The role of Identity in Digital and Virtual Currency Systems

An Insight Paper by SPA

January 2018

1. Abstract

Offering a great opportunity for financial innovation, virtual currencies represent a 'natural fit' with e- and m-commerce transactions - and indeed, could be viewed as 'Internet cash' or e-money. However, because such currencies allow for anonymous transactions, this has attracted the attention of criminal groups as a mechanism to facilitate money laundering.

The current EC initiative to amend Article 65 of the Fourth Anti Money Laundering (AML) Directive could be regarded as a first attempt to regulate the use of virtual currencies in the European Economic Area.

The SPA recognizes the need for legislation to prevent the misuse of virtual currencies. But legislation, it believes, is not the only approach. Debate should also focus on exploring the technology models that could be utilized to address the known security vulnerabilities posed by digital currency or e-money.

This paper examines the potential use cases for digital/virtual money and discusses the digital identity and management frameworks that will be required to address how virtual currencies are issued, processed and redeemed.

Clearly, for alternative payment options such as digital money and/or virtual currencies to become mainstream, then compliance with regulatory frameworks that require payment traceability will need to be achieved.

Note: Throughout this paper, the term 'digital currency' refers to a digital payment mechanism denominated in a fiat currency – e-money. Virtual currencies, on the other hand, are not denominated in fiat currency and have their own unit of account (digital units). Virtual currency is also equivalent to 'cryptocurrency' which relies on the cryptographic mechanisms used to generate and process currency units to engender trust.

2. Anonymity, Privacy, Use Cases and Regulation

The proposed amendment to the AML Directive recognizes that the monitoring of virtual currencies should be based on a "balanced and proportional approach" that safeguards technical advances. It also makes it clear that to combat the risks associated with anonymity, national Financial Intelligence

Units (FUIs) should be able to associate virtual currency addresses to the identity of the owner of virtual currencies.

The amendment also establishes a limited exemption regime, stating that currencies used in limited networks – such as a city, region or among a small number of users – should not be considered as virtual currencies.

While the future legal framework clearly discourages the use of anonymous virtual currencies for evident security reasons, the incentives to use this type of money are examined in the following three use cases.

2.1. Anonymity in cooperative schemes

Peer-to-peer payments are a use case for anonymous virtual currency transfers using a 'private cooperative' blockchain in a collaborative economy. In these scenarios, an anonymous virtual currency would preserve the privacy of the participants in such a scheme.

As discussed, the amendments to the Fourth AML Directive acknowledges that this type of scenario does not correspond to the kind of 'virtual currency' in the spotlight and proposes using the term 'local' or 'complementary' currency to differentiate from "real" virtual money that has global reach and is associated with the risk of money laundering or terrorist financing.

2.2. E-commerce

Virtual currency transactions do not require the disclosure of personal or sensitive data. Unlike other electronic payment methods, the possession of virtual currency units equals ownership and this intrinsic feature removes the risk of identity theft. But, in an e-commerce context, if the currency used to pay is anonymous then this creates challenges for retailers and customers:

- The identity of the customer is needed for the delivery of physical goods (versus digital content), as well as billing and customer management.
- Customer-initiated chargebacks would represent a serious concern for merchants.
- Consumers need to be assured that an online merchant is real, that they will receive a purchase receipt and that a dispute mechanism exists – which would be challenging in a service-centric system where identities can be anonymized.
- Customers may not be able to prove payment – and consequently would be unable to recover from financial loss.

2.3. Cross-border remittances

In these scenarios, the level of anonymity could be fine-tuned in relation to whether the beneficiary lives in a financial crime 'high risk' country and adapted to the evolving nature of money laundering

or terrorism financing threats. Virtual currencies could also be designed to mitigate the risk of misuse. For example, they could be assigned an expiry date and/or metadata describing the purpose (payment for food, medicine, bill payment) of the remittance, with both being cryptographically protected. This would address use case requirements of financial inclusion, or an EU donor making an anonymous transfer for humanitarian reasons.

3. The Sources of Trust on Digital Currencies

Anonymous, partially anonymous or nominal virtual currencies are assets whose value relies on trust, but the source of trust will differ:

- The currency issuer must be trustable and operate under a recognized prudential regime. Trust in the digital currency will rely on the identity of issue – identity that cannot be forged because it is established using strong, proven cryptography.
- Technical mechanisms must be in place to prevent 'double spending' of a unit of digital currency; the issuer will need to maintain a database of all spent e-money and efficient ways of managing the accumulated metadata of every person who has 'spent' the currency needs to be in place – one option would be to use a smart card with a tamper-proof chip to maintain the transaction log of all e-money spent and prevent the same unit being spent twice.
- Virtual currencies need to be designed using cutting-edge security-proven cryptographic mechanisms that minimize payment friction for retailers/consumers but prevent the risk of 'double spend'.
- The intrinsic security offered by the digital currency (unforgettability) should minimize the risk of issuer insolvency as a result of fraud. Regulatory regimes would therefore require the issuance of a more secure form of digital currency (more auditable, with transactions submitted to secure cryptographic protocols).
- From a digital identity perspective, different formats of digital currencies may coexist, provided that the security of digital units is guaranteed. The European Banking Authority notes that users could hold virtual currency accounts on their own devices or entrust these to a wallet provider who may also have custody of the user's public and private key. Wallets could be stored online ('hot storage') or offline ('cold storage'), with cold storage increasing the safety of the balance on the wallet.

Such security counter measures may enable a level of anonymity that is acceptable to regulatory bodies, and the concepts of hot and cold storage are implementation aspects that are worthy of further exploration.

4. Identity Management and Digital Currency Schemes

To start the discussion on the relationships between digital currencies and identity/identities, we propose the following six high-level objectives for any digital currency scheme:

1. Money in the Net is linked to the issues of secure identity and trust in payment systems. It is vital to understand the nature of identities involved – in other words, the digital identity of the digital

currency at issuance, of the digital currency issuer, the purchaser of a digital currency, the currency acceptor and finally, of the entity that redeems digital currency units.

2. Secure transactions must prevent attempts to steal identities for criminal purposes as a fundamental objective.
3. For transaction security, the authentication of identity and of digital units of currency is a primary requirement.
4. The transition to universal digital money requires the transition to universal digital identity management and systems that people trust to guarantee privacy.
5. The link between users' digital identities and digital currencies could be assured by implementing a mobile wallet.
6. If mobile is the universal future device for payments, the security properties of mobile devices eligible for the download, storage and transfer of digital currencies should be standardized – ISO 12812 sets out guidance on these security requirements.

Clearly, the identifying information requirements will be dependent on the way digital currency is issued, downloaded, stored and transferred.

1. In purely online systems, digital currency will be stored exclusively in payment accounts held by entity members of the scheme – in these 'one-shot' scenarios, digital units must be immediately deposited and are not transferable. Payments are perfectly traceable and a checking each payment against a database of spent units prevents 'double spending' of currency units.
2. For offline payments, digital currency units will need to be transferable and the lack of real-time transaction monitoring will be balanced by metadata ID information. However, the amount of metadata will increase with every payment made as the identities of all users of the same unit are added to the chain. In addition to establishing a limit on the number of transfers possible, this raises the issue of the intrinsic value of a digital unit during its lifecycle as the unit of digital currency devalues when approaching its maximum number of transfers.
3. For offline payments, digital money units must be stored in a tamper-resistant device and should only be transferable to a payee's tamper-resistant device. The payment can also credit a payee payment account.
4. While none of the above points apply to virtual currencies that are settled using blockchain technology, the economic impact of the huge amount of processing power that is wasted by miners when validating a bitcoin transfer will need to be resolved.

The SPA proposes the following guiding principles should be considered to ensure the mapping of all the various identities that relate to digital currencies from the point at which a digital unit is issued.

1. At issuance, each digital currency unit has a unique representation as a set of bound attributes that, together, constitutes a liability on the digital currency issuer.
2. This unique representation is the original digital identity of the unit of digital currency and should be protected using well-proven cryptographic methods that ensure strong data authentication. No other entity, other than the issuer, can build the identity of a unit of digital currency.
3. The identity of the withdrawal user of the digital currency scheme may be one of the attributes of the digital currency unit.

4. The digital ID of the currency unit is protected in a way that enables a third party to verify authenticity, without impacting the integrity of the unit's digital ID.
5. If the transfer protocol for a unit of digital currency requires the inclusion of data representing the ID of the acceptor, the digital ID of the unit and the acceptor are bound using secure cryptographic mechanisms. This requirement may be of a legal nature.
6. The metadata generated by identifiable entities/individuals during the lifecycle of the digital currency unit for the purposes of payment monitoring adds to the issuance digital ID of the unit.
7. When presented for redemption, the digital ID of the unit of digital currency is the digital ID at issuance, plus the metadata incorporated during transactions. This principle does not apply to virtual currencies, whose possession does not represent a liability against an issuer.
8. Digital currencies are transferred using different protocols. The execution of the protocol does not represent a liability against an issuer.
9. Prior to acceptance, the verification (authentication) of the digital currency can be undertaken by the payee of its agent, regardless of the identity of the payer. This verification operation shall not impact the nature of the digital currency that is being transferred.

5. Conclusion

Without trust, virtual currencies will never fulfil their potential, but to optimize the fight against money laundering without blocking financial innovation, regulation should focus on mitigating the security risks that are intrinsic to virtual currencies, taking account of different anonymity scenarios.

As we've seen, some use cases validate the need for privacy-supportive virtual currency exchanges and in these scenarios, technology should enable flexibility in terms of linking identity credentials and virtual currency units to be transferred. Digital wallets, implemented using certified hardware card technology – 'cryptocurrency cards' – is an appropriate technology to resolve the various trade-offs required.

Longer term, a standard protocol would facilitate global reach and high transaction volumes and ISO TC68 is currently investigating the production of such a standard, starting with the specification of the security properties digital currencies (FIAT) should feature. However, the legal requirement to identify the participants in an electronic payment and the individuals/organizations that purchase units of virtual currency means the financial industry and governments will need to collaborate to develop global ID management systems that use certified legal names.