather than on fact-based, well-presented analysis.

It is important for CrowdCoin to demonstrate its commitment to providing a legitimate and well-designed platform, so that maximum trust can be established between the CrowdCoin team and investors at this early point.

There are very few in the market that offers the kind of collective services that CrowdCoin has to offer. This puts the platform at an advantage, as we are able to fill an existing gap in one of the fastest-emerging markets in the world and the most talked-about sector of the digital economy.

With 211 ICOs in 2017, raising a total of over $5.6bn[1], and with the first quarter of 2018 have seen the capital raise increase still, with over $5bn raised across the board via new ICOs, we can clearly see that the market for ICO hosting facilities is increasing exponentially.



A pie chart showing the major categories of ICO of Q1 2018, and the amount of money raised by each sector.

[1] http://uk.businessinsider.com/how-much-raised-icos-2017-tokendata-2017-2018-1

Platform User Engagement

As discussed more widely throughout this White Paper, CrowdCoin aims to have a team who will be able to vet potential investment opportunities. This means that only accredited, legitimate ICOs will be offered on our platform.

As the ultimate aim of the platform is to provide a hub for the crypto-community, we anticipate that there will be a sizeable market that is directly reachable through membership, which is an immediate group of around 3,000 (a number which the platform anticipate will rise to between 100,000 and 150,000 users over the course of 18 months) as well as the potential to attract investors from outside of the platform. This is an advantage for CrowdCoin, as it will attract people who are looking to take part in ICOs and convert them into registered users, building the number of visitors to the site on a daily basis.

Demonstrating the presence of a strong and active user base boosts the credibility of CrowdCoin as a platform, which will allow it to recruit a higher quality of ICO than competitors. As the demand for ICO-hosting capabilities is growing, in the face of an unprecedently strong Q1 for 2018, the platform is emerging as the only true integrated exchange and investment service available.

Platform Revenue Model

Platform revenue is funded primarily by the provision of our investment and support services which will operate on a commission basis. When users make deposits and withdrawals, then the CrowdCoin platform will take an according percentage of the transaction as revenue. Every single service provided by the platform - including use of our new Masternode Management Service, will carry a corresponding fee - dependent on the size of the service required. The Custody function will also incur a minor transaction fee on the part of the user - meaning that CrowdCoin is funded well enough to continue both operation and further development of the service. Naturally, our on-site exchange will also charge commission for each transaction, again, dependent on the total amount exchange by the user on our platform.

Furthermore, our investment fund tracking will generate a new revenue stream by charging a percentage of capital allocation to those investment funds.

Platform Revenue Allocation

As described in the road map section, the CrowdCoin platform will be constructed in four phases. Keeping up with the rapid speed of progress is vital to stay relevant and competitive in the ever-changing world of cryptocurrency. This means that we will invest our revenue from the previous successful stages into additional development in order to maintain our place at the head of the pack, until the platform is completed developed, having all aforementioned functionalities available.

The core development team is currently focused on launching the platform, so that operations can begin in earnest.

Primary revenue allocation falls into the following sectors:

1. **Platform development (ca. 45%)**
2. **Cyber security (ca. 25%)**
3. **Legal (ca. 10%)**
4. **Marketing (ca. 10%)**
5. **Other operations (ca. 10%)**

Competitive Environment

General Crowdfunding Sites

A crowdfunding approach is perhaps the most quintessentially 21st century form of finance available to businesses. From an investment perspective, crowdfunding offers the opportunity to fund projects that cannot gain investment via traditional means, by proposing your ideas directly to the public. It is normally made explicit that without the public backing your project, there will be no alternative way to fix a specific function, or to create the specific service, with the promise of eventually delivering the product to the backers upon conclusion. The following sites offer a pure crowdfunding approach, without the focus on cryptocurrency and blockchain-related technologies that CrowdCoin brings to the table.

Their unsuitability for the specialised requirements of ICO make them unlikely to prove a serious challenge to CrowdCoin over the long term, as they occupy different sectors of the digital investment community.

Crypto-focused Platforms

There are a number of crypto-focused sites that offer parts of the flexible and valuable service that CrowdCoin is seeking to introduce. None, however, truly offers the same total experience, as each of the following competitors is lacking sorely in a clear mission statement and an all-encompassing execution of their ideas – meaning that some sites offer great ICO facilities, others strong exchanges, but that overall, none are as comprehensive a platform as CrowdCoin.

There is clearly room for an exchange and crowdfunding platform combination in the market. Of our existing competitors, the UK, EU and US (probably the three richest sources of investment), all remain chronically underserved, leaving a gap in the market for CrowdCoin to fill.

Crypto Exchanges

Exchanges form the lifeblood of crypto trading, allowing users to exchange, buy and sell their coins from anywhere in the world. It is no surprise that the major exchanges are by now very well-financed, increasingly well-regulated entities that are headquartered across the world. This international distribution of exchanges can sometimes work to the advantage of the investor, especially for those who are strong supporters of decentralisation. Major players include exchanges such as China's Huobi, New York's Gemini and other sites, including Jaxx, Coinomi and Amon.

These services all have interesting USPs of their own – be it stablecoin from Gemini, government funded blockchain development in the case of Huobi and even celebrity appeal, in some cases, but CrowdCoin is offering a unique wallet service, with both an integrated exchange and access to our proprietary Masternode Management System – the only wallet available on the market to do this.

Access to everything you require from within your wallet means that there is no need for complex tools and additional apps, as the CrowdCoin wallet takes care of everything that you need. This makes CrowdCoin accessible to new users, and convenient for experienced ones. By massively reducing the complexity and the need to compare hundreds, if not thousands of exchanges constantly, amongst a sea of largely faceless competitors, CrowdCoin makes crypto trading significantly easier than ever before.

Bloomberg have reported that 95% of ICOs never make it onto an exchange. Any coin which reaches the soft cap through our ICO CrowdEx is guaranteed to be listed on our exchange, meaning that investments through our platform will always yield results – a first for the community and markets.

CrowdCoin Fit

There is a significant market for platforms looking to offer new tokens and coins to investors around the world. This is a gap that CrowdCoin is poised to perfectly fill through its innovative and creative platform.

As our non-investment driven user base grows, it will present the platform with an increased number of users who can be directly contacted about ICO opportunities – and as the number of registered investors grows, the more knowledge and traffic the site will generate, helping CrowdCoin to drive success through an organic cycle of user interaction that most similar sites cannot offer.

Technical Information

Before delving into the complex world of cryptocurrency, and the benefits of the CrowdCoin platform, it is worth laying out all the technological information on CrowdCoin in a simple, readable format.

Cryptocurrencies

Modern cryptocurrency (unlike fiat currency) is a form of digital money that exists only in the form of code. Thanks to the blockchain, which uses cryptography and distributed networks, we can avoid the need for a centralised bank, as the information is securely encoded and can then be stored remotely. The best known decentralised cryptocurrency – meaning one that has been *minted* across many different locations, rather than being minted from a central source – is Bitcoin. Bitcoin is powered by a publicly available ledger, which records and then validates every transaction in a chronological order. This is known as a blockchain or a distributed ledger and adds the principle of accountability for every transaction, reducing the risk of theft by merchants, as once the transaction has been made, it is permanent and cannot be voided.

Tokens

A token is a representation of a specific asset, equity, or service, which resides on the top of another blockchain (such as in EOS, Ethereum and Waves). Creating new tokens is a much easier process than creating a blockchain, as the service has been offered in such a manner that you do not need to modify the codes and protocols to do so. All that is necessary to create a token is to follow a standard template that already exists on the blockchain. These templates, like the ones used by the Ethereum platform, then allow users to create their own tokens. The process of token generation has to be encoded and due to the fact there is an underlying blockchain, it does not need *mining* power as it relies on the power of the underlying blockchain. The token generation event is an event created by writing a programme for it, and the distinction between blockchain, in procuring coins and token is that coins are achieved by the computer calculating a difficult solution, while a token is created by a token generation event. This means that, in reality, there is much smaller, one-time expense involved in creating a token. This means you can effectively create tokens out of thin air.

New coins are continuously minted, but all tokens are created at the creation of the coin. In order to transfer a token, they rely on the blockchain, meaning that the cost of the transactions needs to be funded.

Proof of Work (PoW)

PoW is a mechanism that allows the entire system to prevent two different things. The most important feature of the PoW mechanism is that it prevents *double spending* of coins. Double spending is where malicious activity can, in effect, allow a coin to be distributed to two different locations, and used as if they were two separate coins. PoW prevents this from happening by making it more difficult for a single source to take control of 51% of overall mining power.

It is used to define the extensive system of calculations which constitutes mining – the sequence of events that occur on the blocks – to the blockchain. This provides evidence to the blockchain that the computer doing the mining has in fact completed the sequence of calculations necessary to complete the transaction legitimately.

This system also provides the economic reward to recompense miners for the energy spent in mining the coin. This is obviously beneficial for the spread of the network and beneficial for the total amount of mining power available.

The major downside of a PoW operation is that it requires an amount of energy that gets exponentially larger in order to complete. It normally requires the use of a dedicated graphics card or Application Specific Integrated Circuits (ASICs) to complete the mining operations.

This mechanism is used to make it more predictable and stable across the entire system and can help prevent inflation. Due to CrowdCoin's halving procedures, every year the quota of new minted coins is halved. After a few iterations of this halving, the supply of new coins will become zero. After a while, this means the total amount has been minted and mined, so the miners will have only the transaction fees.

Another useful feature of the PoW system is that it prevents an increase in power from contributing to an increase in mining ability. In effect, the more the power of a mining operation is increased, the more difficult the algorithm becomes. This is because the number of coins minted in a day is fixed at the code level, meaning that there is no way that new coins can be released by the network. Preventing more powerful operations from effectively strip-mining the network quickly is an important step to ensuring a safe and sustainable network for all users.

X16R

The mining algorithm that we have chosen for Crowdcoin is x16r due to its asic resistant to make more difficult the constitution of a majority in mining power to reduce the risk of the 51% attack and push forward the spreading of the net to mining participates to sources that have not access to the latest asic technologies.

In case of an attempt of build of taylored machine from the Quantum computing manufacturers We'll operate a soft fork to switch to RoseQ(the quantum resistant mining algorithm we have internal developed that will dissolve any chance that quantum computer could have any unfair advantage in mining the Crowdcoin blockchain)

Technology of CrowdCoin

CrowdCoin's Unique Blockchain

CrowdCoin is a unique PoW-based cryptocurrency evolved from the best parts of DASH with its own blockchain built from the ground up.

The advantages of this are that the CrowdCoin development team is always able to improve on the technology on which the platform is built, as well as being able to quickly implement changes and possible fixes without requiring majority consensus. It also prevents CrowdCoin from being limited by the capacity of a different blockchain due to the fact that it is not a token. An example of this limitation can be seen with crypto-tokens such as the ERC-20 tokens on the Ethereum blockchain, which have caused network congestion due to over usage/implementation.

In addition, CrowdCoin utilises DASH's masternode system in order to provide added stability, flexibility and security to the coin's network and the added masternode governance system, allowing masternode owners to take votes on the future progression of CrowdCoin.

CrowdCoin and Masternodes

CrowdCoin masternodes are computers that run a CrowdCoin wallet 24 hours a day, keeping the network steady and secure, as well as improving the bandwidth, which allows for better synching across the network. Masternodes are owned by different people in CrowdCoin's community and they only require a modest collateral, a public IP address, and continuous uptime. Masternodes will be fairly and randomly chosen to receive a 50% award from every mined block.

Safety also plays a part in masternode ownership. In order to conduct a 51% attack, you need 51% control of the nodes. As the masternode has a stronger vote than a standard node, this requires fraudulent users to have a 51% stake in the masternodes in order to conduct a double-spending attack. This large stake makes it significantly more difficult, as it requires having the collateral to carry out the task.

CrowdCoin Tech Specifications

The basic specifications, and the functionality for CrowdCoin are as follows:

Coin Specification Ticker: CRC

Algorithm: X16R

Block Time: 2 min

Reward 3200 CRC

Block Confirms for Mined Blocks: 5000

Block Confirms for Sending/Receiving: 6

Masternode Transactions Confirmations: 15

Block Max Size: 10 MB (4x faster than sane Bitcoin and 10x more capable)

Max coins: ~83 900 000 000 in 2028

Pre-mine: 80 000 000 000

Halving: previous_block_value-3200/2500000 every single block

Masternode specifications:

Min. coin age: 24 hours

Collateral: 1 000 000 CRC (one input)

Only IPv4 addresses allowed

Default port 8585

The coin can be used as a payment mechanism for the services on the CrowdCoin platform.

CrowdCoin Core Development Team

Luca Paterlini

CrowdCoin founder and technical lead, Luca has been a crypto-evangelist since 2012, getting others into the crypto-community. He has been working as a consultant since 2017. Previously, he worked in the cyber-security sector, with Tesla Consulting, as well as working for Digital London as a consultant for backend development. He is also a crypto-investor, having been involved with several different altcoins in the past. He was a national athlete in Italy for 10 years, competing in middle-distance running and brings the same strength and stamina to his work with CrowdCoin.

There are others within the CrowdCoin team, but due to the hectic demands of working in one of the fastest emerging sectors within the tech world, CrowdCoin has chosen to remain

anonymous for the time being, in order to prevent them from being doxed, as several staff members have suffered severe disruption to their private lives by continuous spam and messages.

Conclusion

In conclusion, the CrowdCoin platform introduces a number of significant safeguards to complement the rapidly evolving cryptocurrency ecosystem. Based on the proven, existing DASH technology, the masternode system that CrowdCoin employs offers a degree of safety and increased participation in a centralised hub for cryptocurrency users and enthusiasts around the world.

The platform, with its four -step map for success aims to be able to unify the crypto-community into a sustainable user base, using the CrowdCoin platform. With an open-source philosophy combined with the momentum from the crypto revolution of 2017, CrowdCoin offers the ability to solidify a decentralised system into a force for good. With the investment platform carefully designed to deliver an effective and secure method of ICO participation for users anywhere in the world, and a concrete plan for connecting the crypto-world to the real world of business in a manner that promotes the use of CrowdCoin both to and from companies, the opportunities to join us on this mission are incredibly exciting.

The use of a dual-tier model, rather than the more popular but potentially dangerous single-tier models popularised by platforms such as Bitcoin, is an exciting development. With a focus on education and increased awareness of the community around them, both through education facilities and a crowd-sourced investment scheme, CrowdCoin will help to unite the cryptocurrency community into a coherent force for change.

The increased sustainability brought about by CrowdCoin will provide a solid platform, with strong fundamental principles to bring closer the prospect of a usable and responsible cryptocurrency to compete with fiat money in the near future.

Appendix A – Major ICOs in 2017

Major ICOs from 2017

A selection of the major ICOs from 2017 show that there is inherent potential for the ICO function of the CrowdCoin platform to meet the targets that we have set out above.

2017 saw 435 successful ICOs, which, on average, raised around $12.7m USD each[2]. Of the total investment for the year, the 10 largest projects were responsible for 25% of total fundraising. Furthermore, the average investment has returned at 12.8 times the initial investment, in real terms. This is conclusive proof that if CrowdCoin can construct an integrated platform capable of attracting the highest tier of ICOs (and by extension, the highest tier of investor), there is a significant financial return to be made.

The major ICOs (and what became of them) is as follows:

1. **Tezos promised to revolutionise the governance issues faced by blockchains. It ironically fell prey to Its own governance issues after raising a staggering $232m in only 14 days[3]. Under the new board, they are finally releasing their much vaunted Tezos coin during Q2 of 2018.**
2. **Filecoin is pioneering file systems via blockchain. Their ICO was littered with technical issues (that largely still remain to this day) and with accusations of financial misconduct. However, this did not stop them from raising $200m in under an hour, thanks to the presence of major investors, including Sequoia Capital, Andreessen Horowitz, and Union Square Ventures[4]. While Filecoin went on to prove a failure, the interest generated in the new technology has proved that there is solid market for investment in pioneering ideas.**
3. **EOS is building a blockchain specifically for businesses and corporations. It plans to provide blockchain solutions that offer efficiency, security and data integrity. They launched their ICO in June 2017 and raised $183m, with the price rising to $700m by the end of the year[5].**
4. **BANCOR aims to construct a decentralised exchange ecosystem that allows investors to employ P2P trading techniques with as small a risk as possible. Interestingly, they aim to support any token that has been successfully issued,**

[2] http://uk.businessinsider.com/how-much-raised-icos-2017-tokendata-2017-2018-1

[3] http://fortune.com/2018/02/22/tezos-coin-ico-launch-foundation/

[4] https://www.coindesk.com/257-million-filecoin-breaks-time-record-ico-funding/

[5] https://news.bitcoin.com/eos-raises-700-million-despite-tokens-affording-no-rights-uses-purpose-or-features/

regardless of the total number of users available (meaning every existing coin will be supported). They managed to raise $153m in June 2017.[6]

5. **STATUS aims to work as a light, mobile-based chat and wallet application built on Ethereum. It managed $95m in June 2017.**[7]

[6] https://www.forbes.com/sites/montymunford/2017/12/12/bancor-starts-to-deliver-on-its-record-breaking-153-million-ico/#6210fa8a3509

[7] https://www.inc.com/brian-d-evans/status-ico-raised-over-100-million-for-ethereum-powered-dapps-on-ios-and-androi.html

Appendix B – CrowdCoin Competitors

There are several platforms currently available to investors that work in a similar way to the CrowdCoin platform, but without the same overall functionality. These platforms include:

General Crowdfunding Sites

A crowdfunding approach is perhaps the most quintessentially 21st century form of finance available to businesses. From an investment perspective, crowdfunding offers the opportunity to fund projects that cannot gain investment via traditional means, by proposing your ideas directly to the public. It is normally made explicit that without the public backing your project, there will be no alternative way to fix a specific function, or to create the specific service, with the promise of eventually delivering the product to the backers upon conclusion. The following sites offer a pure crowdfunding approach, without the focus on cryptocurrency and blockchain related technologies that CrowdCoin brings to the table.

Their unsuitability for the specialised requirements of ICO make them unlikely to prove a serious challenge to CrowdCoin over the long term, as they occupy different sectors of the digital investment community.

CrowdCube

Crowdcube is a UK-registered investment platform that uses a social media-driven approach to drive investors to their site. It allows anyone in the UK to raise money for any cause and, subsequently, does not have the focus and clarity that a dedicated crypto-platform like CrowdCoin offers. This forces potential ICO investors to have to wade through a not inconsiderable amount of alternative, less interesting products before finding what they are looking for.

Indiegogo

Indiegogo was one of the original giants of the crowdfunding scene when the format first rose to prominence online in the later part of the last decade. It has financed everything from beehive automation technology to cinematic sequels.

In 2016, the SEC required them to overhaul their KYC/AML protocols, as they had fallen victim to obviously fraudulent investors on a number of occasions. Due to their massive size, and the number of projects (as well as the sheer variety) available, Indiegogo has simply removed a disclaimer suggesting that their site was free of fraudulent activity.

This is a major problem for many investors and businesses alike.

The tightly-controlled number of ICOs being offered by CrowdCoin means that, in reality, this behaviour should not be repeated on the platform as it will be possible to comprehensively vet each individual project and maintain a higher level of control over what takes place under the CrowdCoin banner.

Crypto-focused platforms

There are a number of crypto-focused sites that offer parts of the flexible and valuable service that CrowdCoin is seeking to introduce. None, however, truly offers the same total experience, as each of the following competitors is lacking sorely in a clear mission statement and an all-encompassing execution of their ideas – meaning that some sites offer great ICO facilities, others strong exchanges, but that, overall, none are as comprehensive a platform as CrowdCoin.

There is clearly room for an exchange and crowdfunding platform combination in the market. Of our existing competitors, the UK, EU and US (probably the three richest sources of investment), all remain chronically underserved, leaving a gap in the market for CrowdCoin to fill.

Tokenmarket

For new investors, Tokenmarket's biggest drawback is that it lacks any real information about anything. There are a great number of pictures of Gibraltar, and functional looking text boxes, but if you are not already entrenched in the world of cryptocurrency, then you will struggle to use the site in a meaningful and impactful manner.

The other services offered by Tokenmarket (such as investment advice) appear to be ancillary at best, as they are simply a rehash of the Rock of Gibraltar/contact button combination that seems to make up most of the Tokenmarket site.

While the Tokenmarket platform clearly offers strong service for new ICOs, it cannot be considered a serious competitor unless it develops its platform to a level beyond simply 'functional'. The serious flaw in their business model is that they will list *any* coin brought to them, without any due diligence on their part, meaning that at any given time, investors are potentially exposed to malicious actors who may seek to take their capital in bad faith.

This is something that the CrowdCoin platform specifically sets out to address with our more robust business model, where creating a trust-based investment process is paramount to our mission.

Cryptonymous

Perhaps the closest competitor to the CrowdCoin platform (though far less ranging than the proposed version of CrowdCoin laid out here), Cryptonomous was launched in the face of the ICO wave of 2017. It offers investors the chance to buy into new tokens by paying with Bitcoin and Ethereum amongst others.

It has managed several impressive ICOs – including Giga Watt, ICOS, Horizon State and Rentberry. It offers an enviable number of services to prospective ICOs – from white paper writing, to PR to technical and analytical strategy. The entire project looks significantly more professional than Tokenmarket, and undeniably offers a range of useful services to clients.

This is where the issues lie for Cryptonomous, however. While it offers an excellent business platform, it is lacking in the vision and the additional features that CrowdCoin brings with it – it is a fantastic platform for professionals and for the tokens themselves – whether it

works as well (and as organically) as the CrowdCoin platform, however, may be open to some debate, as once an ICO is completed, the function of the Cryptonomous platform is completed.

KickICO

KickICO represents the most relevance to CrowdCoin of any site currently available. It integrates many of the features that CrowdCoin brings to the table, but without the overall vision and comprehensive platform that CrowdCoin proposes to bring with it. This means that, although the site is admittedly still in the beta stages of the development cycle, it has not advanced to the level required to sustain itself in the face of a more advanced and complete platform.

Appendix C – CrowdCoin Masternode Technology: An In-Depth Examination

As the masternode technology is based on the system employed by DASH, there are a number of technical similarities between the two systems. However, CrowdCoin has refined the system, and added a number of enhancements to the existing framework.

Transaction Costs

The decrease in the number of full nodes that had occurred on the Bitcoin network, prior to the speculation bubble in late 2017, was the lack of incentivisation by the platform. This did not motivate users to participate in the network by running their own nodes. Over time, the cost incurred in running a full node increases exponentially as the network gains increased amounts of traffic. This cost is exacted in bandwidth and costs the operator more money to maintain. To counteract this rise in costs, many operators will attempt to consolidate their services in an effort to save money or attempt to run a 'light' edition of the client. This negatively impacts the growth of the network. Furthermore, the reduced number of transactions has increased the cost of carrying out each one.

This is the main drawback of the Bitcoin system. As demand for the system grows, the costs incurred in actually using the network to complete transactions also grow exponentially. As only a limited number of transactions can be inserted into the following block, it is necessary to pay a fee in order to have that transaction request validated. The highest fees will see the transaction receive preferential treatment. This means that if you have not bid sufficiently high enough, your transaction will be delayed. This can theoretically continue indefinitely, until network usage has dropped to the point where there is sufficient network capacity to insert your transaction into the block. Effectively, the Bitcoin system requires that users pay increasingly high amounts in order to have their transactions processed.

If your transaction is inserted into the next block, due to the low demand versus capacity (and if the queue of waiting transactions is diminishing), it incentivises you to offer less and less as a transaction fee each time. If demand for transactions is low, then the network enters into a race to the bottom without the need to pay for the services. Inversely, when a network is popular, the price of fees goes up and up as you need to pay more in order to be inserted into the next block.

Bitcoin has employed a fixed minimum transaction cost as a result of these developments. CrowdCoin (and the DASH system on which it is based), however, do not. When there is additional capacity on the network, transactions can be completed free of charge. While this *can* run the risk of transactions being delayed, with a network capacity five times that of DASH and Bitcoin, this should not normally be an issue. This keeps fees (when required) low and can help prevent spiralling costs for operators.

Should the need to address this system become an issue, it can be addressed, but this is not projected to happen for around the next decade.

The Masternode Reward Program

As previously discussed, masternodes constitute a full node, just as in Bitcoin. The primary difference, however, is that a masternode must provide a certain level of service to the network. It also requires a fixed collateral in order to participate, for security reasons. As long as the masternode remains functional, the collateral is not forfeited. This will earn interest on the network for the investors, which secures the value of the currency.

The masternode stores the collateral. While it is active, the node provides service to the network and, in return, receives a randomly assigned share of each block that is distributed amongst all masternodes. This will fund the cost of running the masternode, as well as earning a ROI, as the rewards are a fixed percentage, with half of each mined block. As the number of operational nodes is in constant flux, the exact sum of the reward is subject to change in accordance with this figure.

The payment for a standard day of operation can be calculated by this formula:

$$\left(\frac{n}{t}\right) * r * b * a$$

Where:
n is the number of masternodes an operator controls
t is the total number of masternodes
r is the current block reward (presently averaging about 20 CRC)
b is blocks in an average day. For the CRC network this usually is 720.
a is the average masternode payment (50% of the average block amount)

The ROI for masternode operation can be calculated as:

$$\left(\left(\frac{n}{t}\right) * r * b * a * 365\right)/C$$

C is the collateral needed for a single masternode

Assuming that the variables as the same as those above.

Trustless Quorums

As previously discussed, a trustless quorum prevents a 51% attack. With the addition of the masternode network and the collateral requirements, this secondary network can be used to conduct highly sensitive tasks in a trustless manner. This prevents any single entity from being able to control the outcome. By selecting N pseudo random masternodes from the total pool to perform the same task, these nodes can act as an oracle, without having the whole network do the task, thereby reducing the potential for malicious intent.

Roles

It is possible for malicious actors to misuse masternodes, by failing to provide the quality of service that is required for regular masternode operation. In order to reduce the likelihood

of this occurring, nodes must ping the rest of the network in order to remain active. This is performed by the network selecting two quorums for every block. Quorum A is responsible for checking the service of Quorum B on each block. Quorum A is comprised of the closest nodes to the current block hash, while B is composed of the furthest nodes from the selected hash.

Masternode A (1) checks Masternode B (rank 2300)
Masternode A (2) checks Masternode B (rank 2299)
Masternode A (3) checks Masternode B (rank 2298)

The masternode network itself is responsible for all examinations of active nodes. Approximately 1% of the total network will be checked per block. This means that the entire network is checked an average of six times per day. In order that the system remains trustless, nodes are randomly selected by the quorum. It also requires six violations for a node to become deactivated.

As the six-violation rule is in place, this would require an attacker to be selected six consecutive times in order to circumvent the security protocols.

Attacker Controlled Masternodes / Total Masternodes	**Required Picked Times in a Row**	**Probability of success** $(n/t)^r$	**CRC Required**
1/2300	6	6.75e-21	1,000CRC
10/2300	6	6.75e-15	10,000CRC
100/2300	6	6.75e-09	100,000CRC
500/2300	6	0.01055%	500,000CRC
1000/2300	6	0.6755%	1,000,000CRC

Table 1. The probability of tricking the system representing one individual masternode as failing proof-of-service.

Where:
n is the total number of nodes controlled by the attacker
t is the total number of masternodes in the network
r is the depth of the chain

The selection of masternodes is pseudo random based on the quorum system

Masternode Protocol[8]

Masternodes on the network are propagated by using protocol extensions. These extensions include an announce message for each masternode, as well as a ping message, broadcasting the location of the masternode to the network. These two functions will be all that the network requires to make a masternode active.

Once a masternode has been created, this will then allow the node to propagate across the network. A secondary private key will validate communications by signing all subsequent messages to the network. This also allows the wallet to function independently when in standalone mode.

The use of a *cold mode* is also possible when the private signing key is used on two separate machines. The *hot* client – the primary user– signs the 1000000 CRC input by including the key in the message. This then allows the receiving *cold* client to include the details and operate as a masternode. Once this has occurred, the *hot* client can be switched off safely, without any possibility of an attacker gaining access to the 1000000 CRC after it has been activated.

The masternode announcement message will contain:

Message: (1 000 000 CRC Input, Reachable IP Address, Signature, Signature Time, 1000 CRC Public Key, Secondary Public Key, Donation Public Key, Donation Percentage)

Every 15 minutes thereafter, a ping message is sent proving the node is still alive.

Message: (1000000 CRC Input, Signature (using secondary key), Signature Time, Stop)

After the expiry of a time-to-live, the network automatically removes all inactive nodes from the network. This will prevent the use of 'dead' nodes and prevent payment being made to them. Nodes also ping the network almost constantly, but if they do not leave their ports open to the network, they will become inactive and payment to them will be prevented.

It is for this reason that a public IP is a requirement for the operation of a masternode. This makes it unsuitable for users looking to run a masternode on a consumer-grade home network.

Propagation of the Masternode List

New clients that join the network need to be informed of the location of currently active masternodes in order to make use of them. As soon as a new client has joined the mesh, a

[8] GitHub. (2018). *dashpay/dash*. [online] Available at: https://github.com/dashpay/dash/wiki/Whitepaper [Accessed 7 Mar. 2018].

comment will be sent requesting access to a known list of masternodes from peer connections. Use of a cache object will facilitate the storage of this list, meaning that when a client restarts, the information can be simply retrieved instead of resending a request for the masternode list. This will improve the functionality of the network by reducing the need to wait for responses at every start-up.

Payments via Mining and Enforcement

When mining on the network, pool software (websites that merge the efforts of individual miners) use the RPC API interface to get information about how to make a block. To pay the masternodes, this interface must be extended by adding a secondary payee to GetBlockTemplate. Pools then propagate their successfully mined blocks, with a split payment between themselves and a masternode (GitHub, 2018). This prevents the system from being cheated by malicious actors.

CrowdCoin