Trusted Bitcoin Ecosystem White Paper

A non-technical summary of the proof-of-concept to enable regulatory compliant Bitcoin transactions

June 2017

pwc

Table of Contents

1. Introduction

Non-fiat digital based currencies such as Bitcoin, are setting the stage for mass innovation

Non-fiat, digital currencies like Bitcoin are bringing legitimate challenges and innovation to the banking and financial services industry. Their appeal is broad as they have the technological capability to support a variety of innovative uses cases, from the introduction of a new form of money, to innovative payment rails, and programmability or 'smart' money. They are a cornerstone to any digitally enabled society and financial market.

Encouraging their development is key to enabling a future of truly digital based banking as well as driving innovation in the existing banking environment, which is sorely needed. Non-fiat based currencies are presenting the opportunity for new FinTech entrants to create new products and services and encouraging incumbent banks to explore and experiment in new ways of working.

Despite their highly innovative technology, the inability to satisfy current regulatory regimes have limited their mainstream adoption

Despite the rapid growth of Bitcoin and other cryptocurrencies, many mainstream organisations have chosen not to engage or adopt them. The biggest and often articulated challenge is Bitcoin and its inability to satisfy regulatory requirements (e.g. Know Your Customer - KYC, Anti-Money Laundering - AML, sanctions checks) due to the anonymous nature of users on the protocol, which is by design, and as a result, the anonymous nature of transactions. This presents an almost impossible situation for a bank to perform identity based checks, identify bad actors and manage compliance risk. Without creating new technology to address the problem, the lack of trust in Bitcoin remains a huge obstacle for mainstream adoption.

Developing secure and robust technology to help digital currency meet regulatory requirements, will set the groundwork for wider economic value and adoption

To address Bitcoin's (and other cryptocurrencies') inability to comply with existing regulation, new technology must be developed. This technology must cover a wide range of functions including identity management, compliance management, transaction management and reporting and analytics. By doing this, mainstream banking and financial institutions can provide safe and compliant services to its customers that want to start transacting in Bitcoin. It is here where Bitcoin can legitimately and safely scale to the masses.

To address this opportunity, an experimental proof-of-concept (PoC) was conducted under a Monetary Authority of Singapore (MAS) FinTech innovation programme by a consortium consisting of PwC, leading FinTech startups and a major global bank. The goal of this PoC was to develop a 'Trusted Bitcoin Ecosystem'

In late 2016, this consortium developed a platform to enable fully compliant Bitcoin transactions. The purpose of the PoC was to prove that identity could be provisioned against Bitcoin wallets and transactions and as a result, could comply with regulatory requirements (e.g. KYC, AML, Sanctions checks, etc.).

This white paper, which is a summary of the PoC, is intended to provide key learnings to further drive innovation in the the safe and transparent use of cryptocurrencies in the region.

2. Executive summary

The hypothesis:

PwC can demonstrate key components of a secure and technically rigorous trusted Bitcoin (and other digital currencies) Ecosystem

- Digital currencies are setting the stage for mass innovation and provide the opportunity for advancing financial services.
- However, there are challenges around the technology which limit its mainstream adoption including volatility (not part of this paper), reputational risk and transparency of actors on the networks.
- Developing new secure, robust technology and standards to support these currencies and their protocols will address these challenges and begin setting the groundwork for wider economic value and mass adoption

The opportunity:

Opening up the Singaporean market and neighbouring regions for digital currencies in a safe, trusted and compliant way. There is an opportunity to be the first market to embrace cryptocurrencies as an advancement in financial services maturity and create safe economic growth.

- Mainstream banking and other financial institutions that need to provide safe and compliant services to its customers, can start the next generation of monetary transactions with cryptocurrencies such as Bitcoin.
- To achieve this, new technology in identify management, compliance management, reporting and analytics must be developed.
- This new technology must ultimately protect the customer and the financial system represents an opportunity for Bitcoin to scale to the masses.

Key findings

The foregoing PoC developed new, innovative, secure, robust technologies and standards to support new cryptocurrencies and other digital currencies and the challenges associated with user identity and transaction transparency. The learnings of the project can set the groundwork for wider economic value and mass adoption of these currencies

- Identity can be applied to Bitcoin transactions and a controlled environment can be established to monitor transactions to comply with regulatory requirements.
- There is a basis for mainstream banks and financial institutions to be able to provide safe and compliant Bitcoin and cryptocurrency services to its customers, which can lead to new financial products and services.

Recommendations to MAS and future opportunities within trusted crypto currency ecosystems

There is now an opportunity now to open up the Singaporean market and neighbouring regions for digital currency use in a safe, trusted and compliant way. MAS have the opportunity to be the first market to embrace cryptocurrencies as an advancement in financial services maturity and an opportunity to create safe economic growth.

- Set the foundations to create the first global standards for digital and cryptocurrencies and help encourage and create new financial product and services opportunities (e.g. derivative cryptocurrency Investment and trading markets - asset, currency, derivatives, etc.)

- Use these findings to continue exploring other use cases for cryptocurrencies such as new payment rails including remittance (domestic/FX), merchant/Point-of-Sales (PoS) systems or even central bank backed digital currencies.

- Continue encouraging exploration amongst FinTech players and incumbent financial institutions to develop integrated, production ready systems for Bitcoin and other cryptocurrencies in general.

3. Bitcoin ecosystem challenges

Key Messages:

- Bitcoin was originally designed to ensure privacy as well as anonymity. However, this has presented challenges for mainstream financial institutions who must operate within regulatory boundaries
- Cryptographic keys, one of Bitcoin's core security features is both an asset and vulnerability. It is a powerful mechanism, but also a single point of failure
- When ensuring a safe and secure environment, it important to recognise that 'how' the technology is implemented is as important to the technology itself

Below we discuss a selection of the ongoing challenges facing those interfacing (e.g. financial institutions) with the Bitcoin ecosystem. We will leave aside well known discussions about price volatility, throughput, scalability, transaction fees, and energy consumption. Although, all of these pose legitimate threats to the cryptocurrency's viability and adoption in the long term, they are theoretically solvable. The items below, however, are of particular concern to financial services businesses and regulators.

Privacy vs. Compliance

As discussed earlier, one of the design choices of the Bitcoin protocol concerns privacy: users are to be able to transact Bitcoin with other users without either being required to divulge their identities or fear their identities being discovered. There are, of course, upsides to this feature: user data cannot be intercepted by a third party beyond which is simply stored on the blockchain, which therefore provides a strong privacy measure.

However, there is a trade-off. Since counterparties to Bitcoin transactions cannot be readily identified, not only does Bitcoin pose compliance liabilities through the inability to properly perform KYC (Know Your Customer), AML (Anti-Money Laundering), sanctions and OFAC (Office of Foreign Assets Control), and travel rule checks, but it is also very difficult to identify illicit commercial activity.

For privacy/security reasons, most contraband merchant sites will not even allow users access unless a VPN and TOR are utilised. They ecommend spending to wallet destinations via "washers" designed to disguise senders and recipients (similar to money laundering via shell/shelf companies). The same measures could be taken by those financing terrorism or other illegal activities. Bitcoin's main point of failure in this regard has tended to be "cash-out points" where users can convert Bitcoin to more liquid assets, but these too are notoriously hard to identify.

Partly for these reasons, the risks of enabling customers to use cryptocurrencies have offset any potential benefit for financial institutions. Perhaps ironically, some banks have been willing to invest in Bitcoin companies, but are largely unwilling to take them as customers. Even secure on-boarding of customers is insufficient to guarantee that funds acquired or deployed have not violated the travel rule and IMT regulations, among a range of other customary international regulations. It is very easy to obtain Bitcoin wallets on the internet or mobile app stores that require no onboarding procedures whatsoever and from which one can spend free of oversight.

In the final analysis, privacy and compliance are tradeoffs in permissionless ecosystems and privacy is not something that can be legally or technologically enforced, strictly speaking. This means whatever measures one uses to curb illicit behaviour, by design the underlying technology enables circumvention.

However, from that point of view Bitcoin is no different from cash instruments and in a sense may even be better for financial institutions. Whereas cash secretly spent or laundered cannot be tracked by definition, digital currencies afford the possibility that their owners can be.

Asset security and vulnerability

The Bitcoin protocol uses elliptical curve cryptography to secure owners' assets. An owner is represented on the Bitcoin blockchain by one or more pairs of private and public keys. By analogy to a cheque, one can think of a private key as analogous to an account number and the public key as a routing number. Both keys are required for management of one's Bitcoin assets: the former, which never directly touches the blockchain, is required for spending transactions, whereas the latter, which is visible on the blockchain--is "where" one sends bitcoin in order for it to be reassociated with a new private key, and hence a new owner.

This approach offers an important benefits and liabilities. On the one hand, the fact that users can be represented by cryptographic key pairs enables both user privacy and the asset security. Key pair creation is a purely mathematical construct which requires no need to divulge personal identity information whatsoever. Yet since a private key never directly touches the blockchain and nigh derivable from the public key, it is virtually impossible to compromise Bitcoin ownership from within the blockchain itself. Both identity and assets are incredibly secure.

At the same time, this also means that access to, usage of, and protection of one's private key is the single point of failure. At the simplest, this means that once the key is lost, it cannot be reconstituted, which means strictly speaking one's Bitcoin is no longer accessible, it is truly lost. It also means that Bitcoin cannot be seized unless one obtains that key.

For most users, this poses an additional challenge. Using bitcoin requires the ability to run actions via command line, which means most users *need* 3rd party clients to make using bitcoin simpler. Using a client implies trusting another entity with access to or the provisioning of account details, in effect, mediating one's access to the ledger, the very thing Bitcoin's "trustless" design meant to avoid. Mediation therefore necessarily poses additional vulnerability. Unless one's access to Bitcoin is direct, there are always risks of unsavoury vendors or products. What's more, this also means that Bitcoin is just as vulnerable to phishing, 'man in the middle' and other attacks that plague existing systems since both rely on clients and middleware.

Key focus areas to address

For the reasons above, Bitcoin hacks have less to do with insecurity in the protocol than the challenges of making it accessible to non-technical users. Indeed the vast majority boil down to poor key management or fraud perpetrated by third parties. Proper key management and other best practices will be discussed later in the white paper, but even all the most recent Bitcoin hacks boil down to these failures or their derivatives. The critical learning for us here is to understand how to effectively and safely implement this technology as well as any other technologies that present major security challenges.

In summary, the foregoing challenges suggest Bitcoin service providers must pay avid attention to a few key areas to ensure adequate compliance and security. These include the following:

- Defining what constitutes whole or partial "custody" of permissionless digital currencies, what role service providers want to play, and the corresponding liability?
- Secure onboarding and identity management.
- Procedures for identifying and actioning on illicit transaction behaviours (e.g. money laundering, tax evasion)
- Transaction monitoring, interception, actionability
- User key management and funds recovery

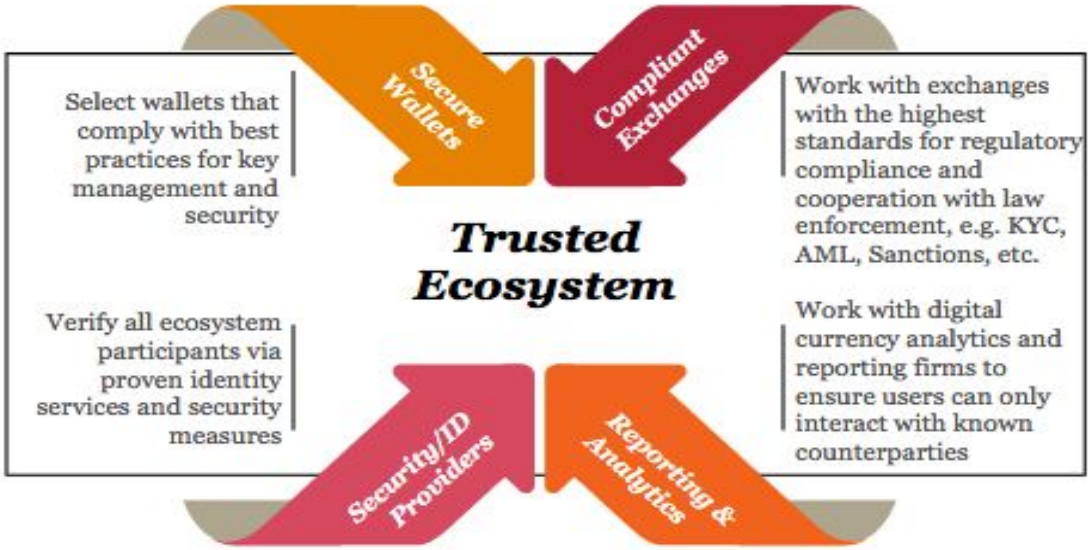
- Ensuring software clients (wallets, etc.) are secure
- Risk mitigation procedures in the event of successful attacks

4. How the Trusted Bitcoin Ecosystem works

Key Messages:

- The platform combines secure wallets, digital identity, integration with compliant exchanges and robust reporting and analytics to create a Trusted Bitcoin Ecosystem
- Compliant Bitcoin transactions are achieved by provisioning identity onto anonymous Bitcoin addresses and therefore enabling required compliance checks
- The platform has the ability to manage risk and control the execution of transactions by verifying the user's provisioned identity and once verified, 'co-signing' the transaction

4.1 What is the Trusted Bitcoin Ecosystem?



PwC was inspired partly by the desire to make permissionless digital currencies like Bitcoin compliant by alleviating the challenges discussed above. The PoC with the major global bank was to test the platform's effectiveness and, based on our results, offer concrete feedback on how financial services might make room for bitcoin and similar cryptocurrencies. Although Bitcoin's future remains uncertain, there is nevertheless renewed interest among financial institutions to enable customers to use them for investment, payments, etc., yet the compliance risks still pose significant barriers. The platform and the resulting Trusted Bitcoin Ecosystem were intended to fill this gap by providing a space where users could securely on-boarded, use bitcoin safely, and provide financial institutions tools for ensuring the integrity of their own customer base and the ecosystem more broadly.

Simply put, the Trusted Bitcoin Ecosystem enabled authorised entities to onboard new users, perform KYC, AML, sanctions, and PEP (politically exposed person) checks, giving them a Bitcoin wallet uniquely tied to their personal identities via a digital certificate. These wallets have the ability to buy, sell, and transact Bitcoin only with other onboarded entities. What's more, the Ecosystem also provides user, admin, and compliance tools that allow various stakeholders to view transactions as well as report, halt or

cancel potentially suspicious ones.

The Trusted Bitcoin Ecosystem describes the environment where parties can transact Bitcoin while satisfying regulatory requirements (e.g. KYC, AML, sanctions and PEP checks). Specifically, the Trusted Ecosystem provides the ability to successfully onboard, buy, sell, send and receive Bitcoin in a compliant manner.

The Trusted Bitcoin Ecosystem was developed in collaboration with PwC, several leading FinTech startups and a major global bank. This collaboration of partners and the integration of their technologies enabled the successful creation of the Bitcoin the Trusted Ecosystem.

4.2 Components of the Trusted Bitcoin Ecosystem

To achieve the Trusted Bitcoin Ecosystem, several core components are required:

- **Wallet** - the wallet plays several core roles within the Ecosystem including onboarding, executing buy/sell functions, executing send/receive functions and maintaining the customer's private key (using multi-signature technology). The wallet was built using as a base the open source Bitcoin wallet - *In the diagram on the following page, "Mobile Wallet"*

- **Identity service** - the identity (and compliance) service is responsible for provisioning ID and the associated ID verification and compliance related checks. If the checks pass, then a digital certificate is issued which is then required for transactions to be processed in a compliant manner - *In the diagram on the following page, "Cert Auth", "Compliance", "Certificate Svc", "S&F Svc" and "Sanctions Svc"*

- **Co-Signer** - the Co-Signer is the key component of the platform that processes (i.e. cOunter-signs) transactions based on whether certificates are present, meaning identity is present and compliance checks have passed. It possesses a second private key (in the multi-signature environment) to sign transactions. - *In the diagram on the following page, "Co-Signer Svc",*

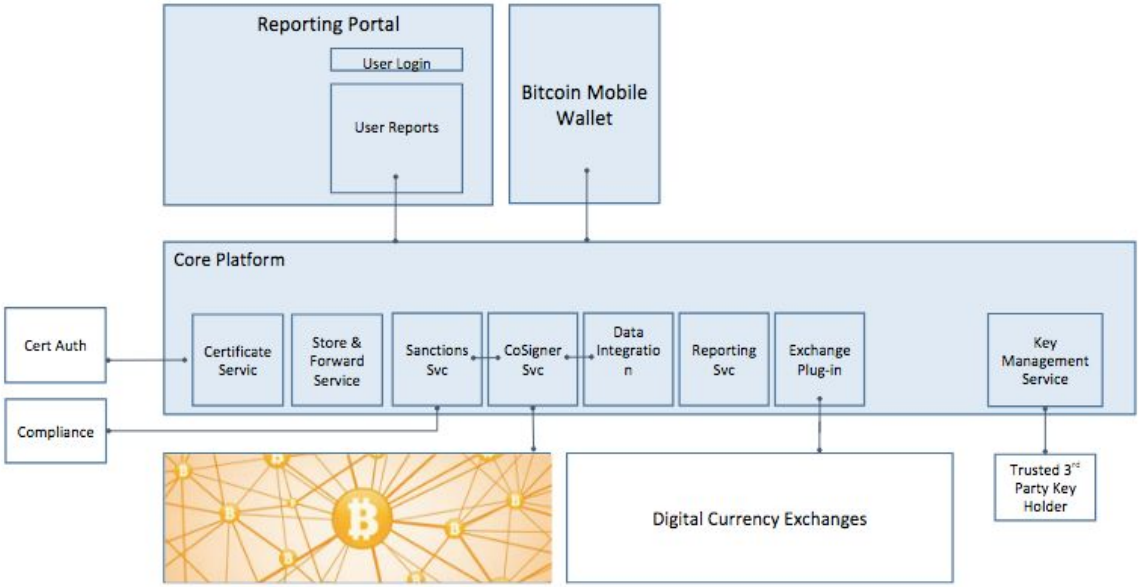
- **Exchange integration** - the platform integrates with digital currency (e.g. Bitcoin) exchanges to allow users buy and sell Bitcoin with fiat currencies. Exchanges themselves undergo due diligence before integrating with the platform. The exchanges themselves also have to satisfy compliance requirements in their respective jurisdictions which further ensures trust in the system. - *In the diagram on the following page, "Exchange Plug-in",*

- **Reporting platform** - the reporting platform captures and presents all transactional data flowing through the system. Its purpose is to supply financial, operational and compliance related reporting[1] - *In the diagram on the following page, "Data Integration" and "Reporting Svc"*

- **Key management service** - the key management service (outside of the scope of this PoC) manages the cryptographic keys required in the platform. This will include, among other things, the Co-Signer's key and a 3rd key or "rescue" key in the event a user loses their phone or wallet. The proof-of-concept only tested a 2 key multi-signature process. A PoC for the key management service is discussed later in the white paper - *In the diagram below, "Key Management Svc",*

[1] The reporting platform does provide the ability for administrators (e.g. the financial institution or the regulator) of the platform to view the contents of transactions, however this can be configured to not do so if required by regulation or other requirements. The platform does not intend to provide blanket access to any administrator. Without this platform, transactions would still be viewable from the blockchain, but only in an anonymous, unidentified form.

The diagram below summarises the core components of the platform and how they interact with each other.



4.3 How compliance can begin to be achieved in the trusted ecosystem

Note: Throughout the white paper, we will refer to KYC and PII. To ensure clarity,

- *KYC (Know Your Customer) requirements will generally cover processes related to identifying and verifying customers. This includes verifying personal information or government credentials*
- *PII (Personal Identifiable Information) is information that can be used to identify individuals and can include names, addresses, contact numbers and passport numbers*

Provisioning identity is the foundational step to enabling compliance

As described in the Bitcoin ecosystem challenges, identity is not required to transact which in turn, challenges the ability to achieve even basic regulatory compliance. To solve this, the platform forces a user to onboard and register their identification, which can then be used to satisfy compliance checks. The onboarding process fundamentally creates a customer identity associated with the wallet and a wallet name. The following steps summarise how the platform provisions identity:

1. Users must create a wallet name that associates a descriptive name to their wallet and Bitcoin address (to supplement the 34 character alpha-numeric address). For example, the customer can name their wallet "Bob.Wallet" or "PwCWallet1" that correlates to their key pair so that the customer never has to directly engage the latter.
2. The wallet name is part of the overall customer identity, but is the main identifier for transactions within the trusted ecosystem. This approach makes it easier for users to send to one another.
3. Users then enter in personal identification information--such as first name, last name, address and date of birth--required to perform proper KYC prior to authorising the wallet for use on the ecosystem. These checks can the be repeated on an ongoing fashion, even on a per-transaction basis.
4. Lastly, users include a government issued identity document for personal verification. In the case of the proof-of-concept, a driver's license was used

5. This data is then utilised by our back-end ID services to certify that a user is authentic and can legally participate in the ecosystem.
6. This information and process now form the basis of a customer's digital identity.

With identify established, compliance related checks can be performed and transactions can be controlled

With a digital identity created that includes granular personally identifiable information ("PII"), verification against various identity sources, watchlists or other regulatory related sources can occur. For the purposes of the proof-of-concept, KYC, PEP and Sanctions checks were performed. The following key points summarise the platform's compliance checking capabilities as well as its ability to control transactions based on the outcomes of these checks:

- Identity is verified against existing 3rd party data sources, for example, a government identity credential database designed to provide verification services. In the case of the PoC, identity was verified in person to reflect common practice in Singapore (the white paper will later discuss the opportunity for digital verification processes).
- Identity data are then checked against various watchlists (e.g. PEP, Sanctions lists) to identify any potentially suspicious actors
- If checks are successful, an identity certificate is created and is associated with the wallet
- As a result of the association between the certificate and the wallet, the Co-Signer has the ability to gauge whether the wallet is safe to transact, as before any transaction, the presence of a certificate can be confirmed. If the certificate cannot be confirmed, the transaction will not be processed
- This implies that a transaction cannot be completed unless a relevant compliance check (e.g. KYC, PEP, sanctions) has been performed as there is no certificate present

This framework is critical to ensuring a level of trust and compliance in the ecosystem. Transactions can only be processed if countersigned ("co-signing") by our ecosystem. Since that signing only happens if KYC, AML, and other checks are successfully performed, all transactions must be legitimate in principle.

It should be noted that at the time of a transaction, AML related checks can be performed and if these check fail, the transaction will not be processed. This type of functionality was not part of the scope of the PoC, but would be part of a fully developed platform to provide a higher level of risk mitigation.

Post-onboarding, ongoing compliance checks can also be performed

As identity is maintained, compliance checks can be conducted on a continual basis, post-onboarding as sanctions, PEP lists or other watch lists can be updated. This would simply use the platforms existing functionality.

4.4 How transactions work within the Trusted Ecosystem PoC

Buy/Sell Bitcoin with an integrated exchange

To enable the buying and selling of Bitcoin with fiat currency, the platform connects and integrates with a Bitcoin exchange through API services developed by the exchange. To facilitate a smooth integration and customer experience between the platform and the exchange:

- A user has an (pre-funded) account with the exchange that is integrated with the wallet
- When the customer logs into the wallet, they defacto are connected or logged into their exchange account

When a user is ready to transact (buy/sell), the following steps occur:

1. The user will enter in the amount either in Bitcoin or fiat currency that he or she wants to buy or sell
2. The platform then validates balances to ensure enough funds exist in the associated exchange account to perform the transaction. If there are insufficient funds, the transaction will fail, prompting the user to try again
3. If an acceptable buy/sell amount is requested, the co-signer proceeds to perform its identity check, that is, it checks whether the wallet has a valid identity certificate present (which is a result of successful compliance checks)
4. The transaction then executes between the customer and the exchange and Bitcoin is sent from the exchange to the user's wallet

To maintain the Trusted Ecosystem the exchange will always be an identified party within a transaction as a result of the nature of the integration and the static nature of the exchange's Bitcoin address. The exchange will never exist as an anonymous party. It should also be noted that exchanges also require their customers to go through their own compliance processes related to customer onboarding, therefore adding a layer of security and compliance.

Send/receive Bitcoin among known parties in the Trusted Ecosystem

Bitcoin transactions within the Trusted Ecosystem will always occur amongst users who have been successfully onboarded, identity provisioned, compliance checks performed and the corresponding certificate provisioned. This sets the foundation for safe and compliant transactions.

To ensure transactions performed by known parties, the following steps occur:

1. The sender will enter in the recipient's wallet name and the platform will validate whether the recipient wallet name is valid and provisioned
2. If provisioned, this implies the recipient has successfully onboarded and has successfully passed identity checks
3. Once the recipient wallet name is verified, the sender can proceed with the transaction. If not, the transaction cannot proceed and the sender will not be able to send (e.g. send button is deactivated)
4. The sender sends a request to the recipient to receive the funds
5. The recipient then receives an approval request to receive funds and if approved acts a final confirmation back to the sender
6. The sender finally approves and confirms the transaction (completing the transaction "handshake") and requests the Co-Signer to process the transaction
7. The Co-Signer then verifies whether certificates are present (as a final check) and proceeds to signing the transaction, therefore completing the send transaction

4.5 How BIP 75 enables trusted interaction between wallets

A BIP, which stands for Bitcoin Improvement Protocol, is part of a series of suggested improvements to the core Bitcoin code and protocol developed by the Bitcoin developer community.

To enable wallet names and the approval and confirmation process amongst wallet to wallet transactions, the BIP 75 protocol was used. This Bitcoin specific protocol is one of the underlying technologies that enables trusted and identified interactions between wallets. It is an extension to BIP 70[2], which provides

[2] BIP70 describes a protocol for communication between a merchant and their customer, enabling both a better customer experience and better security against man-in-the-middle attacks on the payment process.

two enhancements to the existing Payment Protocol:

- It allows the sender of a payment request to voluntarily sign the original request and provide a certificate to allow the payee to determine the identity of the party they are transacting with.

- It encrypts the payment request that is returned, before handing it off to the SSL/TLS layer to prevent man in the middle viewing of the payment request details.

The motivation for defining the BIP 75 Payment Protocol was to allow two parties to exchange payment information in a permissioned and encrypted way, such that wallet address communication can become a more automated process. This improvement also expands the types of PKI (public-key infrastructure) data that is supported, and allows it to be shared by both parties. With BIP 70, only the receiver could provide PKI information, instead of both. Furthermore, BIP 75 allows for automated creation of off-blockchain transaction logs that are human readable and can include information from both the sender and recipient.

The motivation for BIP 75 is threefold:

1. Ensure that the payment details can only be seen by the participants in the transaction, and not by any third party.

2. Enhance the Payment Protocol to allow for store and forward servers in order to allow, for example, mobile wallets to sign and serve Payment Requests.

3. Allow a sender of funds the option of sharing their identity with the receiver (in the case of the PoC, this ability was used). This information could then be used to:

    - Make Bitcoin logs (wallet transaction history) more human readable
    - Give the user the ability to decide whether or not they share their Bitcoin address and other payment details when requested
    - Allow for an open standards based way for businesses to keep verifiable records of their financial transactions, to better meet the needs of accounting practices or other reporting and statutory requirements
    - Automate the active exchange of payment addresses, so static addresses and BIP32 extended public keys can be avoided to maintain privacy and convenience

In short, BIP 75 makes Bitcoin transactions more 'human', while at the same time, improving transaction privacy.

4.6 How funds can be controlled outside the platform

The Trusted Ecosystem ensures that Bitcoin transactions are executed in an identified and compliant manner. If funds can be moved outside the system and further transacted in an anonymous manner, the entire concept fails. The following points summarise how funds can be controlled outside the ecosystem:

- During the onboarding process when the wallet and Bitcoin address is created, multiple keys are provisioned (e.g. the customer key and the Co-Signer key) to sign transactions
- Transactions from this Bitcoin address must require both keys to sign. If only one are present, a transaction from that address will not complete
- If a customer wanted to access their Bitcoin address using a non Trusted Ecosystem wallet, they can register the address with the wallet to view the balance, however they cannot transact with

those funds as they would require both keys

- Customers can still view their own balance in another wallet because the platform still fundamentally sits on Bitcoin addresses. The platform applies a layer of identity and functionality on top of the address as the purpose of the platform is to work with the existing Bitcoin network and helping its transactions meet identity based regulatory requirements
- It should be noted that when Bitcoin addresses and their respective balances are viewed in this fashion, it is done as per the normal way of looking at Bitcoin addresses and balances - you will only see that Bitcoin address (e.g. "1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX") has X balance, but there is no way of knowing who "1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX" is because there is no relation to identity (e.g. first name, last name, etc.).
- Though a customer can see their own balance using another wallet, when it comes to moving funds out of that wallet, the control elements of the platform come into life. Since that wallet or any other non-trusted wallet has no access to the Co-Signer, transactions cannot be performed as it requires the Co-Signer key
- Thus, funds are controlled and must "re-enter" the trusted ecosystem to successfully transact

The co-signer is the key to ensuring control. In the absence of the Co-Signer, a customer could simply access his or her Bitcoin address through another wallet and begin moving funds.

It should be noted, the control of funds coming into the Trusted Ecosystem from outside, unidentified and therefore untrusted sources, were not part of the original scope of this PoC. However, it was discussed conceptually and is addressed later in this white paper. It is also a potential topic for subsequent PoC.

A privacy debate: the open nature of Bitcoin's permissionless ledger

Anonymity (or rather, pseudonymity) is a core feature of Bitcoin and why at its core, users are identified only through Bitcoin addresses which do not translate into how many understand identity today (e.g. first name, last name, home address, etc.). At the same time however, the Bitcoin network also allows any of its users to view its ledger, transactions on the network and balances of each address.

In summary, the Bitcoin network allows all users to see where--that is, to which addresses--funds are flowing and held, but it is incredibly difficult to confirm the identity of who is holding those funds or have transacted since the network itself does not contain that information.

This presents an interesting privacy debate. Taking a traditional banking system view, the ability to openly view customer balances by any party would be an absolute violation of basic privacy principles. Therefore, the transparent nature of Bitcoin (even when de-identified) can be at odds with privacy requirements.

However, Bitcoin is growing and many people recognise that it is thriving today and will continue to thrive in the future. Accepting this begs the question - how do both worlds operate together? For regulators and institutions, this presents a challenging decision. Do they choose to engage the technology and market opportunity or not? Do they attempt to control or not? As cryptocurrencies at odds with regulation (privacy related or not) continue to proliferate, these questions will become increasingly important.

The PoC provided a mechanism for both worlds to operate together and strike the balance

between privacy and the nature of these networks. If institutions accept such a balanced approach should be taken, further innovation will hopefully begin to resolve some of these tensions.

5. Testing of the Trusted Ecosystem hypothesis

Key Messages:

- The PoC proved that Bitcoin transactions could begin to meet identity related regulatory compliance requirements
- Identity was successfully applied to wallets and their respective Bitcoin transactions
- Transactions could be controlled based on the result of successful compliance checks
- The PoC also provided interesting insights to the challenges of the Bitcoin network, the inefficiencies of digital identity and the need for further innovation

5.1 Testing of the hypothesis

The PoC aimed to demonstrate trust, compliance and security amongst Bitcoin transactions and produced the following outcomes:

1. **Identity verified through the onboarding process**

    - Users' personal identity information (e.g. name, address, date of birth) as well as government issued credentials (e.g. driver's license or passport) had their identities verified through an in person identification check in Singapore (e.g. open bank account).
    - The identity was also checked against multiple watch lists (e.g. sanctions and PEP lists provided by a 3rd party provider)
    - Users who had their identities successfully verified and did not have any warnings raised against watch lists, were successfully onboarded
    - Users who could not verify their identify or raised warnings against a watch list, were not onboarded
    - When successfully onboarded, a digital certificate representing verified identity was created

2. **Identity successfully associated with wallet and Bitcoin address**

    - The digital identity certificate, which correlates to the onboarded identity, was successfully linked to the wallet and therefore the Bitcoin address
    - The digital identity certificate was also associated with the descriptive wallet name, which was provisioned during the onboarding process and also associated with the wallet
    - Using the descriptive wallet name, users could successfully look up other wallet names (which as per above, were associated with a wallet, Bitcoin address and digital identity certificate) and establish a recipient for a transaction.[3] Users could not view other users' balances

[3] In the PoC, a user can only search for a full and complete wallet-name. This means users could not browse or search for other users. They had to enter in the entire, correct name and when correct, the system would recognise a match. Wallet-naming functionality reflects the customer need to use human-readable addresses instead of Bitcoin's 34 character alphanumeric address. It also reflects the rise of social messaging based payment platforms where customers want easy ways to send money to their contacts. It is certainly easier for customers to type in a contact in the same way they do in a messenger app versus typing in account information in a payment channel.

3. **Signed transactions based on the presence of an identity certificate**

    - The co-signer successfully identified whether an identity certificate existed for a wallet that initiated a transaction
    - The Co-Signer confirmed the presence of an identity certificate, therefore confirming compliance checks had been passed and signed (executed) the transaction
    - The Co-Signer successfully completed this process for both buy/sell transactions with an exchange and send/receive transactions between wallets

4. **Inability to transact without the presence of an identity certificate**

    - Users could not initiate a transaction without being successfully onboarded and a digital certificate issued. As part of the design, the wallet's transaction functionality was locked until onboarding was successfully completed and therefore could not transact without the presence of an identity certificate
    - Additionally, during development and testing, when the certificate service was temporarily deactivated, the Co-Signer could not sign transactions as there was no presence of a certificate

5. **Inability to transact funds outside the trusted ecosystem**

    - During testing, we attempted to load a Bitcoin address that was provisioned in the Trusted Ecosystem on a wallet outside the Trusted Ecosystem
    - The wallet could load the Bitcoin address and see the balance (as any wallet should), however, funds could not be moved
    - This is a result of how the Trusted Ecosystem provisions new Bitcoin addresses and multiple private keys. Bitcoin addresses provisioned within the Trusted Ecosystem require both a user key and Co-Signer key to transact
    - Since the non-Trusted Ecosystem wallet has no access to the Co-Signer, funds could not move and therefore funds cannot be transacted outside the ecosystem

5.2 Additional insights from the PoC

In addition to proving the hypothesis and specifically testing the ability to execute regulatory compliant Bitcoin transactions, the PoC raised several interesting insights. These insights were both directly and indirectly related to the goal of the project, but should be broadly seen as contributions to broader challenges of making Bitcoin fit for broader public use, including in financial services.

1. **The scalability of the Bitcoin network clearly presents challenges to the customer experience**

    During the testing of the hypothesis, we sometimes experienced long confirmation times (sometimes hours) as well as relatively high transaction fees (more noticeable for low value transactions). The waiting times--at one point, up to 14 hrs.--and costs were certainly not ideal for a technology that is intended to present faster as well as lower cost transactions for customers (though it should be noted that total confirmation and settlement times were still faster than contemporary correspondent based banking transactions).

    To understand these wait times and fees, we must have a deeper understanding of how Bitcoin functions. When a Bitcoin transaction is executed, it undergoes a validation process which runs through the different computers running the Bitcoin protocol around the world. Once a

transaction is verified, it waits to be added to the blockchain, specifically, the next block within the blockchain. Bitcoin miners play the role of receiving these verified transactions and adding them to a block. Until they are added, these transactions will exist as "unconfirmed" transactions.

Bitcoin's capacity limit comes from the way transactions are recorded in each block. Every 10 minutes a new block is added to the blockchain and because each block has a maximum size of one megabyte, this translates to throughput of about seven transactions a second. This certainly presents a challenge to the overall growth of Bitcoin as each block can only hold a finite amount of transactions. As a result, not all transactions are added instantly. Users need to wait for a certain amount of time until a miner decides to pick a transaction and add it into the new block.

To create incentive to add the transaction to a block quickly, users can add a large enough mining fee to it. Miners naturally prioritise transactions with higher fees, therefore the higher the fee, the faster the transaction will process and confirm. This in turn means any transaction that is sufficiently low may wait an indeterminable amount of time before being settled by inclusion in a block.

Bitcoin scalability is, of course, a known issue and has been the subject of intense debate within the Bitcoin community for years. Numerous solutions have been proposed from increasing block size to creating "off-chain" functionality to reduce pressure on the Bitcoin network. Whatever solution is adopted (which could warrant another white paper) will hopefully support positive customer experiences.

2. **The Trusted Bitcoin Ecosystem is not immune to the inefficiencies and lack of innovation in identity and compliance management. This compounds in situations where identity credentials may not be widespread.**

Despite the innovative nature of Bitcoin and the proof-of-concept's ability to apply identity to transactions, the contemporary challenges relating to identity verification still remain. For the PoC, identity was fundamentally verified by creating an interface to a 3rd party identity provider and calling this open data source to check PEP, Sanctions etc. In person identity checks are still common practice within Singapore. End-to-end, digital identity verification processes are not widespread (online verification of key personal digital identity documents) and this in itself presents a costly experience. One of the principal benefits of Bitcoin and cryptocurrencies is the digital nature of the currency and user experience. All core aspects of the technology are digital, making it a relatively low cost technology. Integrating physical identity verification begins eroding the cost benefits of the technology.

Despite this, the core platform was designed to perform purely electronic checks, where personal identity information can be verified against digital verification services (e.g. government identity databases and associated services). Therefore, jurisdictions outside Singapore can realise the benefits of end-to-end, digital identity verification processes and in fact are common practice for many financial services institutions around the world[4].

Building on the challenges of identity verification, the PoC also raised an interesting question - how would identity management work in situations where government issued credentials were

[4] It should be noted there are examples of digital onboarding in Singapore - (a) DBS Bank adopting digital account opening for corporate banks - https://www.dbs.com/newsroom/DBS_launches_fully_automated_online_account_opening_service_for_companies_first_bank_in_Asia_to_do_so_MIGRT (b) OCBC for individuals (Singapore citizens and permanent residents only) - http://asianbankingandfinance.net/banking-technology/news/ocbc-bank-first-in-singapore-enable-account-opening-go

not widespread or mature enough to use as verification mechanisms? A mature system of government issued credentials and the presence of established identity verification services make identity and compliance management far simpler to develop. However, this may not always be the case.

This is a commonly articulated challenge within the "unbanked" population where new and innovative ways to provision identity are required. For Bitcoin, this is an interesting opportunity as its ability to support the "unbanked" has been a common use case. Further innovation in this space is absolutely critical to addressing the "unbanked" challenge.

3. **Managing funds sent from unknown or suspicious sources to users within the Trusted Ecosystem still needs to addressed**

The scope of the PoC addressed funds moving within the Trusted Ecosystem amongst identified actors, however it did not address the potential for funds coming in from actors outside the ecosystem (simply because this this scenario was out of scope for this PoC and is a topic that deserves a PoC of its own).

The sending of funds could be controlled within the Trusted Ecosystem as a result of how wallets/addresses were provisioned and the resulting need for the Co-Signer to sign transactions if an identity certificate was present.

Since wallets provisioned within the Trusted Ecosystem still fundamentally have Bitcoin addresses behind them, they still have the ability to receive funds from any other Bitcoin address. This presents an opportunity for potential bad actors to send funds to Trusted Ecosystem wallets.

Whilst developing solutions to combat against was not in the scope of the PoC, potential solutions were discussed. These ranged from developing quarantining functionality to intercept and hold funds from 'bad actor' addresses to hiding the actual addresses so users could not see Bitcoin addresses associated with their respective wallet and therefore 'bad actors' would have an almost impossible way of knowing which addresses to send funds to.

In context of further developing the PoC, this would be one of the remaining areas to create a fully controlled ecosystem.

6. Security review and learnings

Key Messages:

- As part of the PoC, the platform and its components were reviewed to help identify key security learnings that could set the stage for Bitcoin related (or similar cryptocurrency based transactions) standards. The intent of the review was not to provide prescriptive security solutions, but help provide a path to continuous development and innovation
- Effective key management, securing digital identity, using the BIP75 protocol and securing the transmission and storage of any data were some of the key topics identified in the review

6.1 Security review approach

An important part of the PoC was the opportunity to conduct security related reviews and tests against the platform's functionality. This included testing and reviewing the mobile application and its underlying backend infrastructure. The review was conducted by PwC's Cyber Security team, which was a separate team to the one that developed the platform and delivered the the overall PoC.

The purpose of this review was to provide input into the further development of the platform (and other platforms like it). As this PoC was testing early stage technology for demonstrative purposes rather than mature, production ready technology, we expected to find security gaps that would need resolving as development continued, and which could become focus areas for other developers working on similar platforms. It is important to recognise that these findings are provided as a critical step to ensuring secure innovation for a broad range of stakeholders, from FinTech startups to incumbent financial institutions. Ultimately, these security findings can set the stage for productive innovation and help elicit trust in technology that enable a compliant Bitcoin market.

To complete the security review, two major activities were performed. This included:

1. **An objective based security penetration testing of the platform** was performed to identify possible vulnerabilities. The key risk factors addressed were related to disclosure of sensitive information and unauthorised access to platform services.

   The testing covered:

   - Mobile application data input validation checks and endpoint API connection back to the platform services.
   - Infrastructure vulnerability assessments of supporting infrastructure to identify security vulnerabilities and configuration weaknesses in both internal and external accessible virtual infrastructure.

2. **High-level solution reviews across the platform** to determine if the demonstration environment had applied industry security technical controls to protect the ecosystem components and data.

   The high-level solution assessment was based on ISO/IEC 27002:2013 Information Technology - Security Techniques - Code of practice for information security control. This was used as a guideline to discover security gaps and formulate valuable security insights.

This assessment included:

- Reviewing high level architectural documentation
- Conducting high-level security interview workshops with the platform's key technology FinTech partners

The result of both the objective based security penetration tests as well as the high-level solution review produced security findings and learnings to share across a range of topics. These topics were synthesised into key categories outlined below:

1. General platform security
2. Digital identity certificate issuance and general management
3. Multi Signature Key Management (Practice/Schema)
4. BIP75 related identity and transaction security
5. Bitcoin Exchange integration

6.2 Key security learnings

1. **General platform security**

   In general, information security management practices, industry regulations and compliance standards should be identified as security requirements. Those requirements should be embedded at the beginning of any solution delivery framework and extended to operations, thus providing assurance that the platform's underlying components are compliant and secure by design.

   Network and Access Security

   Security infrastructure penetration tests highlighted the need for continued focus on the platform's database identity authentication and authorisation protection. An insecure database can provide a threat actor the opportunity to exfiltrate, change and delete sensitive information with minimal effort. Securing the platform's database and its sensitive information is clearly an important requirement and is naturally a next step to getting the platform production ready.

   Therefore, it is recommended that identity access management controls and defence are implemented as a critical part of all similar platforms. This will provide key elements for an indepth network security architecture, whereby user access controls are applied and critical assets such as servers and databases are securely segregated away from the public. Network filtering, detection and prevention control will need to be applied to all similar platforms ensuring network segregation and defence. This, in addition to identity and access management controls to proactively permit secure access to the platform's critical services.

Data Protection Security

The mobile penetration tests and solution review assessment highlighted two issues that the developer community should be aware of related to the protection of data. Sensitive data which is stored within the mobile device and database must be encrypted at rest and the connection between the mobile device and a third party proxy transferred private keys over a https protocol. Again, addressing these issues will be a critical step to all similar platform's path to production level security.

The secure storage and transmission of personal identity data will be an absolute minimum operating requirement

Thus, for related crypto platforms, it is a security recommendation that all sensitive and personal information is to be encrypted at rest and in transit. This will provide data confidentiality and integrity protection from mobile devices to data repositories.

The platform will need to apply encryption capabilities at the database instance and volume disk levels.

Additionally, related platforms will need to ensure that all sensitive information that is generated and stored on the mobile device is encrypted at rest, within the device's secure element. Developers also need to ensure that all sensitive transfer of information such as private keys and personal identifiable information are encrypted end-to-end during transmission. This can be achieved through the use of strong cryptographic cipher suites supported by well defined key management processes and procedures.

To secure data, the PoC applied an Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256-bits to ensure integrity and nonrepudiation. As a general learning, encryption strength should be tested during the PoC phases for all similar crypto platform endeavours. Additionally, it is highly recommended as part of any cryptographic management process, to regularly test whether key size and algorithms are inline with international standards and industry information security regulations.

Endpoint Security

Finally, developers should be aware that the endpoint compute hosts that are commissioned to support the platform must apply secure images that contained endpoint security controls protection.

As always, all similar platforms will need to ensure that the servers adhere to platform OS and Application patch management, apply secure best practices for platform configuration and regularly scan for vulnerabilities before deployment and during the platform lifecycle.

Securing endpoints was recognised as an activity that would be part of the continued development of the platform, post the PoC.

Log and monitoring

Application and endpoint compute hosts must also generate security logs to support monitoring and alerting capabilities. Similar platforms will need to ensure that all events of interest logs are to be generated and sent to a secure centralised repository for security operation monitoring and incident response. For the PoC, basic log and monitoring functions were developed.

2. Digital identity certificate issuance and key management

Multi-factor authentication is a basic operational necessity for identity verification and continually pursuing the most effective methods of multi-factor authentication is the key to maximising long term security

Though as part of the onboarding and KYC process, personal identify information (PII - e.g. personal names, home address, etc.) and identity credential information (e.g. driver's license numbers) can be verified on the platform, there is still a need to mitigate against bad actors stealing PII (identify theft) and using that information to legitimately onboard.

Identity theft will remain a common threat against a user, whereby an attacker could steal someone's passport, driver license and/or national Identification number and simply submit that data for verification checks.

Today, this problem can be prevented with in person identification checks. Though a proven method, in person identification is a relatively costly method and finding alternatives to in-person verification is no easy challenge. Across many geographies and jurisdictions, finding alternatives remain an industry challenge, though at the same time, several jurisdictions do accept electronic identity verification (e.g. Australia).

The platform demonstrated a purely digital onboarding and identity verification process. As stated previously, identity 'spoofing' where a bad actor can onboard with a stolen identity can still occur on the platform (and many others like it), and therefore presents an opportunity to improve and mitigate.

To mitigate, the review process recommends additional countermeasures and controls to further strengthen the platform's identity onboarding process. These additional countermeasure controls are outlined below:

- **Combining and integrating with a bank's or other existing identify services such as Social digital identities** (Google, Facebook and Twitter) will further strengthen the identification verification process. This can provide additional layers of verification.

- **Enabling a multi-factor authentication mechanism such as biometric verification** to evaluate unique human attributes such as fingerprints, retina and iris patterns. This will also further strengthen the identity verification process.

- **Implementing one-time passcodes to be sent securely to an endorsed email address or mobile number** during a predetermined enrolment session time. This is another simple, but powerful mechanism.

The additional countermeasures should not be interpreted as a definitive list of security controls to completely replace in-person identification checks, as each of the above will have its own limitations. However, potentially combining them can provide a stronger, overall identity verification mechanism for the platform.

Continual identity verification checks during the lifespan of a customer wallet will help further secure the ecosystem

Identity verification should not be a one time event. For example, customers can lose, forget or have their login credentials stolen or in an even worse case, customers can become 'bad actors' (and be placed on a sanctions or similar list). When events like this occur, identity should be reverified.

Therefore, to protect the customer and the platform against unauthorised access or 'bad acting', it is recommended that the platform's future design includes new functions and processes whereby continuous identity verification can occur during the lifespan of the customer wallet. The PoC demonstrated identity verification and the time of onboarding, but was also designed to perform checks outside of this, such as at the time of transaction. This functionality is intended to integrate with a financial institution's existing risk measures and would be developed as part of the platform's ongoing development.

Additionally, once the end-user has been initially verified via the platform, it is recommended that each end user is assigned a "user profile" whereby their behaviour can be assessed to detect and block potential unauthorised and fraudulent transactions.

The "user profile" should take advantage of data analytics collected from a wide range of sources including internal/external identity sources, mobile device and applications logs as well as existing financial fraud detection and business decision engines. The aim should be to formulate a near real-time active behavioural profile that is used to support and protect the transaction integrity within the platform.

The platform could also initiate a real time second factor identification challenge to the client when the following actions have been executed. Some example actions that trigger an identity verification are listed below:

- Maximum transaction threshold stop limit
- Abnormal time and frequency of transactions
- Modification to client recipient address list
- Modification towards client user profile and application security settings
- Request for user credential change such as password resets

Lastly, the platform could incorporate a second factor failure threshold limit whereby it will automatically disable the client's account and send associated alerts back the the client and platform administrators, indicating potential threats.

The above security recommendations will not completely mitigate the threat of stolen user credentials, however incorporating continuous identification second factor challengers can limit the ability to make unauthorised transactions.

2. Multi signature key management (practice/schema)

Multi-signature (multi-sig) key systems are a minimum operating requirement to protect customers and transactions

Standard transactions on the Bitcoin network are "single-signature", using the private key associated with the Bitcoin address. This simplistic method of approval and authenticating transactions lead to the development of multi-signature (multi-sig) transaction schema to further improve integrity and security.

A multi-sig scheme requires more than one authorised signature to process and approve a transaction. Without a multi-sig scheme, if a customer's phone or wallet and subsequently their private key was compromised, their funds could be accessed and moved. With a multi-sig environment, even if the phone/wallet was compromised, it would still need a second private key to sign transactions.

The platform applied a multi-sig schema whereby the customer's and platform's private keys are processed and approved for each Bitcoin transactions. This provides added transaction integrity and authenticity and is highly recommended to be a foundational operating requirement for any Bitcoin related platform.

How private keys are stored and managed is paramount to ensuring a secure ecosystem

The main learning point and recommendation from the solution review was to develop and implement a key management system to safeguard the cryptographic keys that are generated and stored across the ecosystem. It should be noted that the PoC did not incorporate production level key management and key storage. It is a critical piece of functionality that intended to be developed post the PoC.

The key management system needs to address protection within key generation, wallet creation, storage, usage, key compromise protocols, grant/revoke actions, security testing procedures and audit procedures. This, coupled with privileged user access procedures, will provide trusted key access assurance and protection against unauthorised access.

For a multi-sig schema, such as a 2-of-3 multi-sig arrangement, the platform should have three key storage locations:

Client mobile device - First key

It is recommended that all client sensitive information such as private keys should integrate and leverage existing mobile technology such as "Secure Elements" to store and protect data in a confidential manner.

Platform Environment - Second key

It is recommended to implement scalable FIPS 140-2[5] level 3 or 4 compliant Hardware Secure Modules to protect 'hotkeys' for inline encryption and decryption processes required for transaction execution.

Cold Storage - Third key

In a 2-of-3 example, the third key often acts or functions as a 'rescue key' for a wallet. These keys are not intended to be used unless a customer loses their account and therefore, are often maintained in 'cold storage'. If the client had lost their private key or the platform environment keys are compromised, the third key can be retrieved from the cold storage to support the 2 of 3 multi-sig restoration process.

For this key, it is recommended to implement a network air-gapped key storage solution that is not accessible externally and is isolated within a separate internal network.

It is critical that the physical placement of the cold storage keys is only known and accessed by trusted stakeholders and custodians of the platform. The process and procedure for recovery keys should include multiple trusted custodians that simultaneously access and retrieve keys to prevent single user threats.

Here are some practical examples of air-gapped cold storage key solution that can be considered:

- FIPS compliant Hardware Secure Module
- Server that is able to only read fixed memory cards

It should be noted, the above considerations are based on technologies that exist today. These are just examples of possible solution and should not be seen as a complete and definitive list.

Key management is a critical topic for this platform and any platform like it. Striking the correct balance of protection and accessibility will always be a major challenge and will require in-depth investigation. Continual innovation in cryptography storage and custom key management processes are absolutely essential for the protection of the platform, users and their funds.

Using a multi-sign system as a "smart" control mechanism

Multi-sig systems have the ability to provide far more than a mechanism to safeguard transactions for lost wallets. They can become the primary control mechanism to ensure safety and combat against "bad" or unlawful behaviour.

The PoC demonstrated that transactions could only be signed when certain identity certificate criteria was met. Once that criteria was met, the platform would sign a transaction with the required second key. The programmable rules behind signing transactions can be made far

[5] The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules.

more complex if required.

For example, a "smart" signer could take advantage of anti-fraud related data analytics or any other real time analytic checks and control/freeze transactions where necessary. These checks could also include identity fraud related checks (e.g. trying to execute transactions from two geographic locations at the same time, etc). This is where contemporary risk analytics and processes can be integrated into Bitcoin transactions.

In real life application of the platform and technology, the real time fraud and analytics checks should be part of the bank's or financial institution's existing capabilities and anti-fraud measures.

It should be noted that no real time, anti-fraud checks were tested during the PoC.

3. BIP75 related identity and transaction security

As described in Section 4 of this whitepaper, a Bitcoin Improvement Proposal or BIP (specifically BIP75) is a design document for introducing features or information to Bitcoin. This is the standard way of communicating ideas and enhancements since Bitcoin has no formal, centralised administrative structure.

BIP75 should be used for identity provisioned Bitcoin transactions

As outlined previously, BIP 75[6] is an extension to BIP70[7] that provides new security enhancements to existing payment Protocol Messages of "InvoiceRequest" and "PaymentRequest" whereby it allows the sender's the ability to sign and provide identity certificate to the payee for identification assurance prior to receiving funds.

Bip75 also enables support for encrypted messages using Advanced Encryption Standards (AES) 256-bit whereby the previous protocol message only applied message integrity over Secure Hash Algorithms (SHA) 256-bit.

This protocol enables the provision and use of identity on the platform as well as the secure communication between identities during transactions. This is why it should be used for identity provisioned Bitcoin transactions.

The BIP75 protocol provides an option to encrypt key payment related messages and this option should be used

BIP75 has introduced two variants of message protocols that underpin its core payment related, wallet-to-wallet communication:

1. **ProtocolMessage** - The ProtocolMessage message is an encapsulating wrapper for any

[6] https://github.com/bitcoin/bips/blob/master/bip-0075.mediawiki
[7] https://github.com/bitcoin/bips/blob/master/bip-0070.mediawiki

Payment Protocol message. It allows two-way, non-encrypted communication of Payment Protocol messages. The message also includes a status code and a status message that is used for error communication such that the protocol does not rely on transport-layer error handling.

2. **EncryptedProtocolMessage** - The EncryptedProtocolMessage message is an encapsulating wrapper for any Payment Protocol message. It allows two-way, authenticated and encrypted communication of Payment Protocol messages in order to keep their contents secret. The message also includes a status code and status message that is used for error communication such that the protocol does not rely on transport-layer error handling.

These message protocols specifically support the key payment messages functions, "InvoiceRequest" and "PaymentRequest", which are essential for the payment process.

"ProtocolMessage" and "EncryptedProtocolMessage" both offer SHA 256-bit encryption for integrity with status code and message support. However it is the additional enhancements provided by "EncryptedProtocolMessage" that incorporate message encryption with AES 256 algorithm in addition to SHA 256-bit for message integrity.

Thus, in order to ensure end-to-end communication between sender and receiver is secured, all messages should utilise "EncryptedProtocolMessage" functionality to protect both "InvoiceRequest" and "PaymentRequest" messages.

4. Bitcoin exchange integration

As part of the PoC, legal and reputational due diligence was performed to identify suitable Bitcoin exchanges to integrate with the platform. As a general security learning and as part of this due diligence, it is essential to perform a security assessment to understand the exchange's (or any other third parties) security posture and potential threats.

As part of the high level solution review, the API integration between the platform and exchange was reviewed and the resulting security learnings are outlined below:

Strive for federated identity with single sign-on

In order to provide identity coverage and assurance, it is fundamental to propagate identities, user behaviour profiles and permissions to all third parties such as Exchanges.

Within this inheritance framework it provides the platform the ability to centralise control within the decision engines that is governed by business rules, regulations, sanction and user's threshold stop limits that is transparent to the end user experience.

For the PoC, single sign-on functionality was not in scope and therefore was not tested.

Ensure secure RESTful Application programme interfaces (API) whereby authorisation over a protected connection is enforced

A critical learning is that all network connections between the platform and third party exchanges should traverse through a secure API gateway whereby mutual authentication provides identification, integrity and confidentiality between environments.

As an example, OAuth 2.0 is an industry standard protocol for authorisation used within a secure RESTful API. The OAuth 2.0 framework utilises tokenisation (Bearer token) to support authenticated access between the client and server. The following guidelines are to be taken into consideration. The tokens need to:

1. Be unique
2. Be non-sequential
3. Be non-guessable
4. Apply expiry time
5. Enforce refresh time

Lastly, all communication between client and services must be encrypted over HTTPs as OAuth 2.0 will send the access token back to the client in clear text if not enforced via a URI redirect.

The PoC did in fact utilise an OAuth 2.0 token.

Enforce permission based transactional services for buy and sell

The PoC had integrated with a third party Bitcoin exchange service provider to assist with transactional functions for buy and sell.

The solution review identified that the platform's client or transaction based permission rules did not necessarily integrate with the exchange's permission engines and rules (as this was out of scope for the PoC). Two different parties could have two different sets of rules and though they may not conflict with each other, this environment makes end-to-end assurance challenging.

Therefore, as a security recommendation, it is important to align the platform's permissions or rules to that of the exchange's (or third party's) and allow end-to-end enforcement across all allowable functions. As an example, when the platform applies business rules for transactions (as the platform did with its Co-Signer module), these rules must be maintained within the Bitcoin exchange.

Our learnings had shown us that service calls for buy and sell transactions could enforce the following:

1. User credentials inspection, this could be in the form of an active access token
2. Validation and enforcement of user base permissions
3. Request for multi-factor authentication based on user behavioural profile enforced by decision engines

7. Setting the stage for best practices

Key Messages:

- There are no mature Bitcoin specific regulations, however the industry has begun developing voluntary best practice standards
- The minimum posture for any organisation should be to satisfy basic regulatory requirements like KYC or AML and that often starts with establishing identity
- Security related best practices need to revolve around protecting data assets such as cryptographic keys, identity and transactional data, using secure data transmission and communication protocols and strengthening application access management

Note: the scope of this white paper did not include reviewing all Bitcoin or cryptocurrency related standards and selecting a best standard. This white paper simply highlights their existence and synthesises key learnings from those standards.

7.1 Existing standards, views and regulations

Regulation specific to Bitcoin, cryptocurrencies and digital currencies is still in its infancy. There is no doubt that it is challenging for regulators to develop regulation in areas experiencing such rapid innovation, in a way that challenges many existing financial services models. However, regulatory posturing has occurred to address the rapid pace of change and interestingly, these postures vary regionally.

The US takes an open, collaborative approach, regulating according to existing law and creating a space for innovation. The US' posture toward digital currencies and companies has been largely positive. By and large, regulators have aimed to treat both within existing legal structures, requiring digital currency companies to register as ordinary money services businesses. The State of New York requires an additional virtual currency license ('bit-licence'), though these are usually regarded as legally unnecessary. U.S. Securities and Exchange Commission (SEC), recently permitted the first publicly traded Bitcoin-based security--the BIT trading on NYSE--as well approved To's S-3 for securities issuance via Bitcoin's blockchain. FED Faster Payments Task Force is actively investigating how Bitcoin-like model replace the legacy payments infrastructure.

Most regimes have followed suit. Thus similarly, the UK encourages early and established companies to develop new products and services, even if the market is slow to regulate. The UK government explicitly recognises digital currencies' positive potential in financial services, but has been slow to issue regulatory guidance. In 2015 HM Treasury set aside £10m to establish a multi-institutional committee to advise the government on best practices for digital currency companies and approach to regulation. By contrast, UK FI's have been quicker to engage: the Bank of England is considering a central bank backed cryptocurrency and various banks have actively run PoCs with Bitcoin and blockchain companies.

By contrast, China permits private and commercial use of Bitcoin, but has banned it from financial services altogether. This stems from concerns over price volatility, the resulting impact on financial stability, and reports that citizens have invested in bitcoin to avoid capital controls. Officially bitcoin is deemed a virtual commodity by China, not a currency. The People's Bank of China has stated that it will continue to monitor activity and exchanges have introduced a 0.2% trading fee per transaction in an attempt to cool activity, amid a bitcoin price surge in 2016 that was driven by high volumes in the

mainland.

Whilst regulatory views progress, industry standards are beginning to form. There are several initiatives around the world to develop voluntary standards. The Cryptocurrency Security Standard (CCSS) is an example and was developed by The CryptoCurrency Certification Consortium, an industry consortium whereby its mission is to establish cryptocurrency standards that help ensure a balance of openness & privacy, security & usability, and trust & decentralisation.

The CCSS is a security standard that helps secure all information systems that make use of cryptocurrencies. Its goal is to help standardise security techniques and methodologies used by cryptocurrency systems around the globe and as a result, end-users will ideally be able to make educated decisions about which products and services to use and with which companies they wish to align with.

The CCSS covers two domains split out into several sub-focuses and is outlined below:

Cryptographic Asset Management

- Key / seed generation
- Wallet creation
- Key storage
- Key usage
- Key compromise protocol
- Keyholder grant/revoke policies & procedures

Operations

- Security audits / pentests
- Data sanitisation policy
- Proof of reserve
- Audit logs

The CCSS applies to any information system that makes use of cryptocurrencies. The standards use a 3 level scoring system to identify the depth of capability in each focus area. The highest level (level 3) indicates an information system has proven by way of audit that they exceed enhanced levels of security with formalised policies and procedures that are enforced at every step within their business processes. Additionally, multiple actors are required for all critical actions, advanced authentication mechanisms ensure authenticity of all data, and assets are distributed geographically and organisationally in such a way that they are resilient against compromise of any person or organisation.

The Australian Digital Currency Commerce Association (ADCCA) is another example of standards being developed by industry. In 2016, ADCCA produced a voluntary code establishing externally auditable best-practice standards of conduct for businesses operating in the Australian digital currency industry. The code of conduct covers:

- Reputation
- Consumer protection
- AML/CTF and sanctions compliance

It obligates those who choose to follow the code to follow key financial services regulatory requirements as well as risk management practices.

7.2 Satisfy existing regulatory requirements

Whilst recognising there are few explicit Bitcoin-related legislation and regulation, ensuring existing financial services regulatory regimes is not only good practice, but a necessity.

Due to the nature of the use case and transactions for the PoC, we focused on satisfying existing compliance requirements related to KYC, AML, Counter-Terrorist Financing (CTF), Sanctions and PEP.

It should be noted that for a similar PoC conducted by PwC in another jurisdiction, specific reporting set by the respective regulator, was satisfied in addition to the requirements previously outlined. Engagement with the regulator was critical to understanding specific regulatory requirements.

As a best practice and overarching approach, understanding all relevant and associated compliance requirements should be a mandatory activity. Fortunately, for these types of proof-of-concepts, there was an open dialogue with the regulator aiding the progression of the project. Working with regulators to understand compliance requirements is an important learning process as well as a necessity. Though this may not be a simple exercise, it is certainly a best practice and factor of success.

Whilst the PoC proved the ability to satisfy existing compliance requirements, it also raised interesting thoughts around how those existing compliance regimes could adapt and integrate with Bitcoin and other cryptocurrencies. For example, though the platform works with only identified Bitcoin addresses, anonymous addresses still exist in the broader Bitcoin network and some of these addresses can be associated with "bad actors". To combat against suspicious behaviour, identifying these addresses and understanding whether these addresses are transacting becomes important. There is opportunity to develop practical solutions like "bad actor" Bitcoin address lists (there are several FinTech startups already doing this[8]) and integrate them into regulatory regimes. Practical innovation like this helps marry the rapid pace of innovation with contemporary regulation.

7.3 Establishing identity with Bitcoin transactions

Establishing identity with Bitcoin transactions is the key to pushing it into mainstream banking and finance. This white paper acknowledges that whilst the core structure of the Bitcoin protocol did not include identity and there is a debate on whether it ever should, there is no debate that in its current form, where identity is not provisioned, it cannot satisfy existing regulation.

This white paper also acknowledges that in practice, Bitcoin can exist in a world of both identified and unidentified users, but only the market and its actors will determine the mix.

When identity is applied to Bitcoin transactions, it should be done in a way to satisfy existing regulatory regimes. Basic personal identity information should be applied such as first name, middle name, last name, date of birth, address, government/recognised credential (if possible) or whatever combination is required to satisfy compliance requirements. Additionally, the use of the BIP 75 protocol as described previously in this whitepaper is certainly an effective practice in utilising identity within Bitcoin transactions and should be considered a best practice.

Provisioning identity also comes with the responsibility of storing and managing identity information. The best practice and technology used for provisioning and storing identity should respect identity and privacy laws within relevant jurisdictions. Data security and sovereignty are critically important when it comes to identity data. Protecting the individual is as important as protecting the financial asset.

[8] To this end, a range of services has arisen to mitigate these risks and aid law enforcement and compliance offices. For example, sophisticated transaction analytics services such as Chainalysis, Elliptic, Block Seer, and Skry that use machine learning algorithms to identify, score, and collate suspicious bitcoin addresses throughout the network. Such services enable compliance officers and law enforcement to see interaction between suspicious addresses belonging to illicit services. These services have proven useful--particularly to law enforcement and bitcoin exchanges--to tracking funds along black markets, however not typically because they reveal the identities of address operators. Rather, association with those addresses requires additional circumstantial information, which then enables such services to view cash flows, relationships, and networks that can be leveraged.

7.4 Establishing basic security posturing

The proof-of-concept's security review not only raised specific security learnings specific to the platform, but also broader, more universal insights that can be applied to any Bitcoin related business. There are three broad categories that can be synthesised from the review:

- Protecting data assets
- Using secure data transmission and communication protocols
- Strengthening application access management.

In any online financial services related business, there is as range of data assets that need protection. The PoC certainly proved this fact. Any Bitcoin related business will need to protect a wide range of data assets and the highest priority assets should be cryptographic keys, identity data and transactional data.

Cryptographic keys - secure key management is one of the most important elements of any Bitcoin related business. The entire lifecycle of keys from creation to use to storage must be secure. Every element that uses or holds keys must be secure. This includes mobile phones where wallets lie, any intermediary that provides additional signatures in a multi-sig environment and any type of key rescue service. Compromising keys would be a catastrophic failure for customers and their funds. If 'bad actors' compromise keys, they can move funds.

As mentioned previously, exploring today's technologies like scalable FIPS 140-2 level 3/4 compliant Hardware Secure Modules or any solution that provides an isolated, highly secure, air gapped dedicated storage of keys, coupled with privileged user access process and procedure will provide key assurance and protection. Furthermore, continually exploring the technologies of "tomorrow" should never be marginalised as they will ultimately benefit all.

Using secure data transmission and communication protocols - almost every critical process like identity creation, identity verification processes, wallet-to-wallet payments, exchange related buy/sell transactions and transactional reporting all are facilitated by the transmission of data. Protecting this data transmission through the use of secure data transmission and communication protocols is critical to protecting the entire ecosystem.

At minimum, AES 256 algorithm or Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256-bits should be used to encrypt the transmission of data.

Strengthening application access management - whether it's a mobile wallet or a browser based reporting portal or an identity database, access management is a basic, but critical area to enforce strict security measures.

The following are basic practices for securing application access management:

- Enable security logging and monitoring across the application, and infrastructure stack must be sent to a secure centralised repository for Security Operations.
- Define privileged role based access control measures to protect against unauthorised access.
- Enable 2 Factor authentication for any application login

8. Conclusion & suggested next steps

8.1 Concluding thoughts

The purpose of this PoC was to show that Bitcoin (and cryptocurrency) transactions could satisfy existing regulatory requirements despite the protocol's anonymous nature of users. The PoC demonstrated that identity could be provisioned onto a Bitcoin address and wallet, therefore enabling basic compliance checks. As a result of those checks, transactions could then be controlled. This PoC demonstrated that Bitcoin and similar cryptocurrencies could begin to function within today's regulated financial markets.

To reach Bitcoin's journey of achieving mainstream adoption, usage and compliance with regulations, security must be a key focus for innovation. Both technological as well as operational security will be key to protecting assets, transactions and now, identity. The PoC demonstrated that additional layers of technology could be built on top of the core Bitcoin protocol, which not only added to the overall capability of the core technology, but also introduced technological complexity.

Addressing this complexity is where the key security learnings arose. From secure cryptographic key management, to data encryption and secure identity data storage, there are important lessons

Further exploration and innovation are absolutely critical to helping Bitcoin and other cryptocurrencies achieve mainstream usage.

The opportunity for Bitcoin and other cryptocurrencies to further innovate and transform financial services is immense. Their ability to provide both alternatives to existing financial products as well innovative solutions behind existing financial product, reinforces the need for further innovation.

These future opportunities range from:

- Alternative currencies,
- New assets for investment and trading,
- New payment rails including remittance (domestic/FX) and merchant/PoS systems
- Financial inclusion - new financial services for the unbanked or underbanked

However, these innovations must still address the needs of the regulatory system, which exist to protect customers and the market. Though often seen by many as burdensome, an alternative, positive view should be taken. These future opportunities also spawn more opportunities in new technology around identity management, compliance management, reporting and analytics and more.

Proving Bitcoin transactions can be fully compliant do not produce singular outcomes. They set the stage for wider FinTech innovation.

8.2 Suggested next steps for the extension to this PoC

To progress further innovation in creating a trusted digital currency ecosystem for Bitcoin and other cryptocurrencies, there are natural extensions to this PoC. These extensions should address both the security and operational challenges of creating mainstream financial products and services.

Potential next steps and PoCs could include:

Proving an enterprise ready multi-signature key management platform – A second phase of work could look to prove the security and technical rigor of multi-sig key management platform (digital currencies require one mobile, one 'server side' and one cold storage crypto keys for function).

Successful integration with existing banking platforms – The final phase of this project will be to release this proven technology to the general market via:

- Integrating the platform with a bank's existing retail offering, specifically addressing how a cryptocurrency based wallet integrates with a retail banking platform

- Integrating the platform with existing wealth, investment and trading platforms

Related to this topic, an additional PoC that should be considered relates to innovating digital identity, particularly a Poc that aims to minimise the need for physical identity verification.

The industry - FinTechs, banks, financial services organisations and regulators should encourage sustained interest in digital currency projects with a view toward enabling a range of new financial services. The PoC team believe this collective sentiment represents a golden opportunity for Singapore and the region to light a path for the future of banking infrastructure.

Further the extension of this work - in its current form, MAS have the opportunity to consider the following actions to further progress in this space:

- Issue a form of this whitepaper to create the first global standards for digital currencies.

- Evolve these standards and encourage opportunities to create new financial products and services

- Continue exploring other use cases for digital and cryptocurrencies such as new payment rails including remittance (domestic/FX), merchant/PoS systems or even central bank backed digital currencies.