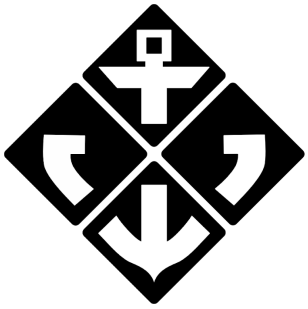

Atlantic Blockchain Company

Author : **Keegan Lee Francis**
Date : April 9th 2019
Website : **www.atlantic-blockchain.com**

Consultation Questions

1. There are additional questions that have yet to be asked
    a. Is “The Platform” jointly owned, or run, by anonymous individuals, as is the case with several Decentralized Autonomous Organizations
    b. Does “The Platform” facilitate illegal activity or serve a **censorship resistant** use case?
    c. Does “The Platform” implement any profit sharing mechanisms based on the performance and usage of the platform?
    d. Does “The Platform” implement dividend based profits from other securities held, or traded on “The Platform”.
    e. Does “The Platform” perform any locking mechanisms such as “staking”, “lending” or “collateralization”.
2. There are additional best practices not covered in the document.
   Exchanges should not allow fake volume to be generated. Although exchanges profit from the mechanism of creating fake volume (**90% of volume is fake**), it should not be a practice that is permitted on an exchange, or it should be openly transparent that fake volume is taking place. A common measure of success in a crypto project, is the amount of volume its associated asset has on exchanges. It is common for the project administrator to generate fake volume (at their own expense, and the profit of the exchange) in pursuit of generating sufficient “hype” to “moon” the price of their coin. Fake volume may be a signal for investors to buy an investment, identifying fake volume is one way to mitigate risk.

   Overall, this section was well put together, and rather exhaustive in the list of risks.

3. Wyoming is currently leading the regulatory framework battle of digital assets in a number of ways. Firstly, Wyoming has initiated a new classification of digital assets,

creating three new classifications for assets based on blockchains. A “Digital Security”, or investment contract, a “Digital Consumer Asset”, or utility tokens, and “Virtual Currencies” such as Bitcoin, Ethereum, and Monero.

This is a sensible, and reasonable approach for the regulation of blockchain assets. Each of these assets can then acquire property rights for holding, trading, and managing these three asset classes. With respect to investment contracts, the digitization of securities would allow for more advanced lending schemas to take place. For example, an entity holding stock in a company could use this stock as collateral for additional lending, without needing to involve the company that the stock actually pertains to.

Wyoming has enacted bill HB-70 Utility ICO bill which exempts Utility Tokens from being classified as securities, which is a common barrier for blockchain businesses to overcome.

Wyoming accepts state tax in Bitcoin and other cryptocurrencies, all the while, waving property tax for entities mining Bitcoin.

Wyoming has four rather progressive and utilitarian bills that just recently came into law.

- **Special Purpose Depository Institutions:** This is to create institutions to service blockchain companies that cannot access traditional banking services. However, these institutions are prohibited from providing loans and must maintain 100 percent of its deposits in its reserves. They must also comply with applicable federal laws.
- **Commercial Filing System:** This blockchain bill authorizes the Secretary of State to create a blockchain-based commercial filing system for business entity registration submissions and reports, certain financial statements, and other similar types of filings.
- **Corporate Stock Certificate Tokens**: This bill allows businesses in Wyoming to issue ‘certificate tokens’ on a blockchain rather than stock certificates. This way, they can choose whether to list certified or uncertified blockchain shares.
- **Digital Assets – Existing Law:** This classifies digital assets by type (virtual currencies or digital securities) and specifies how each one should be treated in the context of existing commercial laws. Wyoming banks can also opt to become custodians of digital assets under the terms of this bill

4.

Standards:

a. Multisignature wallets: The decentralized/multi ownership models for private keys. There are many schemas of “weighted” keys wherein a predefined threshold of “votes” are required in order to act upon a wallets funds. For example. A multisig wallet held between 3 people could be configured such that any 2 of the 3 individuals have the sufficient power to move/act upon the funds. Any 1 of the individuals would not have sufficient power to act upon the funds.

Furthermore, any one of the 3 aforementioned individuals, could also be a multi signature account, that requires approval/action from multiple parties.This is tiered ownership, and would enforce rigorous, and robust ownership models that are resistant to centralized control.

One example of a platform wherein these dynamic ownership models is possible, is within the EOS blockchain, where multiple key types exist, as well as the ability to create tiered and multi-weight ownership models.

In the example of the QuadrigaCX case of January 2019. One individual held 100% of the operational keys for the exchange, resulting in a multitude of problems when the untimely death of that individual occurred.

b. A “Dead Man’s switch” is a mechanism that would allow for a living individual, who becomes deceased, to safely and securely transfer their responsibility to a trusted 3rd party. An “analog” version of this mechanism would simply be a will, containing the private keys for assets, that is sealed, held, and kept safe by a trusted 3rd party, such as Estate Lawyers. This analog approach may work for some situations, but may not work with systems that have dynamically changing keys. With systems that change keys on a regular basis, this would be infeasible to keep up with on an analog level. A digital approach would be required, and even recommended for owners of exchanges, and large amount of individuals’ investments.

   I would draw attention back to the QuadrigaCX example of January 2019, to illustrate the practicality for such a system.

5. There exists platforms that fall under the category of a “DEX” or “Decentralized Exchange”. These are blockchains that do not have any form of centralized control, and therefore no centralized ownership. By definition, these exchanges lack an authority that speaks for, or represents, the ownership of all assets tracked, and held by the blockchain. Another term used to refer to these platforms is DA(O/C) (Decentralized Autonomous Organization/Company).

   These platforms are built, and used by participants of the system. Any interaction taken by any of the users of the system are permanently recorded by the system, in the traditional blockchain like fashion. All assets that are created, destroyed, and traded on the platform are publicly accounted for at all times, perfectly, transparently, and without error.

6. The **benefits** of an exchange not assigning a private key to each and every users’ accounts are as follows:

a. The platform and users avoid **blockchain** transaction fees for every transfer/exchange that takes place on their platform.
b. The platform is centralized, and can therefore leverage the speed of a centralized system for facilitating trades and exchanges on the platform. This is crucial with financial markets where seconds and microseconds matter deeply within the markets. The users of the platform benefit from the speed at which the exchanges can take place.

The **challenges** that an exchange faces by holding crypto assets are as follows:

a. There is an expectation for exchanges to keep up with blockchain events that result in “rewards”, “dividends”, or “additional profits”. These events include, but are not limited to, “Hard Forks”, “Airdrops”, “Dividends”. This becomes difficult for the exchange to manage, as additional programming and logic may be required to accurately and appropriately distribute the rewards that correspond to a user’s account balance.
b. Private key management inside an exchange is difficult as private keys are the aspect of a blockchain that determines the ownership of an asset. If an exchange has allowed for private key ownership by its users, then every exchange that takes place on the platform must happen on an address to address level (decentralized and slow), rather than an account to account (centralized and fast) level.

7. This is a very broad question. I am assuming the asker of the question is looking for any and all aspects upon which an experienced crypto-investor is evaluating an investment.
    a. Github Activity/Commits - This is a good indication of “progress” being made on the core underlying technology of a particular blockchain / coin / investment. This would be analogous to market activity, or development updates by a company traded on a regular stock exchange.
    b. Social Media - Reddit, Facebook, Telegram, Discord, Twitter, LinkedIn. Are there founding members, or representatives, on these platforms? Do they respond quickly and appropriately to questions and critiques? Do they have a good history of entrepreneurship and have they conducted a history of successful business based or technical endeavours?
    c. Founders / Team - Do they exist? Are they real people? Find the teams information, and make sure that the owner of the website did not put stock photos of “professionals” on the website. If they exist, is the team reputable?
    d. What does the asset do - Does the asset actually solve a real world problem? Or is it a problem that can be solved better, without a blockchain. If the asset is for a blockchain that a centralized system can solve better, then the asset is worth $0 and should be valued as such.
    e. Does the asset produce dividends - It is now becoming more common for blockchain enterprises to build into their token, the ability to distribute a portion of the profits gained from the blockchain itself. The daily / monthly / yearly dividend amount should rightfully be factored into the equation as to the price of the asset.

f. Does the underlying technology make sense - The underlying blockchain must be able to scale in order to handle the supposed use case. If the underlying technology does not scale well (cannot meet tx/s demand) then it doesn't matter how good the idea is, if mass adoption of the idea takes place, and the platform cannot handle the load, the entire system is virtually useless. Once a blockchain is started, it is technically difficult and complicated to "pitch fork" the assets to a different blockchain.

8. I am unaware of any reliable and unbiased pricing sources. There are plenty of sites that will tell you information about the asset, the team, and the market associated with the asset, but then fail to give a reasonable estimate of fair market value.

9. I believe it is reasonable for platforms to set and enforce their own rules. It is their system, they should be able to define their rules as they like, as long as they are compliant with their local regulations. Platform rules are some of the ways that platforms can differentiate themselves from their competitors. Some exchanges have games or competitions that take place on the platform where they give away prizes for particular actions taken by the users. (Ex. Referrals)

10. A Market Integrity Requirement should be that all reasonable effort should be given to identifying and preventing fake volume on the exchange. Such traffic is misleading and difficult for investors to interpret.

11. On private exchanges (exchanges owned by private companies) there does not exist a way for regulatory bodies to conduct surveillance on the exchanges that take place on the platform. There is no way to tell WHO is making the exchanges, only that the exchanges are taking place. Most exchanges have opened their "order books" through a public API (Application Programming Interface) for programmers to query and receive real time information about what trades are taking place on the network. This is the foundation for any and all "trading bots" that automated investors have implemented. The skills that are required for polling and analyzing this information is intermediate/advanced knowledge of any popular programming language such as JavaScript, Python, GoLang, etc, coupled with economic analysis tools.

12. A common strategy for trading crypto assets, is to base your trades off of secondary information such as the amount of people googling the word "bitcoin". In the past, there has been positive correlation between the price of Bitcoin and the volume of searches with the word "Bitcoin" in the query. The same methodology can be applied to search for trends in global social media platforms such as Reddit, Facebook, Twitter, and Instagram. This strategy is commonly referred to as identifying market "hype".

13. N/A

14. If the Platform is in possession of significantly large amounts of the asset that corresponds to the platform (example is Binance or BNB coin), then any large transfers and the details/conditions of such assets should be made publicly available as to inform users that there could be price fluctuations due to large amounts of such assets entering the marketplace.
    If there exists mechanisms within platforms that allow for users to “set the price” or publish a “price feed” for a particular asset, then this information should be made publicly available as to guard against this privileged user manipulating the price in their favour. (example is BitShare with SmartCoins or User Issued Assets).

15. A platform is not able to manage conflicts of interest if there is no central aspect of authority or control. The best example of this is BitShares or EOS wherein they are defined as DAO’s and lack any centralized authority. This opens up the opportunity for bad actors to take advantage of the lack of authority and manipulate sub-systems as they see fit.

16. Any and all insurances would be nice for an exchange to have, however, I don’t anticipate these insurances being reasonably priced such that the exchanges would benefit from obtaining them. At the moment, cryptocurrency in general is dangerous, volatile, and towing a rather bad reputation as a safe-haven for hackers. Making an insurance policy for exchanges that exchanges actually want to purchase would be more trouble, and more expensive than it is worth.

17. Articulated in 16

18. Proof of distributed authority, Key Management Systems, & Dead Man’s Switch. Articulated in 4a, 4b.

19. There exists other models of clearing and settling crypto assets. I’ve spoken about several of the exchanges that make this possible. BitShares and EOS both make all trades and exchanges publicly accessible on a public ledger. Everything, including the account name (which does not necessarily disclose the identity of the account holder) is published on the ledger which is publicly available. The risk of such a system is it inherits some of the properties of blockchain technology, one notable property is that the exchange is permanent and irreversible, whereas with a centralized exchange, there is someone you can call (support staff) if something doesn’t go the way you planned.

20. The risks are as follows:
    a. Permanent - All transactions that take place on DLT’s are permanent and irreversible. (Some exceptions exist)
    b. Anonymous - All transactions that take place on DLT’s are more or less completely anonymous, or difficult to ascertain the identity of the two parties.

c. Identity Fraud - It is much easier to fraud you identity in a digital ecosystem, than that of a modern established securities exchange. Such an implication opens the door to money laundering and other financial crime.

21. Black Swan events are market crashes that cause unintended side effects. There exists coins that are referred to as “Collateralized Stable Coins” which are massively complex systems of collateral that back an asset. The underlying asset that collateralized the stable coin is what upholds the value of stable coins. If the underlying asset crashes significantly, then there is a risk that a cascade of smart-contract triggers are fired, executing large amount of clearings and settlements. **Collateralized Stable Coins are a modern phenomenon worth grasping fully, and completely.** Stable coins have massive potential and geopolitical implications for the disruption of modern currency, more so than Bitcoin. What Satoshi Nakamoto purposed in 2008, is not what Bitcoin is today. Bitcoin behaves more like a stock or commodity, much like digital gold, as opposed to its intended purpose, a peer to peer digital cash/currency. Bitcoin is slow, and volatile, which currency is not. Stablecoins made the advent onto the world stage in 2014, but didn’t hit mass adoption (in the cryptosphere) until 2017/18.

22. N/A