CipherBlade

Blockchain Investigation Agency

MEMORANDUM

Bitbuy Proof of Reserve and Security Audit Report

Contents:

1. EXECUTIVE SUMMARY

On March 18th and 19th, 2019, CipherBlade CSO/Co-Founder Richard Sanders (author of this Memorandum) was present on site at the Bitbuy premises in Toronto. Prior to this visit, CipherBlade submitted a list of preparatory items to Bitbuy in order to streamline the review process and ensure all relevant items could be reviewed in a timely matter. The list of preparatory items was extremely extensive, and Bitbuy was able to ensure these items were ready, enabling this review to be conducted in full over the course of two days.

The review was conducted to evaluate solvency, proof of reserves, liquidity, cold storage policies, and staff risk.

The results were the following:

- All fiat holdings (custodial or otherwise) reported by Bitbuy were verified by bank statements and accurately reflected in the Bitbuy admin panel balances. Attestations by bank officers were made available for a second level of verification.

- There was a 100% match between a ledger of user account transactions and amounts in related accounts.

- The sum of digital assets held in Bitbuy's cold and hot wallets matched the sum of digital assets held across Bitbuy user accounts resulting in a 1:1 match of custodial assets. This process provided 100% Proof of Reserves verification of Bitbuy custodial assets.

- Based upon physical security conditions of the cold storage as well as the OPSEC-mindedness demonstrated by the Bitbuy team, Bitbuy's cold storage is unlikely to be compromised in any way.

- The pertinent accounts for liquidity were reviewed for corresponding transactions in line with best practice methodologies. These accounts were also reviewed for security. Bitbuy's liquidity accounts exceeded standards in both areas.

- Team background checks, past employment checks and ID checks were completed with no issues and no reason to believe that any current employee would compromise Bitbuy operations in any way.

Bitbuy aims to be a highly compliant and transparent trading platform, setting themselves apart from competitors that are not taking appropriate steps for regulatory and public confidence purposes. One of the steps Bitbuy has taken for this initiative is engaging CipherBlade to conduct this review.

2. BACKGROUND

As a response to an expected increase in regulatory oversight, and a lack of consumer confidence in the wake of recent events regarding QuadrigaCX, this report was focused primarily on:

- *Solvency:* The case of QuadrigaCX[1] illustrates how an improperly run exchange faces solvency risks on both fiat and cryptocurrency to the detriment of its clients. QuadrigaCX was not licensed as a Money Services Business (MSB) and has been reported to have handled its funds highly improperly, including the form of physical cash prone to disappearance; and during much of 2018, the exchange had no access to much of its fiat holdings, which had been frozen by banks due to apparent unclarity on the source of funds. After the disappearance of the company's founder (alleged to be deceased) QuadrigaCX appeared to lack not only sufficient fiat assets to cover client balances, but also cryptocurrencies, with much unclarity around which wallets even belonged to the exchange. QuadrigaCX publicly states that their missing, and allegedly deceased, founder was the only person to have control of its cold storage wallets - whose existence has never been verified in the first place. Adherence to proper procedures can minimize the risk of such a situation: fiat money should be managed to the standards required of licensed money services businesses (and a license as such maintained), and proper audited records need to be kept of all cryptocurrency assets and access modalities, which need to be tiered and redundant to prevent single points of failure.

[1] QuadrigaCX is a cryptocurrency exchange which filed for creditor protection after a series of peculiar circumstances, many of which have been viewed with skepticism: https://www.chepicap.com/en/news/7210/the-quadrigacx-timeline-as-it-happened.html. Despite uncertainty regarding all circumstances of QuadrigaCX, numerous security and transparency elements would have prevented this situation from unfolding if they were implemented in the first place.

- *Team risk:* The QuadrigaCX team had individuals that used fictitious names, likely in hopes of hiding questionable pasts[2], and had QuadrigaCX users been aware of these pasts, far less use of the QuadrigaCX platform (as well as trust in the custody of assets) would have taken place. A lack of due diligence on those responsible for running the QuadrigaCX exchange has resulted in industry-wide expectations of transparency for custodians of assets and money transmitters.The blockchain industry has matured to a point where anonymous teams fall under great skepticism. However, it has not yet reached a stage where the level of skepticism voiced and acted upon is sufficient to proactively thwart a replica of the QuadrigaCX situation. For example, the existence of a LinkedIn profile is not ample due diligence for an individual with access to large sums of customer assets. CipherBlade's opinion on best practice, which we convey to all exchanges and regulatory bodies, is that a bare minimum audit consisting of physical government-issued ID checks for all core team members and verification through pertinent databases (to include both IDs and general background checks) should be a baseline expectation going forward. Verification that the team has nothing to hide provides clout to operate these types of services, and verification that the pertinent team is utilizing real-world, attributable identity minimizes flight risk in the event of misconduct by the pertinent teams.

Other areas of focus will be included in this report, such as a cursory review of security measures and KYC/AML initiatives. These supplementary areas of focus were considered in order to assess

[2] https://news.bitcoin.com/quadrigacx-co-founder-michael-patryn-is-actually-convicted-fraudster-omar-dhanani/

regulatory risk to Bitbuy, and, subsequently, assist in decision-making for existing and potential Bitbuy clients.[3]

3. THE BITBUY TRADING PLATFORM

Bitbuy is a trading platform based out of Toronto, Canada, and has operated since 2013. Bitbuy serves as an online platform for customers to buy and sell Bitcoin (BTC), Bitcoin Cash (BCH) Ether (ETH), Ripple (XRP) and Litecoin (LTC). Bitbuy does not currently provide services for the purchase of other "tokenized" assets including any "ICO" tokens or "alt-coins". Bitbuy currently restricts its business dealings to Canadian resident clientele and transacts exclusively in Canadian and U.S. dollars with the proviso that it cannot exchange currencies on behalf of any clients.

Bitbuy users may deposit Canadian dollars and cryptocurrency to their account in the same process users would be familiar with from most major cryptocurrency exchanges. Bitbuy users may deposit fiat, exclusively CAD, to their account via bank transfer, Interac[4], and Flexepin. Bitbuy's fees are readily accessible on their website[5] and are relatively simple to understand.

Members of the Bitbuy team are public-facing[6] and all work out of the Bitbuy office in Toronto. Bitbuy is the core business unit of First Ledger Corporation (FLC,) a leading Canadian blockchain and digital currency

[3] These supplementary areas of focus were conducted while on-site due to permissive time. The initial scope of this audit (the primary focus areas) was expedited by a high level of client participation, enabling CipherBlade to review further areas of regulatory and public interest.
[4] Numerous Interac deposit methods are available for users to deposit CAD to their Bitbuy accounts.
[5] https://bitbuy.ca/en/fees
[6] https://www.linkedin.com/company/bitbuyca/people/

company. FLC's other lines of business include over-the-counter (OTC) digital currency trading, digital currency merchant solutions, and blockchain implementation consultation.

Adam Goldman, Founder of Bitbuy, originally called the platform InstaBT when he co-founded the service in 2013. His vision is to provide a quick and simple way for Canadians to obtain Bitcoin. Over the subsequent years, that company evolved into what is now known as Bitbuy.

4. THE AUDITOR

CipherBlade is a company that provides varied services, some of which include:

- *Blockchain Investigations:* The most well-known service CipherBlade provides is investigative services. Many clients are directed to CipherBlade via word-of-mouth referral after experiencing a scam or hack. CipherBlade has been a core component of numerous large-scale investigations, including the breach of influencer Ian Balina, in which CipherBlade assisted in tracking stolen cryptocurrency, exchange intercepts, investigation/evidence gathering on persons of interest, and fusing information that assisted in asset recovery and prosecution. A combination of on-chain and off-chain forensics is compiled into a report that provides law enforcement "what they need in a neat little box" - in essence, simplifying and streamlining next steps in resolving these matters. Reports from CipherBlade have shed insight to law enforcement on situations prior not identified, including an incident where hundreds of victims were affected by a keylogger

that was created by a nation state actor. CipherBlade's self-developed investigative methodology is perceived as cutting edge and best practice by law enforcement, of whom often consult with CipherBlade.

- *Expert Witness Services:* CipherBlade CSO and Co-Founder Richard Sanders is a credentialed expert witness in blockchain forensics and cryptocurrency cybercrime, and has collaborated with eight different law firms, with some examples including OTC disputes and ICO mismanagement. CipherBlade has provided clarity on highly complex blockchain situations to legal decision makers that were acquainted with Bitcoin mere days prior via reports simplifying blockchain data science.

- *Blockchain Security Advisory:* CipherBlade creates tailored cybersecurity plans for blockchain organizations, which tend to focus on asset security and counter-social-engineering initiatives,[7] as well as travel-PERSEC[8]-focused training.

- *ICO Services and Advisory:* CipherBlade offers sprint-based services and general advisory to ICOs. These services include elements in the Blockchain Security Advisory category from a complete life cycle approach, typically with community-focused oversight on fraud prevention. Contingent with ongoing participation in panels at conferences, boards for self-regulation, and sharing of insight (and proposed best practice) with regulators, CipherBlade also provides

[7] The majority of asset loss in the blockchain industry (excluding exchange hacks) stems from social engineering, such as impersonation scams.
[8] Some examples of training provided include conference-focused items such as MitM attack prevention and counter-ransom mitigation.

regulatory-centric advisory. CipherBlade provides these services for renowned ICOs, such as Dusk, Verv, Resistance, and ChromaWay.

5. COMPANY FILINGS / TEAM BACKGROUND / ACCESS LEVELS / BACKEND

The entirety of the Bitbuy staff, including customer support services, are retained on a full-time basis by the company; there are no functions currently outsourced. The Bitbuy team provided CipherBlade with scans of government-issued IDs for all members of their team. These government-issued IDs were visually inspected, then run through pertinent databases to confirm validity. All names presented by Bitbuy match the names presented on these IDs, and all IDs returned with a valid match in the queried databases.[9]

Scaled background checks were conducted on Bitbuy team members, with special emphasis given to Bitbuy team members that would have access to critical infrastructure. No criminal records, mental health records, or other indicators of risk regarding team member history were found.[10] These checks included randomly selected employment and education verification of Bitbuy team members.

While a lack of past history that would demonstrate an increased risk for malicious acts is not, in and of itself, a stopgap to malicious acts, it is certainly a fair expectation of the general public from teams running these

[9] These databases include the Ontario MoT PRIS system.
[10] These findings are confirmed again in Consent to Act as a Director paperwork, which includes a Canadian government investigation regarding bankruptcy status, status under the Mental Health Act or other findings of incapability by a court of law (Canadian or elsewhere) to perform these duties

types of services. Much more importantly, the fact this team is indeed who they claim to be, and operating in a jurisdiction that quickly verified this, the likelihood of both malicious acts and flight risk is significantly reduced.

It is publicly known that Bitbuy is a division of First Ledger Corp[11]. Bitbuy provided copies of their registration and incorporation to CipherBlade, which were verified, and may indeed be easily publicly verified[12].

Bitbuy also provided verification[13] of their MSB registration. A registered MSB (or specific country equivalent) is not only an indicator of a compliant business, but is an additional indicator of confidence in a lack of malicious actions from the pertinent team, as well as an increased likelihood of assistance from law enforcement (via Bitbuy collaboration) in the event of defrauding of a client. Exchanges that do not have or provide the equivalent credential may not be regulatorily compliant (contingent with jurisdiction), and it is worth noting that this regulatory status entails an extensive list of measures such as ongoing reporting to FINTRAC. In the current state of cryptocurrency exchanges, compliant exchanges file SARs (or equivalents), while less than compliant exchanges in questionable jurisdictions do just enough to fall below the international radar - perhaps responding to law enforcement inquiries to avoid subpoenas that would reveal more.

11

https://www.globenewswire.com/news-release/2019/02/04/1710014/0/en/Bitbuy-Continues-to-Scale-Despite-Recent-Events-in-the-Cryptocurrency-Industry.html

12

https://beta.canadasbusinessregistries.ca/search/results?search=%7B2606121%7D&status=Active

13 http://www10.fintrac-canafe.gc.ca/msb-esm/public/detailed-information/msb-details/7b226d73624f72674e756d626572223a3135343331372c227072696d617279536561726368223a7b226f72674e616d65223a224649525354204c454447455220434f52504f524154494f4e222c22736561263685479706 5223a317d7d/

Bitbuy provided all Consent to Act as a Director forms for FLC directors. In order for one of these forms to be executed, Canadian authorities conduct extensive vetting to ensure applicants are qualified for this responsibility[14].

Bitbuy provided copies of pertinent property and insurance documents to CipherBlade for review, which passed scrutiny.

Bitbuy discussed both onboarding and offboarding procedures for team members with CipherBlade, and provided example forms and process for the aforementioned. These steps ensure ex-employees (in particular, a hypothetical disgruntled ex-employee) would not have power or ability to disrupt Bitbuy operations.

It is a common error of many companies, particularly in the blockchain industry, to give team members "full keys to the castle," such as providing shared cloud storage credentials with access to critical data a respective employee would not need within the scope of their duties. This common oversight vastly increases the threat surface for such an operation.

Bitbuy shared a tiered access list with CipherBlade, which shows which team members can access particular items. These items are not limited to assets (which are discussed in-depth later on), but any items that would be of notable impact to Bitbuy operations, such as social media accounts, backends, records, etc. It is CipherBlade's assessment that the levels of access provided to each employee reflect the right balance between their job duties and security.

[14] https://corporationscanada.ic.gc.ca/eic/site/cd-dgc.nsf/eng/cs06643.html

Bitbuy's backend is secured by administrator accounts which have a data sanitization policy, password policy, stringent account creation and reset policies, and 2FA. CipherBlade suggested procurement and implementation of hardware based 2FA, and Bitbuy ordered appropriate equipment as advised by CipherBlade, with rapid implementation into their backend and changeover of pertinent accounts.

6. CLIENT DATA / KYC PROCESS

While on site, a new user account was created on the Bitbuy trading platform. A complete review of both user-facing and backend elements of this process was conducted in real-time. Elements of the registration process, including email and SMS aspects, were reviewed. The KYC process was reviewed as well. All elements of the Bitbuy KYC process passed regulatory and security standards.

One optimization CipherBlade proposed while on site was to require registering clients to include a piece of paper in their KYC photo stating 'For Bitbuy use only' with the current day's date. This process improvement would negate the likelihood[15] of stolen KYC credentials being utilized. In the highly unlikely[16] event of a breach of Bitbuy's KYC storage, stolen KYC documents would be far less likely to be usable elsewhere. In the far more likely event of individual Bitbuy clients being personally breached[17], this proactive measure vastly lessens the risk of identity theft.

[15] Upon review of thousands of leaked KYC documents and performing source attribution, some KYC images with similar "For entity use only" measures were attributed to being leaked from sources that were not the labeled entity. However, this is the responsibility of lackluster verification procedures from the breached entity (which should not have accepted these KYC images), and not from the initial source of KYC collection.
[16] A review of access to this storage, as well as future plans, was conducted, which found a level of security that exceeds standards.
[17] Based upon the frequency individuals are breached relative to exchanges

Bitbuy heard this optimization, developed a plan, and implemented it the same day CipherBlade suggested it. Optimizations of this nature are easily implemented with no downside, and demonstrate industry best practice. Exchanges which do not utilize these extremely easily implemented process improvements are not keeping a sufficient pulse on best practices.

As Bitbuy continues to scale, they have availed themselves to an outsourced KYC provider. This KYC provider has a customized set of deliverables they are providing to Bitbuy, which includes both the aforementioned limited-use element and further enhanced data storage. CipherBlade has reviewed documents between Bitbuy and this provider reflecting the aforementioned. Bitbuy's methodologies are in full compliance with FINTRAC regulations, including the credit file and dual process identification methods.

7. FIAT MANAGEMENT AND SOLVENCY

The new user account registered on-site at Bitbuy was utilized to demonstrate events which unfold on the Bitbuy backend contingent with user account transactions.

A demonstration of all fiat methods for this new Bitbuy account was conducted. These methods include Interac eTransfer, Flexepin and Bank Wire. The process of transferring funds to a user account was conducted with this fresh account, with a simultaneous review of the Bitbuy backend for each step of the process. Fiat transfers for user accounts are manually processed by Bitbuy staff. Bitbuy backend account balance changes reflected all user account balance changes with each step of this process for both fiat deposits and withdrawals.

Bank statements reflecting Bitbuy backend balances verified all fiat holdings (custodial or otherwise). Attestation by bank officer was made available for a second level of verification. All bank accounts are associated with the business, not an individual or external business.

Bitbuy currently realizes profit only in fiat (and does not charge for cryptocurrency withdrawals). This process is conducted with a periodic[18] scraping of balances, which segregates custody fiat and fee fiat prior to transfer to pertinent accounts. CipherBlade was present for one such scraping and reviewed the asset levels which Bitbuy should hold in custody, observed fees by deposit/withdrawal method, and the process in which these specific accounts are resolved. There was a 100% match between a ledger of user account transactions and amounts in related accounts.

8. CRYPTOCURRENCY MANAGEMENT AND SOLVENCY

The primary purpose of this review was to review Bitbuy's management of cryptocurrency held in custody and associated solvency. In light of this purpose, cryptocurrency management and proof of reserves were the most stringent audits performed.

As described earlier in this report, a Bitbuy account was created for purposes of this audit, in which cryptocurrency deposits were generated. Bitbuy's current infrastructure entails shared hot wallets across accounts, with timely manual verification for cryptocurrency deposits. As Bitbuy

[18] CipherBlade is aware of the frequency of the specific timeframe, however, the specific timeframe will not be included in this report for purposes of operational security.

scales, new architecture is planned in order to ensure continued timeliness of cryptocurrency deposits.

Under the current infrastructure, an audit of associated hot wallets is far more streamlined, as the quantity of these hot wallets is significantly decreased, and other elements that would be reviewed in an audit such as a review of creation of user-specific wallets was not pertinent.

Bitbuy user cryptocurrency deposits go to the hot wallet established for that particular cryptocurrency and reflect in account balance once manually verified. This process was reviewed for each cryptocurrency offered on Bitbuy via a transaction send to the Bitbuy trading platform, demonstration of the backend approval process, and subsequent reflection in the user account once approved.

The same process takes place for Bitbuy user cryptocurrency withdrawals: the request is initiated from the user, approved on the Bitbuy backend, and sent from the pertinent Bitbuy wallet to the user's requested wallet address once approved. A live execution of withdrawals for all cryptocurrencies Bitbuy offers was conducted, and corresponding hot wallets sent the requested funds to the requested wallets with expected balance changes.

A report was pulled from the Bitbuy back end which contained Bitbuy user accounts and amounts of cryptocurrency held by users on these accounts. The sum of cryptocurrencies held in Bitbuy cold and hot wallets matched the sum of cryptocurrencies held across Bitbuy user accounts, verifying a 1:1 match of custodial assets. This process provided 100% Proof of Reserves verification of Bitbuy custodial assets.

Satoshi tests were performed between all Bitbuy cold and hot wallets. These tests verified that Bitbuy owns the wallet addresses in question for the cold wallets[19] and served as a demonstration for the procedure in which Bitbuy transfers holdings between their cold and hot wallets.

Bitbuy retains cold wallets in a dedicated cold storage room with extensive physical security elements[20]. The specific criteria for transfer between hot and cold storages is determined based upon several factors, which include recent user activity. These transfers are conducted on a regular basis. Bitbuy demonstrated a transfer between hot and cold wallets to CipherBlade, which requires the presence of a minimum of two parties with the credentials necessary to access the room itself and initiate the transactions.

CipherBlade was not present for the establishment of Bitbuy's multisignature private keys, and an area of improvement would be establishment of hot and cold storages complete with key generation events with an external auditor present. In the current conditions, CipherBlade is unable to evaluate whether or not these keys have been compromised since their creation.[21] However, based upon physical security conditions of the cold storage (which would record any use of required hardware for these transactions) as well as the OPSEC-mindedness

[19] Ownership of Bitbuy hot wallets was demonstrated via user deposits/withdrawals.
[20] For purposes of operational security, precise specifics will not be provided. However, some examples include cameras which record to a redundant offsite storage, a door mechanism which only multisig parties have credentials for and which changes on a regular basis, tamper-proofing, and external view obfuscation.
[21] Credentials of this nature (information) do not need to be physically removed from one's possession in order to be in the possession of another individual. Based upon both the nature of blockchain technology and setup process leveraged by Bitbuy, CipherBlade cannot prove that these credentials have not been duplicated and subsequently that Bitbuy is in exclusive possession of the credentials.

demonstrated[22] by the Bitbuy team, it is CipherBlade's assessment that these credentials are unlikely to be compromised. There are numerous hedges to risk of malicious transactions outlined in previous sections of this report. A further hedge against unauthorized transactions is the establishment of wallet monitoring via transaction notifications that will notify members of the Bitbuy team as well as CipherBlade in the event transactions take place. In the event these transactions are observed as unauthorized, CipherBlade's network of exchange contacts as well as law enforcement will be notified for asset interception and seizure. Bitbuy has engaged CipherBlade to perform a post-audit review - at which time CipherBlade will be present for all seed and key generation events.

All cryptocurrency hardware wallets utilized by Bitbuy were procured directly from the pertinent vendors, negating risk of a supply chain attack.[23] All devices are stored in tamper-proof, serialized bags as an additional layer of security and for mutual accountability.

Bitbuy discussed a Key Compromise Protocol with CipherBlade, which has been further optimized with rehearsals.

Recovery seeds for hardware wallets were handwritten on paper[24] and are stored in separate bank safety deposit boxes at separate financial institutions, which both require the presence of two Bitbuy directors to access. Bitbuy has established business continuity plans in the unlikely

[22] The Bitbuy team retains the credentials required for their particular portion of the multisignature process on their person in serialized tamper-proof bags. This methodology makes individual credential compromise highly unlikely.
[23] Receipts were provided to CipherBlade to substantiate this portion of the audit. Receipts for computers the hardware wallets are utilized on, as well as receipts for varied other relevant items, were presented as well.
[24] This is a safer method than printing, let alone storing as a digital file.

event three of the four Bitbuy team members with this access level pass away.

CipherBlade suggested the minor optimization of transitioning the recovery credentials to steel,[25] and BitBuy has since procured the necessary items to execute and has made this transition. The Bitbuy team escorted their auditor to multiple banks to review the bank safety deposit box access process and confirm the presence of these credentials, which are also stored in serialized tamper-proof bags, further hedging unlikely risks.

A review of Bitbuy's liquidity process was conducted as well. The pertinent accounts for liquidity were reviewed for corresponding transactions in line with methodologies established prior in this report. The pertinent accounts were also reviewed for security. Bitbuy's liquidity accounts exceeded standards in both areas.

Despite the aforementioned aspects of Bitbuy's profit-realization model (via fiat), a review of Bitbuy's non-custodial cryptocurrency holdings was performed as well, with the same conditions utilized to review aforementioned cryptocurrency holdings. These assets also passed security and management scrutiny.

9. SUPPLEMENTARY ITEMS OF REVIEW AND SUMMARY ASSESSMENT

While the scope of this audit was not designed to inherently review items such as AML implementation or in-depth physical security, a cursory review of these and other varied areas establishes further data points for

[25] While bank safety deposit boxes have levels of fireproofing, storing recovery credentials on steel is a best practice due to being offline, fireproof, and waterproof: https://medium.com/changelly/hardware-wallets-101-88442ac385b2

the public to determine appropriate trust levels for the Bitbuy trading platform. The preparation conducted by the Bitbuy team for their solvency audit enabled high-level reviews of these varied other areas to be executed.

The physical security of the Bitbuy site was reviewed by CipherBlade. Some elements of review included a complete audit of site perimeter, entry mechanisms, access logs, access capability (to include property management and vendors), and varied other physical security metrics. The physical security of the Bitbuy office passes standards one would expect of a trustworthy cryptocurrency trading platform. CipherBlade did note several aspects of physical security which could be optimized, which are pending future implementation. However, none of the aforementioned optimizations pose a large nor likely security risk, and the aforementioned optimizations are primarily in line with future growth of the Bitbuy trading platform.

Various members of the Bitbuy team held conversations with CipherBlade in which hypothetical questions were asked, such as "what would you do if you received a file with an unknown or unexpected extension type?" All answers to these questions passed security scrutiny, indicating the Bitbuy team is cognizant of best practices such as sandboxing and prevention of social engineering. Bitbuy accounts, including email accounts[26], are not prone to SMS reset (and subsequent susceptibility to sim-swapping).

As outlined earlier in this report, Bitbuy is a MSB and subsequently responsible for fulfilling an extensive set of requirements in order to maintain adherence to regulations. Bitbuy provided CipherBlade with

[26] This includes the use of personal recovery emails (which administrators would not have oversight of settings for) being used to reset corporate accounts, negating this common sim-swapping tactic.

pertinent AML/KYT ("Know your transaction") policy documentation for review. Bitbuy demonstrated parameters that would trigger a transaction and account for manual review, as well as demonstrated their processes for handling of assets and accounts in question.

In addition to demonstrating past fulfillment of FINTRAC reporting criteria, Bitbuy takes initiatives which, while not required, demonstrate a level of perceived importance of, and interest in combating, money laundering. Some of these initiatives include required team-wide AML training, conducted on a minimum bi-monthly (often monthly) period, for which notes and training material were shown to CipherBlade. Bitbuy has also procured numerous tools to be more than just compliant, such as KYT software solutions. These efforts are demonstrative of an organization that has correct priorities and will subsequently have a much higher likelihood of continuing operations than exchanges that do not take such additional steps.[27]

10. CONCLUSION

As outreach from regulators[28] continues while the blockchain industry defines itself, the opportunity to establish self-regulation best practice is present now more than ever. Many in the blockchain industry claim to desire a minimal amount of regulation, and the only way to make this desire a reality is by blockchain companies being held to a higher standard

[27] It is extremely common for blockchain projects, most commonly ICOs, but also exchanges, to spend substantially more money on aggressive marketing than on areas such as compliance/legal or security.
https://medium.com/cipherblade/horrifying-truths-of-cybersecurity-in-blockchain-e2d71a39f836?source=friends_link&sk=c40ff267fdb2311c8c973b9acc5e394a

[28] https://osc.gov.on.ca/documents/en/Securities-Category2/csa_20190314_21-402_crypto-asset-trading-platforms.pdf

and self-regulating. Cryptocurrency users must speak with their money and utilize highly-compliant, risk-averse exchanges, and avoid exchanges with red flags such as anonymous teams and a lack of transparent oversight on key areas like solvency to the extent they are ran out of both relevancy and business. The responsibility to avoid over-regulation is shared both with cryptocurrency exchanges and users of cryptocurrency.

Platforms like Kraken[29] and Bitbuy which proactively demonstrate transparency are setting a precedent of expectations for a more mature blockchain industry. As an industry, steps of this nature are something we are currently not seeing enough of, yet are required steps to be taken if mass-adoption is to be realized. As Kraken suggested, the utilization of an (external) trusted auditor and publicly-verifiable records represents an ideal balance between privacy and transparency.

[29] https://www.kraken.com/en-us/proof-of-reserves-audit

ITEM REVIEWED	PASS/FAIL	REMARKS
Team IDs through government databases	✔	Mostly drivers licenses, which were ran through RCMP. Three passports which were ran through other systems. All came back with match in database including names, verifying public-facing names are accurate.
Team employment history	✔	Seven employers (selected contingent with relevance to role) were called to confirm employment history. All were confirmed.
Team background checks	✔	No records exist that indicate any Bitbuy employee has a history of fraud or any other type of charges that would indicate heightened risk given the responsibility of employment by this type of business.
Company policies	✔	Onboarding/offboarding, data sanitization, 2FA, password reset, site access, training on AML and cybersecurity, critical incident response, and numerous other policies were verified as existing and implemented.
Asset access tiers	✔	Team member access to varied items (both digital and physical) were verified as sensible within the scope of their duties.
Asset access requirements	✔	Access to the most critical solvency-specific assets are met by implementation of multisig and physical access requirements.
Credential storage	✔	Methodology for credentials related to all sensitive items exceed security standards. Varied risk factors, such as physical security and supply procurement, all passed scrutiny.
Secure redundancy of access credentials	✔	Redundancy of credentials was confirmed (negating the possibility of one individual's untimely passing resulting in a lack of access to assets.) Methodology

		behind this redundancy was confirmed secure.
Cryptocurrency solvency	✔	Collective client account balances were confirmed 1:1 for Bitbuy cryptocurrency balances.
Fiat solvency	✔	Collective client account balances were confirmed 1:1 for Bitbuy fiat balances.
Client information handling	✔	Collection and storage of client information was verified as secure. Bitbuy is compliant with regulatory measures for data sharing with authorities (in particular, FINTRAC reporting) and implements supplementary AML initiatives.
Company registration, licenses, and accounts	✔	Company registration/incorporation documents verified. MSB license verified. Bank accounts verified as being registered under applicable business names and types.