The Journal of FinTech
Vol. 1, No. 1 (2020) 2050001 (27 pages)

DOI: 10.1142/S2705109920500017

World Scientific
www.worldscientific.com

Toward a Public-Key Management Framework for Virtual Assets and Virtual Asset Service Providers

Thomas Hardjono*
MIT Connection Science & Engineering
Massachusetts Institute of Technology
Cambridge, MA 02139, USA
hardjono@mit.edu

Alexander Lipton
MIT Connection Science & Engineering
Massachusetts Institute of Technology
Cambridge, MA 02139, USA
alexlip@mit.edu

Alex Pentland
MIT Connection Science & Engineering
Massachusetts Institute of Technology
Cambridge, MA 02139, USA
pentland@mit.edu

Published

The recent Financial Action Task Force (FATF) Recommendations define virtual assets and virtual asset service providers (VASPs), and require under the Travel Rule that originating VASPs obtain and hold the required and accurate originator information and the required beneficiary information on virtual asset transfers. In this paper, we discuss the notion of key ownership evidence as a core part of originator and beneficiary information required by the FATF Recommendations. We discuss the approaches to securely communicate the originator and beneficiary information between VASPs, and review the existing standards for public-key certificates as applied to VASPs and virtual asset transfers. We propose the notion of a trust network of VASPs in which originator and beneficiary information, including key ownership information, can be exchanged securely off-chain while observing the individual privacy requirements.

*Corresponding author.

Keywords: Virtual asset; virtual asset service provider; blockchain; public-key certificates; key management.

1. Introduction

Since the emergence of the Bitcoin cryptocurrency system (Nakamoto, 2008) over a decade ago, there has been a growing interest in the use of blockchain technology as the basis for exchanging various types of *virtual assets* beyond the original Bitcoin cryptocurrency (Buterin, 2014; Lipton *et al.*, 2018). More recently, in 2018 the Financial Action Task Force (FATF) provided a definition of virtual assets and their service providers, placing cryptocurrency exchanges under the category of *virtual asset service providers* (VASPs). One implication, among others, is that the existing FATF regulatory framework applies to these exchanges, and that exchanges must obtain and hold the originator and beneficiary information in the case of virtual asset transfers.

In this paper, we review the use of existing standards in the area of public-key certificates and certificate management in the context of VASPs. There are several goals of this paper. The first goal of this paper is to review the existing methods and standards dealing with information pertaining to public keys, key ownership and key operators. More specifically, we discuss the use of the existing standards for public-key certificates and the services used by certification authorities (CAs) as a means to obtain originator and beneficiary information prior to the transfer of virtual assets, thereby providing a compliant solution for these new types of service providers. We also discuss the need for VASPs to exchange customer information using the existing standards for attributes or claims. The public-key certificates of customers, as well as their attribute information should be communicated out-of-band (off-chain) between VASPs.

The second goal of this paper is to propose and discuss the notion of a *trust network* of VASPs as a way for the community of VASPs to exchange out-of-band relevant information regarding their customers and related keys (Sec. 8). The trust network should be based on the common *operating rules* which govern the daily running of the trust network.

Our third goal is to propose a number of areas of innovation for the nascent virtual asset industry (Sec. 9). This includes new mechanisms to expand the discoverability and reachability of VASPs globally. This will allow better connectivity and information sharing among the various VASPs around the world — in much the same way as internet service providers

(ISPs) in the Internet share route and endpoint reachability information among the community of ISPs globally.

2. Virtual Assets and VASPs

The *Financial Action Task Force* is an inter-governmental body established in 1989 by the ministers of its member countries or jurisdictions (FATF, 2019a). The objectives of FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering (ML), terrorist financing (TF) and other related threats to the integrity of the international financial system. The FATF is a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

The FATF has developed a series of *Recommendations* that are recognized as the international standard for combating money laundering and the financing of terrorism and proliferation of weapons of mass destruction. They form the basis for a coordinated response to the threats to the integrity of the financial system and help ensure a level playing field. First issued in 1990, the FATF Recommendations were revised in 1996, 2001, 2003, 2012 and most recently in 2018 to ensure that they remain up to date and relevant, and they are intended to be of universal application.

With the emergence of blockchain technologies, virtual assets and cryptocurrencies, the FATF recognized the need to adequately mitigate the ML and TF risks associated with virtual asset activities.

In its most recent Recommendation 15 (FATF, 2018), the FATF defines the following:

- *Virtual asset*: A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.
- *Virtual asset service providers*: Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: (i) exchange between virtual assets and fiat currencies; (ii) exchange between one or more forms of virtual assets; (iii) transfer of virtual assets; (iv) safekeeping and/or administration of virtual assets or instruments

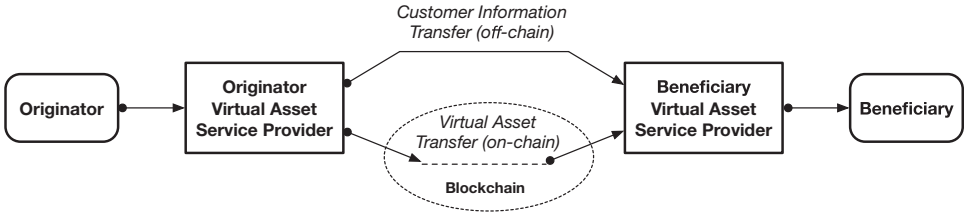

Fig. 1. Information transfer between VASPs occurring off-chain (out-of-band).

enabling control over virtual assets; and (v) participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

In this context of virtual assets, transfer means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another (see Fig. 1). Furthermore, to manage and mitigate the risks emerging from virtual assets, the Recommendations state that countries should ensure that VASPs are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.

3. The Travel Rule for Virtual Assets on Blockchains

One of the key aspects of the FATF Recommendation 15 is the need for VASPs to retain information regarding the originator and beneficiaries of virtual asset transfers:

> "Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers, submit the above information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities. Countries should ensure that beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers, and make it available on request to appropriate authorities. Other requirements of R.16 (including monitoring of the availability of information, and taking freezing action and prohibiting transactions with designated persons and entities) apply on the same basis as set out in R.16. The same obligations apply to financial institutions when sending or

receiving virtual asset transfers on behalf of a customer" (FATF, 2019b, Para. 7(b)).

The implication of the note (FATF, 2019b) is that cryptocurrency exchanges and related VASPs must be able to share the originator and beneficiary information for virtual asset transactions. This process — also known as the *Travel Rule* — originates from under the US Bank Secrecy Act (BSA — 31 USC Secs. 5311–5330), which mandates that financial institutions deliver certain types of information to the next financial institution when a funds transmittal event involves more than one financial institution. This rule became effective in May 1996 and was issued by the US Treasury Department's Financial Crimes Enforcement Network (FinCEN). This rule was issued by FinCEN concurrently with the BSA record keeping rules for fund transfers and transmittals of funds.

Given that today, a virtual asset on blockchain is controlled through the public–private keys bound to that asset, we believe there are other information (in addition to the customer and account information) that a VASP needs to retain in order to satisfy the Travel Rule:

- *Key ownership information*: This is information pertaining to the legal ownership of cryptographic public–private keys.

  When a customer (e.g., originator) presents his/her public key to the VASP for the first time, there must be a "chain of provenance" evidence regarding the customer's public–private keys which assures that the customer is the true owner. The point is that just because an entity can prove possession of the private key, it does not necessarily follow that the entity is the legal owner of the public–private keys. Proof of possession alone is insufficient to prove legal ownership. The ability to prove legal ownership of the public–private keys may be crucial in different types of applications of virtual assets (e.g., property ownership).
- *Key operator information*: This is information or evidence pertaining to the legal custody by a VASP of a customer's public–private keys.

  This information is relevant for a VASP who adopts a key-custody business model in which the VASP holds and operates the customer's public–private keys to perform transaction on behalf of the customer.

We believe that the Travel Rule provides the emerging VASP industry with opportunity today to develop competitive innovations around the correct identification of owners of virtual assets and provide them with user-friendly ways to transfer virtual assets at a global scale. Early attempts to use

public-key certificates for blockchain systems have been made [see, e.g., Peyton (2018)], but more research and development need to be conducted. Rather than weaken the Travel Rule to satisfy the short-term needs of a small number of VASPs, governments and VASP businesses should direct research and development into future infrastructures for virtual assets, digital identities, public-key certification and the safe management of customer keys. We discuss several possible areas for innovation in Sec. 9.

4. VASPs as Virtual Asset Exchanges and Key Operators

In recent years, two popular types of VASPs have emerged, namely *centralized exchanges* (CEXs) and *decentralized exchanges* (DEXs). A centralized exchange may or may not hold a customer's private key. In the case that it does, we refer to the exchange as a "custodial exchange" because it has legal custody of the public and private keys. In this case, the CEX uses the customer's public–private keys under legal custody to perform (sign) transactions sent to the cryptocurrency network.

In contrast, some centralized exchanges do not hold a customer's keys. Instead, they simply create an account for the customer in the traditional manner. Here, the CEX has one or more public–private keys of its own which it uses to interact with the cryptocurrency network, and it is the CEX that controls these keys (not the customer). Furthermore, the CEX simply commingles all its customer's funds or virtual assets into one consolidated fund. For the customer, the custodial CEX approach has the attraction of relieving the customer from having to manage cryptographic keys. It also relieves the customers from having to obtain on their own financial insurance over their virtual assets. The CEX could obtain insurance over the entire commingled funds.

The notion of DEX is the one where the various functions (e.g., bid, ask, trade) related to trading are performed in the blockchain system itself (e.g., smart contracts running on nodes of the blockchain). The user employs a *wallet* (hardware and/or software) which holds the user's public–private keys and which performs the signing of transactions using the private key. Here the users trade directly from their wallets without having to trust a centralized entity.

Currently, the VASP landscape is evolving and as a result there is a degree of confusion today with regard to the notion and functions of an exchange in the context of virtual assets. As mentioned previously in Sec. 3, we believe that the Travel Rule will necessitate VASPs who operate as a centralized exchange to address the issue of retaining key ownership information and key

operator information. This is particularly important for VASPs from a risk exposure management perspective and from the virtual asset insurance requirements (Chavez-Dreyfuss, 2018). Figure 2 attempts to summarize the relationships between VASPs, the originator/beneficiary and the location of keys used to perform transactions. Note that Figs. 2(a1)–2(c1) are

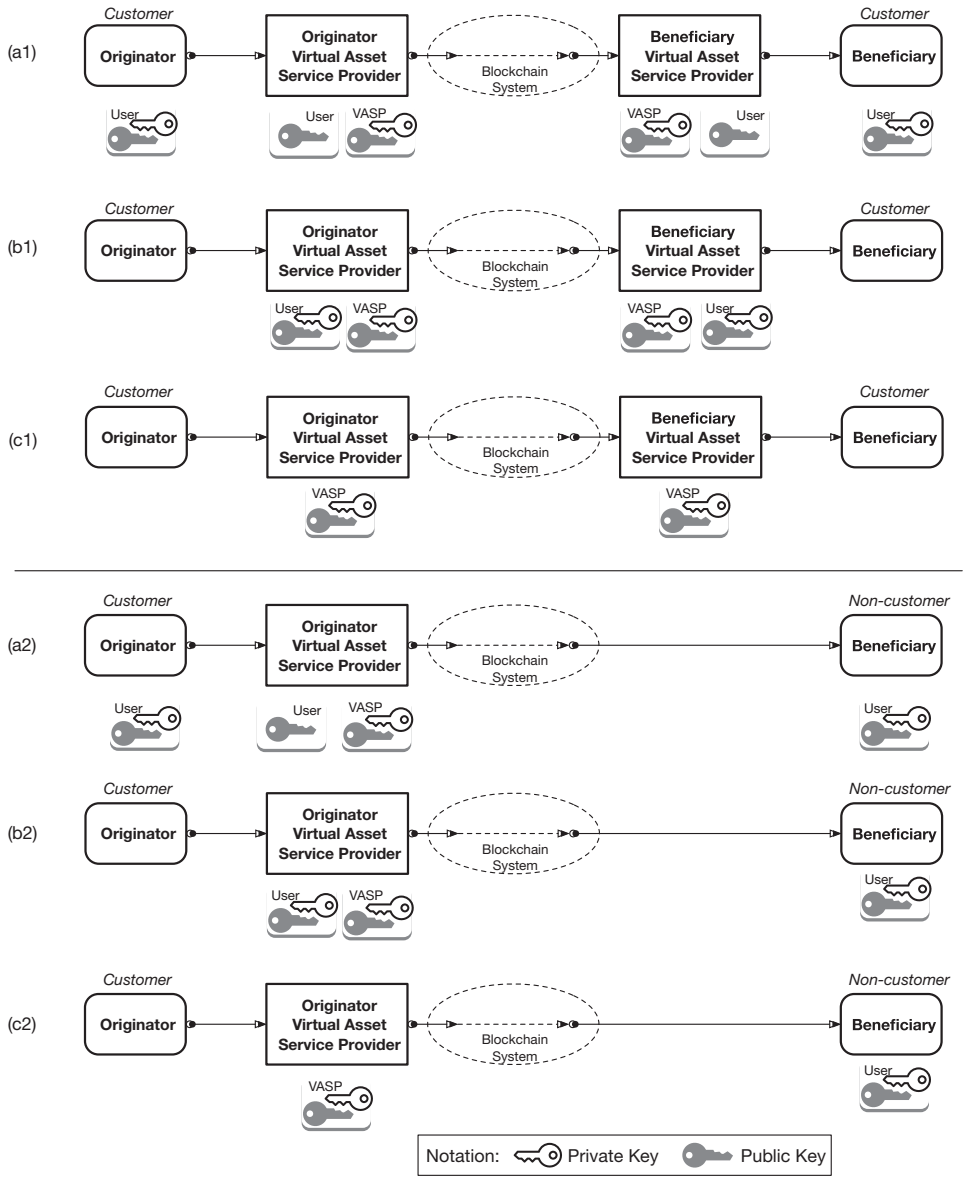

Fig. 2. VASPs as virtual asset exchanges and key operators.

symmetrical in that there is an Originator-VASP and a Beneficiary-VASP. In contrast, Figs. 2(a2)–2(c2) are asymmetrical in that there are no Beneficiary-VASPs present.

An overview of the relationships shown in Fig. 2 is as follows:

- *VASP-mediated asset transfers*: In this model the customer holds his/her public–private keys while the VASP holds a copy of the customer's public key only (not his/her private key). This model may be suitable for customers who seek the mediation of the VASP in asset transfers (e.g., for legal purposes) but who may not wish to provide the VASP with their private key. This is represented in Figs. 2(a1) and 2(a2).
- *VASP key-custody asset transfers*: In this model, the VASP holds custody of the customer's public–private keys. Upon instruction from the customer, the VASP signs transactions on behalf of the customer using the customer's private key. This is represented in Figs. 2(b1) and 2(b2).
- *VASP key-commingled asset transfers*: In this model, the VASP uses its own public–private keys to perform virtual asset transfers. This is represented in Figs. 2(c1) and 2(c2).

  Multiple asset transfer instances could be merged into a single transaction, thereby saving some transmission cost of the Originator-VASP [e.g., "gas" fee in Ethereum (Buterin, 2014)]. The beneficiaries information must still be communicated by the Originator-VASP to the Beneficiary-VASP out-of-band.

Note that combinations of models represented by Figs. 2(a1)–2(c1) can be achieved. For example, on the sending side the originator entity could be holding its public–private keys as shown on the left-hand side of Fig. 2(a1), while on the receiving side the beneficiary entity could be using a key-custody service offered by the Beneficiary-VASP as shown on the right-hand side of Fig. 2(b1). Although not shown in Fig. 2, customers may be using other public–private keys to establish a secure and authenticated channel between the customer and the respective VASP. In the remainder of this paper we will not discuss these auxiliary keys, and focus solely on keys that are used to transfer virtual assets on the blockchain (i.e., the public keys that are recorded on the confirmed transactions on the ledger).

5. Public-Key Certificates and the Travel Rule

One of the fundamental challenges of public-key cryptography since its inception in 1978 (Rivest *et al.*, 1978) is that of *proving ownership* of a given

public key. When two parties sign a contract or exchange signed messages, both parties need assurance that they are employing the correct public keys belonging to the respective parties (i.e., not stolen from another user). They also need the feature of *non-repudiation*, meaning that a signer must be deterred or prevented from cheating by way of claiming — after a contract has just been signed — that his/her private key was stolen before the contract was signed (e.g., thereby repudiating the signing of the contract). In the context of the Travel Rule (FATF, 2019b, Para. 7(b)), VASPs will need to retain evidence of key ownership for compliance purposes. The existing standards pertaining to *public-key certificates* may provide the basis for VASPs to record information regarding the ownership of public keys related to virtual assets.

In the late 1990s the computer industry developed the notion of public-key *ownership registration and certification* (Housley and Polk, 2001). The idea of registration and certification is to unambiguously determine the legal ownership of a public key, and therefore, provide the recipient of a signed contract or message with a degree of *assurance* — for business risk assessment — of the true identity of the signer (the owner of the public–private keys). The goal was to establish a *public-key framework* (Barker *et al.*, 2015; Barker, 2016) that allowed for legal interpretation to be created atop the framework, where roles, responsibilities and liabilities would be unambiguously identified and risks allocated. The notion of a public-key framework paved the way for the eventual establishment of the e-Signature Act in 2000 (United States Congress, 2000).

In contrast, around the same time, some in industry sought to develop "self-certification" for public keys in which the key owner would self-declare his/her ownership to friends and family in a "web of trust" model [see, e.g., PGP in Atkins *et al.* (1996)]. However, in the context of business transactions, self-certification came to be viewed as having little or no value, and as such the "web of trust" philosophy failed to gain adoption in the business community.

In order to understand why public-key certificates are core to conducting business on the Internet, it is important to understand the notion of *technical trust* and *business trust*. In order for two transacting parties to obtain assurance of each other's key ownership, a neutral *trusted third party* is needed to "vouch" for key ownerships of the respective parties — by way of performing ownership registration and certification of public keys. This trusted third party is referred to as the *Certification Authority* (CA), and the result of certification is a data structure referred to as *public-key certificates*, typically employing the X.509 standard format. A certification authority issues an

version	*The version of the specification used (e.g. X.509 version 2 or 3)*
serialNumber	*The unique serial number of this certificate*
signature	*The signature algorithm-identifier employed for this certificate*
issuer	*The Certification Authority (issuer) who issued & signed this certificate*
validity	*The validity duration of this certificate (not before; not after)*
subject	*The subject (user) who "owns" or holds the matching private-key*
subjectPublicKeyInfo	*The public-key of the subject (user)*
extensions	*The extensions included in this certificate*
signatureAlgorithm	*The algorithm used by the Certification Authority (issuer) to sign this certificate*
signatureValue	*The digital signature Certification Authority (issuer)*

Fig. 3. Summary of X.509 (v3) certificates (Housley *et al.*, 1999).

X.509 certificate by digitally signing the certificate using its own private key. By signing it, the certification authority legally *attests to the truthfulness* of its assertion that the public key listed in the X.509 certificate is owned by the subject (person or organization) listed in the same certificate (see Fig. 3). One can therefore say that a certification authority "binds" a given public key to its owner (the subject). The overall goal of a certification authority issuing (signing) a public-key certificate under a given public-key framework is to support the correct identification of the subject and indirectly provide the basis for the *chain of provenance* of the public key. The standard protocols and formats related to public-key certificates are the X.509 public-key standard (Housley *et al.*, 1999; Cooper *et al.*, 2008; ISO, 2017) (ISO/IEC 9594-8). Figure 3 summarizes the typical X.509 public-key certificate, while the JSON-based format has also been standardized recently.

The certification authority itself asserts the ownership of its public key in the form of a *root certificate* using the same X.509 certificate standard. The X.509 root certificate is typically self-signed by the certification authority using its private key (matching the public key stated in the root certificate). In order to prevent the certification authority from cheating by way of modifying the root public–private keys, the root certificate is typically made available to the broad community in numerous ways. This can be achieved, e.g., by publishing the root certificate in newspapers and bulletins, by shipping copies inside browsers, by inclusion in hardware and so on. In this way the certification authority is prevented from repudiating or falsifying its own self-signed root certificate.

As a neutral trusted third party, a certification authority operates services pertaining to the registration, certification and revocation of public-key ownership. As a legal business entity, a commercial certification authority must publish (e.g., on its website) a service-level agreement (SLA) pertaining to these services. This service agreement is referred to in industry as the *Certificate Practices Statement* (CPS) (Chokhani *et al.*, 2003). Prior to registering his/her public key to a given certification authority, a key owner (subject) must review the CPS document belonging to that certification authority and determine whether the terms of the service in the CPS (e.g., key management procedures, liabilities, warranties for key loss, etc.) are acceptable to the key owner. Some examples of CPS statements can be found in Symantec (2013) (from Symantec/VeriSign, Inc.) and Apple Inc. (2019a) (from Apple Inc.).

Today X.509 certificates are ubiquitous across different markets, verticals and applications. The X.509 certificates are used extensively within banking and finance (SWIFT, 2017; Trustis, 2017), in defense and military networks (CNSS, 2009), in government and federal systems (Barker *et al.*, 2015; Kuhn *et al.*, 2001), and within many consumer electronic products [e.g., PCs (Apple Inc., 2019b; Microsoft, 2018), TPM hardware on laptops (Hardjono, 2008; Microsoft, 2017), smartphones (Apple Inc., 2019b), USIM smartcards (Gemalto Inc., 2008), cable-modems (CableLabs, 2019), etc.]. They are used extensively within routers, Virtual Private Networks (VPNs) and other network elements. Today in the networking industry, the VPN sub-segment alone is forecasted to reach US$70 billion dollars in the next few years. Most, if not all, websites today employ one or more X.509 certificates (of varying qualities) for SSL connections, and billions of SSL connections are made every day from the users' browsers to the various certificate-enabled websites around the world.

In the context of VASPs and virtual assets bound to public keys, there are at least two approaches that VASPs can adopt with regard to public-key certificates as a means to prove key ownership (Fig. 4):

- *VASP outsources customer public-key certification to a CA*: In this approach, a VASP outsources the management tasks relating to its customer's public-key certificates to an external (commercial) certification authority. This approach allows a VASP to focus on its primary business, leveraging the expertise of the certification authority. All public-key certificate management tasks, including certificate revocation, are performed by the external certification authority.

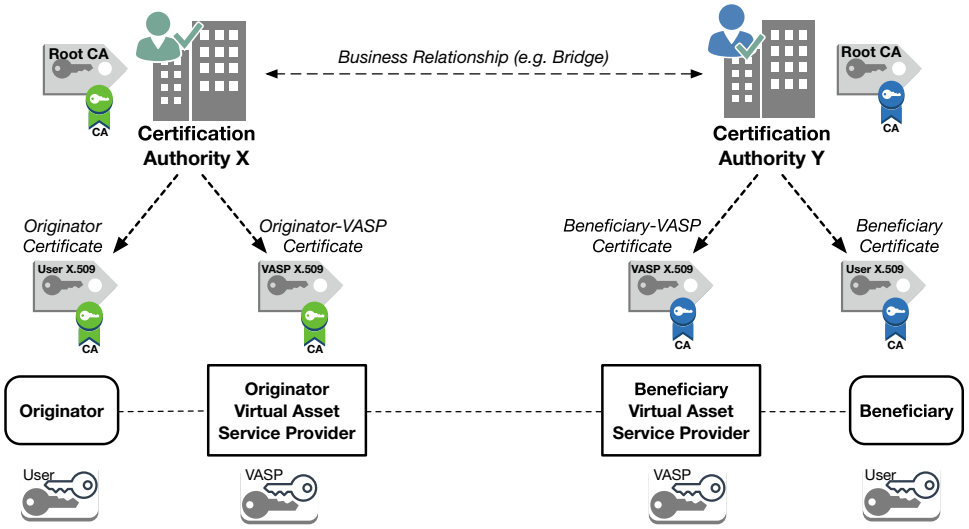

Fig. 4. Role of certification authority for key ownership for the virtual assets.

Here, when an entity (individual or organization) as the subject seeks to open an account at the VASP accompanied by its public key [see Figs. 2(a1) and 2(a2)], the VASP can redirect the entity to the external certification authority with whom the VASP has a business relationship. After the entity has been successfully issued with an X.509 certificate for its public key, the certification authority can provide a copy of this certificate to the VASP. A similar approach can be used for VASPs which adopts a key-custody model, in which the VASP requests a public-key certificate for each customer key in its custody.

Identification information collated by the external certification authority for the enrolling subject can be shared with the VASP, thereby aiding the VASP in its efforts to comply to the Travel Rule.

- *VASP becomes a public-key certification authority*: In this approach, the VASP itself becomes a certification authority for its customer's public-key certificates. This approach may be attainable by a VASP depending on its business needs and on the size of its customer base. However, all the complex certificate management tasks must be performed by the VASP.

A third possible approach is a blend between the above, in which a *hosted* certification authority approach is used. Here the certification-related services are operated by a commercial certification authority (as a "white-labeled" service), but the issuance of the certificates and key management are

under the full control of the VASPs as the legal issuer. In this case the VASP takes on the legal liabilities as the customer-facing certification authority.

6. Off-Chain Exchange of Customer Information between VASPs

For virtual asset transfers, the Travel Rule requires that originating VASPs obtain and hold the required and accurate originator information, and the required beneficiary information. They are also required to submit this information to the beneficiary VASP and make it available upon request to appropriate authorities (FATF, 2019b, Para. 7(b)). Traditionally, this information includes the originator's name, account number, address, the identity of the Originator-VASP, the amount, execution date and the identity of the Beneficiary-VASP. Additionally, on the side of the Beneficiary-VASP, for the incoming asset transfers, the VASP must obtain and hold information regarding the beneficiary's name, account number, address and other beneficiary identifiers.

In the context of blockchain systems as the medium of transacting using public keys, the scope of information regarding the customers (originator and beneficiary) must now include their public-key information — or what is referred to as the "address" in the blockchain colloquial terminology. As we suggested in Sec. 3, this account information must now include (i) key ownership information and (ii) key operator information for the customer's public–private keys used on the blockchain. As further discussed in Sec. 4 and as illustrated in Fig. 2, an Originator-VASP must retain key ownership information and key operator information for (a) the Originator-VASP itself, (b) the originator customer, (c) the Beneficiary-VASP and (d) the beneficiary customer.

There are several aspects related to the collection of customer information in the context of public keys:

- *Customer information collected at the time of certificate creation*: Customer information must be collected prior to the issuance of their public-key certificates. Certification authorities commonly require customers (subjects) — whether individuals or organizations — to submit the required information in the *Registration* phase of the certificate management lifecycle (Housley *et al.*, 1999; Housley and Polk, 2001; Kuhn *et al.*, 2001). During this phase it is the main task of the certification authority to perform identity verification (of the subject) enrolling for the certificate.
- *Standardized certificate classes based on customer information provenance*: Over the last two decades, several CAs have developed the notion of *classes*

or *grades* of public-key certificates that reflect the confidence in the accuracy and provenance of the information regarding the customer to whom the certificate was issued. The classes or grades of certificates issued by a certification authority are commonly described in the CPS (Chokhani *et al.*, 2003) of that certification authority.

As an emerging industry, VASPs can collectively define the notion of classes of certificates for their industry based on the required customer identification information and confidence level during the customer registration phase. A *standard definition of certificate classes for the VASP industry* allows VASPs to require (demand) that certification authorities fulfill the relevant customer identity verifications and report this information and level of confidence to the VASP as part of the service agreement.

- *VASP's collation of customer identity information from the certification authority*: In the case where a VASP outsources the issuance of certificates to an external CA, the VASP must obtain a copy of the customer identity information from the certification authority and retain it as part of customer due diligence (CDD) for compliance to the Travel Rule.
- *Refusal of customers without certificates or with uncertain identities*: In order to comply to the requirements of the Travel Rule, a VASP should simply deny customer requests for virtual asset transfers when the customer does not possess a certificate issued by a known reliable certification authority, or when the issuing certification authority has only low-assurance (low-confidence) information regarding the customer.

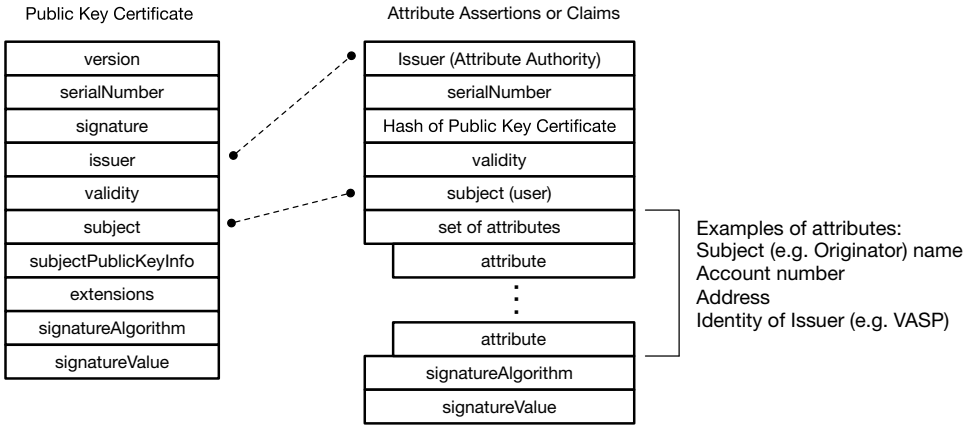

Fig. 5. Representation of customer information in attributes assertion.

- *Certificate validation prior to virtual asset transfer*: Prior to a virtual asset transfer, an Originator-VASP must perform certificate validation of the public-key certificates of (i) the originator customer (the customer of the Originator-VASP), (ii) the Beneficiary-VASP and (iii) the beneficiary customer (the customer of the Beneficiary-VASP). This is discussed further in Sec. 7.
- *Customer information communicated out-of-band between VASPs*: As mentioned in Sec. 2 and illustrated in Fig. 1, VASPs should exchange customer information and customer certificates (and their own VASP certificates) out-of-band over a secure and authenticated channel. Here, the VASP industry can standardize the APIs and connection-endpoint definitions to allow inter-VASP exchange of customer information in a fast and efficient manner prior to the virtual asset transfer. This is discussed further in Sec. 8.
- *Standardization of customer attribute information*: The VASP industry should define and profile the customer (subject) data items required under the Travel Rule to be exchanged between VASPs as part of any virtual asset transfer event. We refer to these data items as the *attributes* of the originator, beneficiary and their corresponding VASPs.

  There are several standards in existence to represent attribute information of a subject (e.g., individual or organization) and protocols which support the delivery of these attributes securely in the open Internet of today. Examples include the X.509 *Attribute Certificate* (Farrell and Housley, 2002), the XML *Security Assertions Mark-up Language* (SAML) (OASIS, 2005), the OpenID *Identity Token* (Sakimura *et al.*, 2014) and the recent JSON-based *Verifiable Claims* (Sporny *et al.*, 2019).

7. VASP Verification of Beneficiary Public-Key Certificates

As we mentioned previously, an Originator-VASP needs to validate all relevant pubic-key certificates prior to virtual asset transfer. This is because any errors related to the destination public keys or about the subject identities can have dramatic impact on the VASP from both economic and regulatory compliance perspectives.

Unlike wire transfers in correspondent banking, transactions on blockchain systems such as Bitcoin (Nakamoto, 2008) are "permanent" (or "immutable" as commonly stated) in the sense that once it is confirmed the transaction remains in the recorded blocks (ledger) of the blockchain system. This means that an erroneous asset transfer transaction cannot be canceled, reversed or

removed from the ledgers of the blockchain system once the transaction has been confirmed. This lack of a *multi-phase commitment scheme* (Gray and Lamport, 2006) means that a mistake or error in an asset transfer to a Beneficiary-VASP requires the Beneficiary-VASP to return the asset in a separate transaction on the blockchain. It is worth noting that currently most wallets and blockchain systems generally do not employ a phased commitment model in which a "pre-commit" phase is followed by a "final-commit" phase in the sense of classical transactional database system. New blockchain systems such as the Hyperledger Fabric (Androulaki *et al.*, 2018) employ Orderers and Endorsers (i.e., special nodes) that create temporary read/write sets prior to finalizing the read/write set of transactions. However, this process occurs as part of the consensus-making cycle and is outside the control of the sender or receiver VASPs.

The implication here is that in order to avoid errors in virtual asset transfers, in addition to verifying user account information an Originator-VASP must validate the origin and destination public keys of the parties *prior* to broadcasting the transaction to the blockchain system.

However, there are other circumstances that may complicate this validation process:

- *Originator possesses only its own uncertified public key*: Many cryptocurrency users today employ a digital wallet (software and/or hardware) that holds only the user's own public–private keys and the public keys ("addresses") of other users. As such, there are cases where the originator customers may not as yet possess a certificate for their public keys. If the originator is a customer of the VASP, one possible course of action is for the VASP to redirect the customer to enroll for a public-key certificate following the standard X.509 enrollment process.
- *Originator possesses public-key certificate*: In the case that the customer provides a copy of his/her public-key certificate, the VASP must validate the certificate status to the issuing certificate authority. The X.509 standard has protocols to perform this validation in an efficient manner (Myers *et al.*, 1999; Santesson *et al.*, 2013).
- *Originator possesses only the uncertified public key of the beneficiary*: Similar to the previous scenario, an originator customer of a VASP may only be in possession (i.e., in his/her wallet) of the public key of the beneficiary, without a corresponding certificate.

  In this case, the Originator-VASP has the task of searching for the beneficiary's certificate among other VASPs or certificate authorities.

Typically X.509 certificates can be fetched from the issuer service via a standardized endpoint (e.g. Uniform Resource Identifier (UFI) for certificates) (Gutmann, 2006).

- *Originator only knows the beneficiary account information*: In this scenario, the originator customer may only be in possession of the beneficiary's name and account number, and possibly the name of the destination Beneficiary-VASP.

  In this case, the Originator-VASP has the task of locating and inquiring the Beneficiary-VASP about the account of the beneficiary at that VASP using traditional means.

In order to prevent an Originator-VASP from querying every known certification authority in the world — an approach that is not only impractical but vastly inefficient — one potential solution is for the community of VASPs and their respective certification authorities to form a trust network that shares known good public keys and also the certificate revocation lists. This topic will be discussed further in Sec. 8.

8. Toward a Trust Network of VASPs

The Internet has been successful over the past three decades because of a number of sound architecture designs. One architecture design decision was to allow organizations to own and operate portions of the Internet as *autonomous systems*, allowing each autonomous system to run its own interior routing protocol with its own network topology for its network elements (e.g., routers, bridges, etc.). Each autonomous system would be allocated unique identifier (i.e., AS number) and each autonomous system would represent independent networks (e.g., Local Area Networks (LANs), WANs, backhaul networks, etc.) owned and operated by various independent entities (e.g., ISPs, universities, governments, military, etc.). Thus, the Internet of today is in reality composed of numerous autonomous systems that are "stitched" together, presenting to the user end-to-end IP connectivity. Autonomous systems employ *peering agreements* or contracts among themselves in order to negotiate the IP traffic volumes and routing patterns. These agreements permit each autonomous system to *advertise routes* that are available through that autonomous system, resulting in the reachability of (most) IP addresses globally.

Similarly, the SWIFT banking network that began in the 1970s as a messaging network for sharing bank and account information has evolved over the past three decades into a global network that employs IP-based

messaging (SwiftNet). Instead of employing pair-wise (bilateral) key exchanges, it has also adopted public-key certificates as a more scalable solution for end-to-end entity authentication of members of the network (Finextra, 2004; SWIFT, 2017).

We believe that in order to solve various issues around the Travel Rule and challenges in obtaining the originator/beneficiary customer information, it is in the best interest of VASPs to collectively establish a *VASP trust network* in a manner similar to the ISP community on the Internet.

Some of the fundamental requirements of a VASP trust network are as follows:

- *VASP-only network*: The VASP trust network should allow the exchange out-of-band of relevant customer-related information as well as blockchain-transaction details. The trust network among others should include a technical public-key framework, a common definition of services and interfaces and a legal framework (system rules definition) for all its membership.

  The trust network could also deploy a VASP-only management-supporting blockchain system for solely the purposes of common audit and reporting. Depending on the design of this VASP-only management blockchain, hashes of the latest list of known good public keys (and pointers to their file locations) could be captured periodically on this blockchain.
- *Independence from asset transfer blockchains*: The VASP trust network must be independent of any blockchain system as the medium of virtual asset transfers. Like the Internet routing autonomous systems, in the future there will be dozens to hundreds of blockchain systems operating around the world (e.g., for different types of virtual assets), presenting several challenges for blockchain interoperability (Hardjono *et al.*, 2019). As an emerging industry, VASPs must ensure that their trust network architecture can interoperate with any and all future asset transfer blockchains.
- *VASP-to-VASP secure channels based on VASP public-key certificates*: In order to have the ability to quickly establish secure and authenticated channel pair-wise between VASPs in the trust network, the members of the trust network should each possess public–private keys and a certificate solely for interacting on the trust network. The use of certificates simplifies the task of communicating the public keys of members of the trust network. In the case that the trust network employs a VASP-only management blockchain system, then separate public–private keys must be used for that blockchain system.

Some VASPs today are already employing X.509 certificates for protecting SSL connections from the customer's browser to the VASP service platform. However, this minimal use of SSL certificates needs to be enhanced (e.g., end-to-end integration with customer wallets, validation of chains of certificates and attribute claims, cross-VASP certificate queries, etc.).

A trust network of VASPs enables and promotes virtual asset transfers globally in the following ways:

- *Synchronization of blockchain transactions to customer identity*: The use of a trust network running parallel to the asset-transactions blockchain allows an Originator-VASP to communicate to the Beneficiary-VASP ahead of the transaction on the blockchain. The tight synchronization between the customer information sent through the trust network and the asset transaction on the blockchain provides the foundation for (i) post-event auditing/reconciliation and (ii) evidence for conflict resolution among VASPs who are members of the trust network.
- *Exchange of information about active and revoked customer certificates*: VASPs who are members of the trust network can exchange with each other some minimal information regarding the public-key certificates of their respective customers.
- *Exchange of signed assertions about customers*: When an Originator-VASP queries another VASP in the trust network and obtains a valid copy of the public-key certificate of a customer of that VASP, the Originator-VASP has the option to further query that VASP for additional account information regarding the customer of that VASP. There are several standard protocols that can be used to deliver customer information assertions or claims [e.g., SAML (OASIS, 2005) and OIDC (Sakimura *et al.*, 2014) are used extensively in various identity provider communities].
- *Global interconnection of multiple VASP trust networks*: In order for the VASP industry to scale up its services toward a global customer base, the trust networks of VASPs need to be interconnected in the same manner as autonomous systems are interconnected together based on ISP peering contracts. A global interconnection of multiple VASP trust networks allows a VASP in one trust network (domain) to obtain "clues" as to the existence of another VASP in a different trust network (foreign domain) who may be in possession of information relating to a destination customer's public key.

For example, in Fig. 6, the VASP at point A in Trust Network 1 who is seeking to fulfill an asset transfer request from the originator in Trust

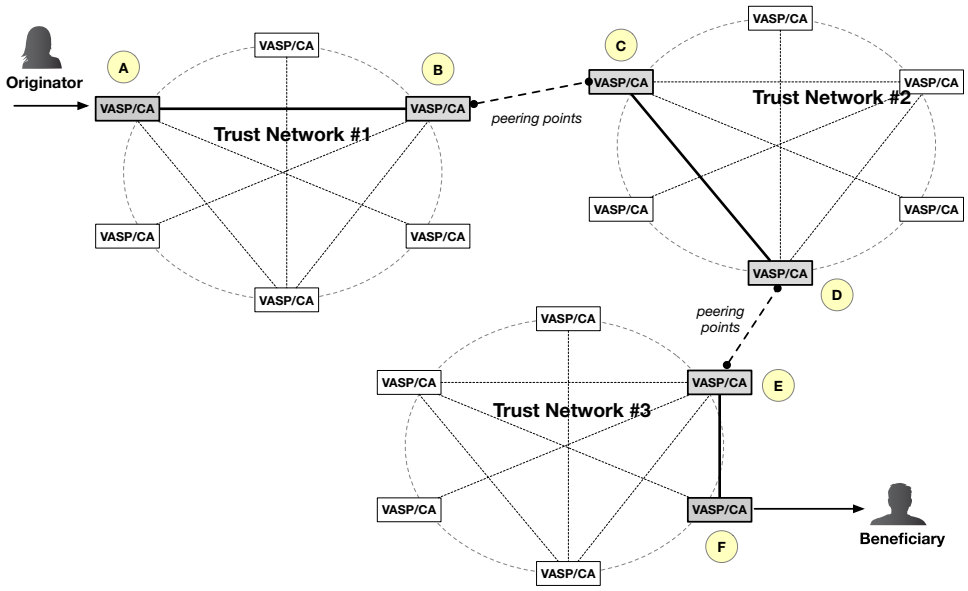

Fig. 6. Global interconnection of multiple VASP trust networks.

Network 1 to a beneficiary in Trust Network 3 may obtain reachability knowledge about a remote VASP at point F within Trust Network 3. The expectation is that the VASP at point F may possess the public-key certificate and assertions regarding the beneficiary (who is expected to be a customer of that remote VASP).

This reachability information can be "advertised" from the VASPs in Trust Network 3 through Trust Network 2 into the VASPs at Trust Network 1. This can be achieved through the peering point between the VASPs at point B and point C, and the peering point between the VASPs at point D and point E. That is, the Originator-VASP at point A hears about Beneficiary-VASP at point F because of the "route advertisements" — namely the summary list of public keys or serial numbers known in Trust Network 3 — being shared through the VASPs within Trust Network 2.

9. Areas for Innovation

There are several areas of innovation where VASPs as an emerging industry can take leadership and define the next-generation infrastructure for the global virtual asset commerce.

9.1. *Operating rules for the trust network of VASPs*

Following on from the discussion of VASP trust networks in Sec. 8, one area of innovation for the virtual assets and VASP industry is the development of a common set of *operating rules* suitable for the VASP industry.

Similar to other organizations [e.g., NACHA (NACHA, 2019), Visa (Visa, 2013), OIX (Makaay *et al.*, 2017)] the operating rules for the VASP trust network describe a legally enforceable set rules and agreements that govern the day-to-day running of the trust network as a multi-party system established to achieve the common purposes of its members. In the case of the trust network of VASPs, these common purposes include the sharing of: (i) VASP entity information, (ii) customer information, (iii) key ownership information, (iv) key operator information and (v) VASP reachability parameters. These operating rules must be founded on a common set of business requirements and technical specifications. This in turn allows each member of the trust network to obtain assurance that each of the other participants will follow the same set of rules, defined for their particular role in the trust network.

Good operating rules for a VASP trust network provide its members with several benefits. First, they provide a means for the members to *improve risk management* because the operating rules will allow members to quantify and manage risks inherent in participating within the trust network. Second, the operating rules provide the members with *legal certainty and predictability* by addressing the legal rights, responsibilities and liabilities of the participants in the trust network. Because the operating rules are a legal agreement, they are legally enforceable upon all members. Third, the operating rules provide *transparency* to the members of the VASP trust network by making the terms of agreements, technical specifications (e.g., Application Programming Interface (API), minimal performance delivery, etc.) and other member business rules — comprising the operating rules — accessible to all participants.

There are several business drivers for establishing a VASP trust network. Beyond the basic set of services that members must implement to be part of the trust network, each member is free to offer product/service differentiation in the market while complying to the operating rules. This in turn allows a VASP to broaden market adoption by enhancing these basic services with better features (e.g., faster response, richer customer information set, better privacy protection for customer information, etc.). From the cost-reduction perspective, standardizing the technical functions across all services of members of the trust network allows for reusability of components (e.g., share

common set of APIs and software libraries) and more efficient compliance adherence, thus having the overall effect of lowering costs for all members and their respective customers.

9.2. *Certificate profiles and CPS for VASP trust network*

An important part of the operating rules of the VASP trust network is the standardization of common technical solutions relevant to the shared goals of the trust network. For example, in relation to the questions of key ownership information and key operator information, the members should develop a common CPS and certificate profile (CP) for the public-key certificates within the trust network. The operating rules should define all aspects and phases of public-key management lifecycle for all members of the VASP trust network.

There are several technical decisions regarding the certificate features that can be defined or expressed through the certificate profile. For example, the certificate profile could narrow the permitted usage of the public–private keys to that of signatures only (not encryption). Additional VASP-specific extension could be defined that may limit usage of the public–private keys to only specific blockchain systems (e.g., can be used to sign transactions only for the Ethereum network).

9.3. *Expanding the discoverability and reachability of VASPs*

Following on from Sec. 8, there are several possible areas of innovation pertaining to the exchange of VASP-related information — within a trust network and across trust networks (inter-network as shown in Fig. 6) — for the purpose of expanding the *discoverability* and *reachability* of VASPs. The ability for a VASP to broadcast a query to the trust network in search for a public-key certificate of a beneficiary represents an innovative function that promotes scaling of VASP services. Queries should lead to responses that indicate whether an originator/beneficiary is associated with a VASP within the local trust network or with a VASP in a different trust network.

Standard protocols exist today to allow access to certificate stores via a HTTP/SSL connection (Gutmann, 2006). However, additional technical extension needs to be developed that allows VASPs in a trust network to exchange lists of serial numbers (or valid certificates) as well as list of public keys. These periodic exchanges or broadcasts in the trust network can be based on incremental changes — so-called "deltas" [akin to Delta CRLs in Cooper *et al.* (2008)] — in order to minimize bandwidth consumption.

A given VASP may belong to multiple trust networks, or it may have a bilateral business agreement with another VASP in a different trust network. These VASPs could become "gateways" to allow certificate-related information to flow from one trust network into another trust network, thereby increasing the "reach" of the cross-network services as a whole.

9.4. *Anonymous-verifiable identities and public keys in the trust network*

Further research and development should be devoted to a class of cryptographic schemes that support a capability which we refer to informally as *anonymous but verifiable identities* (public keys) with "selective disclosure" features. This capability could be made available to customers of VASPs who are members of a VASP trust network with legally-binding operating rules. Here the cryptographic scheme should allow a customer to possess a single private key bound to multiple public keys in such a way that the public keys are *unlinkable* to each other when viewed by external entities. Thus, when these public keys are used on a blockchain system, it should be computationally difficult (infeasible) to deduce a mathematical connection among these public keys. The holder of such keys can prove it is a legitimate member of the group (i.e., member of the trust network).

We outline such an anonymous-verifiable scheme for blockchain systems in Hardjono and Pentland (2016). There are several variants of anonymous-verifiable cryptographic identity schemes that can be used [see, e.g., Brickell and Li (2012), Camenisch and Lysyanskaya (2002) and Camenisch and Van Herreweghen (2002)], but a discussion of this topic is outside the scope of this work.

10. Conclusions

In order for the emerging virtual asset industry to develop and evolve services that are globally accessible, VASPs need to work collaboratively to create the next-generation infrastructures that are not only compliant to the existing FATF regulatory framework but also provide innovative solutions to customers globally.

VASPs need to develop a trust network following the principles of the Internet architecture, allowing the exchange of customer certificates and attributes that provide transparency into the movement of virtual assets. The use of existing standards for public-key certificates provides a starting

point for this trust network. These standards can be extended to incorporate features that are specific to virtual assets and to customers of the service providers. The overall goal is to enable originators and beneficiaries around the world to exchange virtual assets in user-friendly and seamless manner, compliant to regulations pertaining to combating money laundering and the financing of terrorism and proliferation of weapons of mass destruction.

As part of developing the next-generation infrastructure, the virtual asset industry should invest in research and development in several areas of innovation. These areas of innovation include the development of the operating rules of the VASP trust network, information sharing within the trust network and across trust networks, and development of new cryptographic schemes that solve the need of customer anonymity while complying to the requirements of the Travel Rule.

References

Androulaki, E., A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick, 2018, Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains, in *Proceedings of the Thirteenth EuroSys Conference*, ACM, New York, NY, USA, pp. 30:1–30:15.

Apple Inc., 2019a, Apple Public CA Certification Practice Statement, Certificate Practices Statement, June, available at: https://images.apple.com/certificateauthority/pdf/Apple_Public_CA_CPS_v4.2.pdf.

Apple Inc., 2019b, Apple PKI, Root Certificates, June, available at: https://www.apple.com/certificateauthority/.

Atkins, D., W. Stallings, and P. Zimmermann, 1996, PGP Message Exchange Formats, IETF Standard RFC1991, August, available at: http://tools.ietf.org/rfc/rfc1991.txt.

Barker, E., 2016, Recommendation for Key Management (Part 1: General), NIST Special Publication 800-57, Part 1, Revision 4, National Institute of Standards and Technology, Gaithersburg, MD.

Barker, E., M. Smid, and D. Branstad, 2015, A Profile for U.S. Federal Cryptographic Key Management Systems, NIST Special Publication 800-152, National Institute of Standards and Technology, Gaithersburg, MD.

Brickell, E., and J. Li, 2012, Enhanced Privacy ID: A Direct Anonymous Attestation Scheme with Enhanced Revocation Capabilities, *IEEE Transactions on Dependable and Secure Computing*, 9(3), 345–360.

Buterin, V., 2014, Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform, *Bitcoin Magazine*, January, available at: https://bitcoinmagazine.com/articles/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211/.

CableLabs, 2019, CableLabs New PKI Certificate Policy: Version 2.1, Technical Specifications, January, available at: https://www.cablelabs.com/resources/digital-certificate-issuance-service.

Camenisch, J., and A. Lysyanskaya, 2002, A Signature Scheme with Efficient Protocols, in S. Cimato, G. Persiano and C. Galdi (editors), *Security in Communication Networks (SCN2002)*, Lecture Notes in Computer Science, Vol. 2576, Springer, Berlin, 2002, pp. 268–289.

Camenisch, J., and E. Van Herreweghen, 2002, Design and Implementation of the Idemix Anonymous Credential System, in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, ACM, New York, pp. 21–30.

Chavez-Dreyfuss, G., 2018, Cryptocurrency Theft Hits Nearly $1 Billion in First Nine Months, *Reuters Business News*, October 10, available at: https://www.reuters.com/article/us-crypto-currency-crime/cryptocurrency-theft-hits-nearly-1-billion-in-first-nine-months-report-idUSKCN1MK1J2.

Chokhani, S., W. Ford, R. Sabett, C. Merrill, and S. Wu, 2003, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, IETF Standard RFC3647, November, available at: http://tools.ietf.org/rfc/rfc3647.txt.

Committee on National Security Systems (CNSS), 2009, Instructions for National Security Systems Public Key Infrastructure X.509 Certificate Policy: Under CNSS Policy No. 25, CNSS Instruction No. 1300, October, available at: https://www.hsdl.org.

Cooper, D., S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, 2008, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, IETF Standard RFC5280, May, available at: http://tools.ietf.org/rfc/rfc5280.txt.

FATF, 2018, International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, FATF Revision of Recommendation, 15 October, FATF Secretariat, Paris, France, available at: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html.

Financial Action Task Force (FATF), 2019a, Who We Are, available at: http://www.fatf-gafi.org.

Farrell, S. and R. Housley, 2002, An Internet Attribute Certificate Profile for Authorization, IETF Standard RFC3281, April, available at: http://tools.ietf.org/rfc/rfc3281.txt.

FATF, 2019b, Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers, FATF Guidance, June, FATF Secretariat, Paris, France, available at: www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-RBA-virtual-assets.html.

Finextra, 2004, Swift to introduce PKI security for FIN, *Finextra News*, October, available at: https://www.finextra.com/newsarticle/12620/swift-to-introduce-pki-security-for-fin.

Gemalto, Inc., 2008, LINQUS USIM 128K Smartcard — ESIGN PKI Signature Application, Product Specifications, available at: https://www.commoncriteriaportal.org/files/epfiles/cible2008_37en.pdf.

Gray, J., and L. Lamport, 2006, Consensus on Transaction Commit, *ACM Transactions on Database Systems*, 31(1), 133–160.

Gutmann, P., 2006, Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP, IETF Standard RFC4387, February, available at: http://tools.ietf.org/rfc/rfc4387.txt.

Hardjono, T., 2008, Strengthening Enterprise Applications Using Trusted Platform Modules, *Network Security*, 2008(6), 15–18.

Hardjono, T., A. Lipton, and A. Pentland, 2019, Towards an Interoperability Architecture Blockchain Autonomous Systems, *IEEE Transactions on Engineering Management*, doi: 10.1109/TEM.2019.2920154.

Hardjono, T., and A. Pentland, 2016, Verifiable Anonymous Identities and Access Control in Permissioned Blockchains, Technical Report, MIT Connection Science & Engineering, April, available at: https://arxiv.org/abs/1903.04584.

Housley, R., W. Ford, W. Polk, and D. Solo, 1999, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, IETF Standard RFC2459, January, available at: http://tools.ietf.org/rfc/rfc2459.txt.

Housley, R., and T. Polk, 2001, *Planning for PKI: Best Practices for PKI Deployment*, John Wiley & Sons, New York.

ISO, 2017, ISO/IEC 9594-8:2017: Information Technology — Open Systems Interconnection — The Directory — Part 8: Public-Key and Attribute Certificate Frameworks, Standard, February, International Organization for Standardization, Geneva, Switzerland.

Kuhn, D. R., V. C. Hu, W. T. Polk, and S.-J. Chang, 2001, Introduction to Public Key Technology and the Federal PKI Infrastructure, NIST Special Publication 800-32, February, National Institute of Standards and Technology, available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf.

Lipton, A., T. Hardjono, and A. Pentland, 2018, Digital Trade Coin (DTC): Towards a More Stable Digital Currency, *Journal of the Royal Society Open Science*, 5(7), 180155.

Makaay, E., T. Smedinghoff, and D. Thibeau, 2017, OpenID Exchange: Trust Frameworks for Identity Systems, June, available at: http://www.openidentityexchange.org.

Microsoft, 2017, TPM Key Attestation, Microsoft IT Pro Center Report, May, available at: https://docs.microsoft.com/en-us/windows-server/identity/adds/manage/component-updates/tpm-key-attestation.

Microsoft, 2018, Microsoft X.509 Public Key Certificates, May, available at: https://docs.microsoft.com/en-us/windows/win32/seccertenroll/about-x-509-public-key-certificates.

Myers, M., R. Ankney, A. Malpani, S. Galperin, and C. Adams, 1999, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol — OCSP, IETF Standard RFC2560, June, available at: http://tools.ietf.org/rfc/rfc2560.txt.

Nakamoto, S., 2008, Bitcoin: A Peer-to-Peer Electronic Cash System, available at https://bitcoin.org/bitcoin.pdf.

National Automated Clearing House Association (NACHA), 2019, Operating Rules and Guidelines, Specification, available at: https://www.nacha.org.

OASIS, 2005, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, March, available at: http://docs.oasisopen.org/security/saml/v2.0/saml-core-2.0-os.pdf.

Peyton, A., 2018, Singapore Regulator Gives Customer Onboarding Guidance, *Fintech Futures*, 8 February, available at: https://www.fintechfutures.com/2018/02/singapore-regulator-gives-customer-onboarding-guidance/.

Rivest, R., A. Shamir, and L. Adleman, 1978, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Communication of the ACM*, 21(2), 120–126.

Sakimura, N., J. Bradley, M. Jones, B. de Medeiros, and C. Mortimore, 2014, OpenID Connect Core 1.0, Technical Specification v1.0 — Errata Set 1, November, OpenID Foundation, available at: http://openid.net/specs/openid-connect-core-1_0.html.

Santesson, S., M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, 2013, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol OCSP, IETF Standard RFC6960, June, available at: http://tools.ietf.org/rfc/rfc6960.txt.

Sporny, M., D. Longley, and D. Chadwick, 2019, Verifiable Credentials Data Model 1.0, W3C Candidate Recommendation, March, W3C, available at: https://www.w3.org/TR/verifiable-claims-data-model.

SWIFT, 2017, SWIFT Qualified Certificates for Electronic Seals, Certification Practice Statement, October, available at: https://www.swift.com/pkir-epository.

Symantec, 2013, Symantec Shared Service Provider Certification Practice Statement, Certificate Practices Statement Version 1.14, April, available at: https://www.symantec.com/content/en/us/about/media/repository/ssp-cps.pdf.

Trustis, 2017, Open Banking Certificate Policy, Version 1.0 (T-0328-001-GH-001), available at: http://ob.trustis.com/production/policies/.

Visa, 2013, Visa International Operating Regulations, Specification, October, available at: https://usa.visa.com/dam/VCOM/download/merchants/visa-international-operating-regulations-main.pdf.

United States Congress, 2000, Electronic Signatures in Global and National Commerce Act (ESIGN), Public Law 106–229, available at: http://govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf.