BLOCKCHAIN AND CRYPTOCURRENCY

Blockchain-based Project Investment Framework

iMining Blockchain & Cryptocurrency Inc.

January 2020

Purpose

The purpose of this framework is to give investors and enthusiasts a guide to navigate the complicated, confusing, and increasingly risky environment that cryptocurrencies and blockchain related projects have turned out to be. The goal is to provide reference material that will help investors evaluate potential investments using critical thinking. This framework will also give investors, teams, institutions, and the public a look into how iMining views and evaluates projects that approach us. We hope you find this valuable.

Background

In the years following Bitcoin's release in 2009 there were numerous other blockchain implementations and ideas pursued. The nature of the environment allowed for this, and while many of the initiatives may have meant well, some were blatantly disingenuous and left investors with only their shirts. A large majority were and many still are either unintentionally, or unknowingly scamming many people.

The story begins like this, Bitcoin's creator[s], under the pseudonym Satoshi Nakamoto, released the code in its entirety through a private mailing list. The code eventually ended up on Sourceforge, and then Github, both web-services enabling collaborative programming efforts on free or open-source software projects. In 2011, Charlie Lee, a Google employee at the time, forked the Bitcoin code with some adjustments, notably faster block-times, greater supply of coins, and a different hashing algorithm[1]. He named this new currency Litecoin; as a silver to bitcoin's gold status.

Two years later, during the infamous bitcoin run-up, the market cap of Litecoin hit $1 billion[2]. We speculate many developers and software engineers following the Bitcoin project at the time noticed the potential alternative currencies (altcoins) could have as not just fun experimental projects, but speculative instruments to generate money. Today there are thousands of projects with coin listed on different exchanges[3]. What's concerning is that many most of these projects have unproven, or even unknown, teams, capabilities, track records, business models, or road maps.

While we acknowledge that there exists significant opportunity to generate great returns by investing in tokens and blockchain-based projects, it can be overwhelming to take the time to research these opportunities and often extremely risky. One must apply an understanding of finance, computer science, and have a solid grasp of economics to make an educated analysis. Sometimes you

---

[1] https://bitcointalk.org/index.php?topic=47418.0

[2] https://www.forbes.com/sites/reuvencohen/2013/11/28/cryto-currency-bubble-continues-litecoin-surpasses-a-billion-dollar-market-capitalization/#31acfde84548

[3] https://coinmarketcap.com/all/views/all/

may get lucky, but in reality the function of investors is to be consistent over long time horizons, which ends up consisting primarily of risk-management.

This problem has been compounded in this new wild-west of ICOs; instead of bootstrapping projects like bitcoin and Monero, projects are raising tens or even hundreds of millions of dollars using impressive graphics and websites, without having a line of code or complete vision worked out[4,5]. A recent paper from Boston College found that an estimated 56% of ICOs fail within the first 4 months after the token/coin sale ends[6].

The entire process of traditional due-diligence and business model scrutiny is removed. We are advocates for the efficiencies that blockchain technology can have on traditional finance and banking, but real utility is garnered from experience and skill in properly evaluating entrepreneurs and projects, which should not be discarded.

As a result, iMining has developed an internal framework in which we can evaluate different projects and proposals as a way to mitigate risk and avoid pitfalls common with the nature of this business. Below we offer a condensed public version that may help individual investors and institution in assessing potential projects. Some of the developed criteria will **not** apply to all projects, for example, ICO-structured endeavours have different goals and requirements.

Our Framework

[4] https://en.bitcoin.it/wiki/Mining
[5] https://diar.co/volume-2-issue-9/
[6] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3182169

People	What to Look For | Where to Look
Credibility	The team and/or contributors are known (or mostly known), and have a track record of success or contribution. Multiple links on website/forums to contributors GitHub pages to review and confirm they have contributed code. Core contributors are available for, and respond to, concerns and criticism.
Character/ Aptitude	The team has thought the project through thoroughly and have viewed potential obstacles/pitfalls from multiple perspectives. Project assumptions and projections are realistic and have solid rationale. Proposed financial requirement and current valuation are appropriate. The team is coachable.
Product/Service	**What to Look For | Where to Look**
Purpose	There is passion and motivation in the purpose of the project. The problem it looks to solve is meaningful and addresses a real pain point for a significant market. It doesn't take long to understand or realize why this project exists.
Utility	The project provides real value, creates a meaningful efficiency, or removes a significant barrier or pain point.
Feasibility	Given the assumptions made and resources required the project goals can be reasonably achieved.
Security Status (ICOs)	Project is not defined as a security as per the '**Howey Test**'.
Network	

Decentralization	The project has a well thought out plan for achieving decentralization (if applicable). The project has node and miners in different geographical locations, using various equipment from different manufacturers, in diverse political/regulatory environments, and hashing power/voting is spread.
Node Growth/Count	Node growth is healthy, numbers are increasing or have a strong amount for the stage of the project. Nodes are reliable; stay online and many are listening (open to connections).
Capital	What to Look For | Where to Look
ICO	Project avoids pursuing ICO route of fund raisins. (Some cases can make good business sense depending on the factors below and need for community support for network effect.)
Founder's Reward/ Token holdback	Team doesn't implement a Founder's reward, or it is well thought out and is a reasonable incentive mechanism. See the "Zcash & the founder incentive trilemma" for the difficulty surrounding this model[7]. Token holdback is not excessive based on the assumptions made. Majority of tokens/coins are available for purchase by users or outside investors.
Premine	The project avoids a premine, or distributes/allocates premined coins so as to avoid investor concern about manipulation. See the article "Instamine vs Premine" for more info[8].
Public Escrow Account	If running an ICO, the address is publicly available for audit and review. It's important participants know how much has been submitted. If there is private funding in addition to the ICO, this has been made public.
Capital	

[7] https://medium.com/@arjunblj/zcash-the-founder-incentive-trilemma-fe7689fc8293
[8] https://nulltx.com/instamine-vs-premine/

Use of Funds	A detailed allocation of funds raised has been documented. If project is running ICO, use of funds is public prior to launch and open to community feedback.
Timeliness of Token Release	Date is provided for when tokens will be issued to investors.
Liquidity	Token is listed, or will be listed, on multiple exchanges. Typically, exchanges have a criteria for listing that is less comprehensive than this. Additionally, exchanges often charge fees for listings, this has been thought out and prepared for.
Volume	If token/coin is already launched it has a healthy 24hr volume relative to its stage and existing top coins. See CoinMarketCap for aggregate coin volumes from different exchanges[9].

Economics	
Incentives	Project has a sound incentive structure for stakeholders in the network, miners, users, developers. This includes block rewards, founder's rewards, development fund, and network fees.
Issuance/Supply	There is a protocol level hard cap on number of coins that will be in existence. Inflation schedule/coin issuance is well thought-out. There may be rational for projects to not have a hard cap and have an on-going supply, such as with appcoins and in addressing non-negligible amount of coins gets lost or destroyed every year.
Technology	What to Look For | Where to Look
Free Software/ Open-source Software	If the project aims to be decentralized then it should be a prerequisite that the software be free or open-source software so as to ensure a robust, peer-reviewed codebase, or in the case of free software absolute liberty of use, modification, and distribution[10].
Technology	

[9] https://coinmarketcap.com/
[10] https://www.fsf.org/about/what-is-free-software

Proprietary Software/IP	If project is not focused on decentralization and is creating an efficient centralized system related to blockchain or cryptocurrency, then well documented or novel IP exists.
Code/Language	Code base is available for review and/or audit. Appropriate language and framework for given project. Preferably using microservices structure. Often difficult to evaluate without senior developer or engineer on hand. Available code is well documented and organized. Code, especially for protocol and wallets, has been stress-tested for vulnerabilities and other security risks.
Community	
Developers	Strong, diverse talent pool of code contributors. Code is not all equal, an engineer capable of writing software at protocol level is more valuable and much harder to come by than a front-end web developer. Active GitHub repository. See Bitcoin or Monero's repository as reference for healthy and active developer community[11,12].
Support	Large, growing community of advocates and ambassadors, often unpaid. Twitter, bitcointalk.org, and Telegram can be good places to look for this.
Governance	
Decision Making	The project, especially with regard to decentralized initiatives, has acknowledged the difficulty in governance and decision making in protocol level changes or improvements. A robust process of research, peer-review, discussion, and implementation has been documented and thought through. For insight and reference read Pierre Rochard's "Bitcoin Governance"[13].

[11] https://github.com/bitcoin/bitcoin
[12] https://github.com/monero-project/monero
[13] https://medium.com/@pierre_rochard/bitcoin-governance-37e86299470f

Glossary

Escrow Account - An escrow account in the case of ICOs is a cryptocurrency wallet (usually a multisig wallet), that accepts the funds submitted during a sale. There are usually more than one, typically one for bitcoin and one for ether. As these are on public blockchains the amounts sent and received are publicly available.

Multisig Wallet - A multisig wallet is type of wallet that enables N of M signature be required to spend from the wallet. For example, 2 of 3 multisig wallets require that 2 of the 3 account holders sign the transaction before funds can be sent. This feature is very popular with ICOs because they can use a 3 of 5 or another variation and give the keys of one or more signatures to a neutral 3rd party to avoid the team from stealing or losing the raised funds.

ICO - an Initial Coin Offering is the means of raising funds through an unregulated money first, product later structure. It is akin to a crowdfunding style where contributors and enthusiasts contribute money towards a project they support and want to see thrive. However, they do not own any stake in the company; the token does not represent equity. Historically, because these tokens or coins are listed and tradeable on exchanges speculation drives price and early investors profit off price run-ups.

'Howey Test' - The Howey Test, or an equivalent test, is an assessment performed on a transaction to determine whether or not it was an investment contract (making it a security), and falling under the jurisdiction of a governing body such as the SEC (Securities and Exchange Commission), or in British Columbia, the BCSC (British Columbia Securities Commission).

Standard form for the test is as follows:

1. An investment of money
2. In a common enterprise
3. With the expectation of profit
4. That comes significantly from the efforts of others

Premine - A premine is where the initial miner, usually the founder or founding team mine a significant amount of coins prior to public access or involvement.

Proof of Stake - Is an alternative consensus mechanism to the original proof of work that Bitcoin uses. It uses a stakeholder model where members or delegates must purchase or own x number of coin or token and keep them stored under certain specifications in order to vote on the validity of the blockchain's state. In many models of PoS, if delegates act poorly (ie. validate false/fraudulent transactions) or go offline, they can have their stake slashed. That's to say their staked coins will be burned or taken away, and the number of required coins to stake is non-negligible. For example, Ethereum is planning to migrate to proof of stake and expects requiring 1000 ETH ($578,000) in order to stake.

Security - A Security is a negotiable financial instrument that represents a type of financial value, usually in the form of a stock, bond, or option.

Token Holdback - Is the act of holding back a portion of tokens or coins as part of an ICO