Tokenising Digital Identity

Exploring the Promise of a Blockchain-based KYC Solution

by

Scott Chamberlain and Richard Holland

21 June 2021

1. Identity on a Blockchain

1.1 One problem people are attempting to solve with blockchain technology is digital identity. There are many approaches, including webs of trust[1] and decentralised identity/identifiers.[2]

1.2 However, we want to look specifically at the problem of Know Your Customer ("KYC") because it is a growing problem for cryptocurrency ecosystems, and it is identified as an area of interest in Australia's National Blockchain Roadmap[3].

2. KYC: Challenge and Opportunity

2.1 Anti-money laundering and associated KYC laws ("AML/KYC laws") require businesses involved in moving or handling money or money-like value to ensure they know their customers and to implement risk management strategies to prevent facilitating money laundering or terrorism. These laws apply to cryptocurrencies because they allow people to move money-like value.

2.2 Cryptocurrency Exchanges have KYC obligations in most jurisdictions, including Australia.[4] Recently, The Financial Actions Taskforce ("FATF") recommended extending KYC obligations beyond Exchanges to all Virtual Asset Service Providers ("VASPs"), with VASP being defined broadly to include almost anyone conducting a business with cryptocurrencies.[5] Further, FATF recommended that a VASP's KYC obligations should include knowing who controls the blockchain addresses/accounts its clients use to source or remit cryptocurrencies.[6]

2.3 These recommendations are in response to concerns about how easily cryptocurrencies facilitate money transfers outside traditional payment rails. FATF even contemplates regulating purely peer-to-peer transactions, a recognition that the traditional strategy of deputising financial institutions to do the governments' policing work may be ineffective with cryptocurrencies.[7] So, all cryptocurrency ecosystems will likely need a KYC solution to operate lawfully.

[1] See, eg, 'The Future of Digital Identity' *Data Zoo* (Web Page, 3 June 2020) <https://www.datazoo.com/the-future-of-digital-identity/>.

[2] See, eg, '(DID) The Decentralized Identifier' *Decentralized Identity*, (Web Page, 2 December 2020) <https://decentralized-id.com/web-standards/w3c/wg/did/decentralized-identifier/>

[3] Department of Industry, Science, Energy and Resources (Cth), *The National Blockchain Roadmap: Progressing Towards a Blockchain-Empowered Future* (2020) 43

[4] *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) pt 6A

[5] Financial Action Task Force, *Updated Guidance for Risk-Based Approach to Virtual Assets and VASPs* (Draft, 2021)

[6] Ibid 18

[7] Ibid 37

2.4 Fortunately, any viable KYC solution is likely to have broader benefits as a useful digital identity management platform. Quick, cheap, convenient ways to know with whom you are dealing – or just to know you are dealing with a real person – are likely to be very useful in many contexts as life and commerce become increasingly digitized. The Australian Government has recognised this. In its National Blockchain Roadmap it identified digital identity and KYC as a challenge and an opportunity for blockchain.[8]

3. Tokenising Digital identity Is Not Easy

3.1 Digital identity is not an easy problem to solve, even with blockchain technology, especially in the case of KYC, for several reasons.

(a) **You Don't Own an Identity:** While self-sovereign identity advocates insist you should "own" your identity, identity is not something you can own. It is something you claim, and the other party chooses to accept it, potentially only after a trusted third party has verified your claim, depending on the importance of you being "you" in the context of the transaction.

(b) **Identity is a Joint Venture:** Identity resembles a joint venture. The joint efforts of claimants, verifiers, and accepters generate the shared outcome of an identity claim that people are both willing and allowed to trust in the context of their relationship or transaction. This is reflected in the Public Key Infrastructure (PKI) approach applied for managing SSL certificates for websites where an ecosystem of participants is needed to provide trust in the certified identity.

(c) **Blockchain Alone Doesn't Solve This Problem:** The joint venture nature of digital identity means it is not an easy problem to solve with blockchain technology.

(i) Blockchain Works Best with Native Assets: Blockchains work for assets like BTC, XRP and ETH. Those assets are native to their blockchain, making them virtually impossible to forge or double spend.

(ii) Identity Is Not a Native Asset: People are not native to any blockchain. While there is an unbroken chain of events from your birth to the present that would conclusively prove only you can be the person you claim to be, that chain is not generated or recorded on any blockchain.

(iii) Identity Must Be Tokenised: Your identity must be "put onto" a blockchain. This generally means creating a token on a blockchain that represents or points to an identity verified by a trusted third party. Done well, it captures (tokenises) the work involved in verifying your identity, potentially turning the one-off cost and effort into a persistent asset.

(iv) Tokenising Identity Requires Trusted Third Parties: While the token might be protected against forgery and double spending, (because of the mechanics of blockchains) the link between that token and your physical self is not. The claimed link is only as trustworthy as the trusted third party. But "trusted third parties are

[8] Department of Industry, Science, Energy and Resources, (Cth) *The National Blockchain Roadmap: Progressing Towards a Blockchain-Empowered Future* (2020) 43-45

security holes and lawyer magnets",[9] and inherently centralising.

(d) **KYC Has Legislated Standards:** AML/KYC laws create specific obligations on reporting entities when confirming the identity of the people with whom they do business. Any digital identity solution that tokenises KYC efforts must do so in a way that meets the KYC obligations of the reporting entities. A decentralised identity/identifier solution that doesn't meet KYC obligations is no solution to the problem of KYC in cryptocurrencies.

4. Design Principles

4.1 Given the above challenges, we want our solution to meet the following design principles:

(a) **AML/KYC Compliant**: Certified identities must meet AML/KYC laws in a way that makes them useful to regulated financial institutions and digital asset exchanges.

(b) **Self-sovereign**: Unlike the traditional KYC process, users should control the initiation, use, and cancellation of their certified identity.

(c) **Secure**: The solution should not be open to attack or fraud.

(d) **Decentralised:** Anyone should be able to use it and there should be no single point of failure.

(e) **GDPR Compliant**: The solution should meet or be capable of meeting the GDPR as the highwater mark of global privacy requirements.

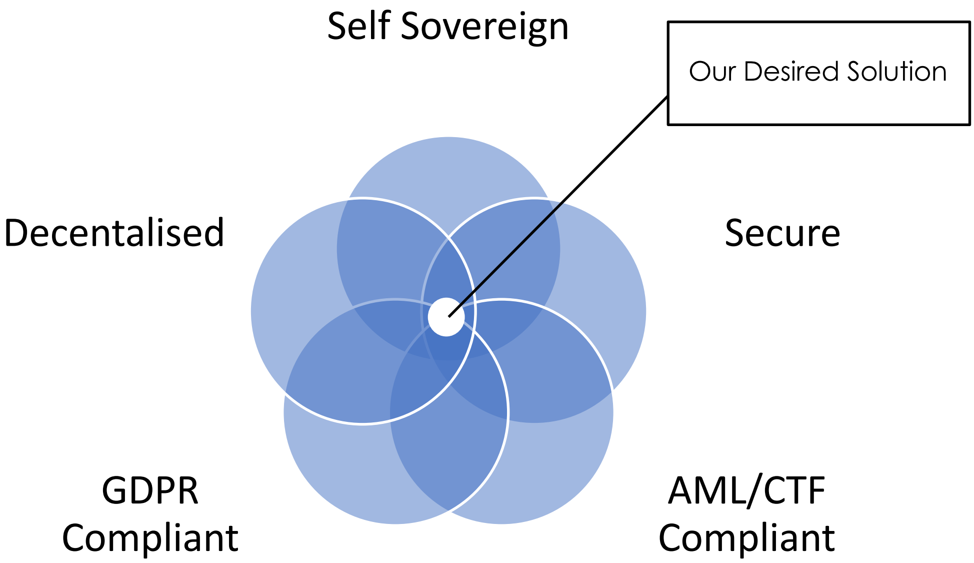

Figure 1 – Self-KYC Design Principles

4.2 Each of these principles are examined below.

[9] Nick Szabo, 'Trusted Third Parties are Security Holes' *Satoshi Nakamoto Institute* (Web Page, 2001) <https://nakamotoinstitute.org/trusted-third-parties/>

Design Principle 1 - AML/CTF Compliance

4.3 Any identity solution needs to result in identities people can trust. In the case of KYC, there are legislated requirements. A solution that is trusted but does not meet these requirements is not a solution for KYC purposes.

4.4 In Australia, the AML/KYC obligations of financial institutions and digital currency exchanges are governed by the *Anti-Money Laundering/Counter-Terrorism Financing Act 2006* (Cth) ("AML/CTF Act") and the associated *Anti-Money Laundering/Counter-Terrorism Financing Rules 2006* (Cth) ("AML/CTF Rules").

4.5 Under the AML/CTF Act and AML/CTF Rules, financial institutions and digital currency exchanges must take appropriate steps to ensure they know the identity of the people with whom they deal and to ensure their services are not used to finance terrorism or launder money.

4.6 While the AML/CTF Act and the AML/CTF Rules work on a risk assessment and minimization regime, there are safe harbour provisions that specify steps entities can take to ensure compliance. In relation to electronic confirmation of identity of new customers who are considered "medium/low risk individuals" under the ALM/CTF Rules, the safe harbour provisions deem an entity compliant if it can confirm the client's name and date of birth and/or residential address from two reliable and independent electronic sources.[10]

4.7 The AML/CTF Act and AML/CTF Rules do not define "reliable and independent" electronic data sources. Industry practice is to rely upon third-party identity verification services which, in turn, confirm each customer's identity against a series of government databases. Access to these databases is via a formal, licensed regime overseen by the Australian government.[11] It follows that any self-KYC solution using electronic identity documents should also use licensed third-party identity verification services to confirm the validity of the presented electronic records against the Australian government's data bases.

4.8 In our opinion, this rules out "web of trust" and "decentralised identifier" models. It is insufficient for the reporting entity to believe, from a risk management perspective, that it knows its customer. It needs objectively to meet the safe harbour provisions, and this will almost certainly mean using licensed identity verifiers who run cross-checks against government databases.

Design Principle 2: Self-Sovereignty

4.9 Axiomatically, a self-KYC solution must also be self-sovereign. Self-sovereignty is the concept that Users should own or retain control of their identity, not those with whom they share it.

4.10 Blockchain and Distributed Ledger Technology make self-sovereign identity possible. The increasing concern over data privacy makes it a priority for Users, while the increasing cost and liability for privacy breaches makes it attractive to businesses. It is not credible today to launch an identity solution unless the User controls their identity credentials.

4.11 To meet this principle our solution must ensure the User always remains in control of both their identity information and the fact it has been verified. The User must control their identity's creation, verification, utilisation, and deletion.

[10] *Anti-Money Laundering/Counter-Terrorism Financing Rules 2006* (Cth) paras 4.1.12-4.2.14
[11] See generally *Digital Identity* (Web Page) <https://www.digitalidentity.gov.au/>

Design Principle 3: Security

4.12 Any digital identity solution must be secure in terms of both the use and storage of private information. We plan on using a blockchain-based technology, which we believe is more secure than traditional client/server solutions.

4.13 We consider the solution meets this design criteria if it employs end-to-end encryption of all private data so that no one – not even the owners of the Nodes on which the solution runs - can access the data without the User's express consent.

Design Principle 4: Decentralisation

4.14 We want a solution that is not owned or controlled by a single entity or that has a single point of failure. We consider this principle necessarily arises from trying to use blockchain technology to solve the problem. We consider our solution meets this design principle if:

(a) Anyone can decide to use it.

(a) It runs on multiple Nodes.

(b) Anyone can run a Node.

4.15 We expect this principle will be difficult to meet. There is a very finite universe of decentralised systems that are also capable of meeting Design Principle 1 because the law forces elements of centralisation – trusted third party verifiers - into the solution.

Design Principle 5: GDPR Compliance

4.16 Any identity solution will necessarily involve handling people's private information (in the form of their identity documentation), including biometric data (in the form of photo ID and facial recognition). It is generally accepted that the high watermark in terms of global privacy requirements is the European Union's General Data Protection Regulation ("GDPR").[12] Therefore, our solution should be compliant with the GDPR to stand a chance of general adoption.

4.17 The GDPR is generally regarded as difficult to reconcile with blockchain technology. The globally distributed, tamper-proof, and permissionless nature of public blockchains makes it difficult to enforce both:

(a) the User's rights, including the rights to give and revoke express consent for the collection, processing, correction, and deletion of their private data; and

(b) the protocol's legal obligations as to governance and design requirements surrounding data minimisation, privacy by design and default, binding agreements between controllers and processors, and compliant cross-border information transfers.[13]

[12] *Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (Data Protection Directive)* [2016] OJ L 119/1

[13] Scientific Foresight Unit (STOA), European Parliamentary Research Service 'Blockchain and the General Data Protection Regulation. Can Distributed Ledgers Be Squared with European Data Protection Law?' (PE 634.445 – July 2019)

4.18 However, Faber et al (2019) have suggested that blockchain technology could enhance privacy protection where a user centric design model employs blockchain technology to store pointers to off-chain data, and where users control access to these using private keys only they possess.[14] Our HotPocket technology is suitable for developing a similar system, but with the difference that encrypted personal identity data is held on chain (on servers/nodes that no single entity controls) rather than off-chain.

5. Why A DPKI Model is Preferred for Self-KYC

5.1 Given the challenges of tokenising identity, and the inherent tension in our five principles, we think a Decentralised Public Key Infrastructure (DPKI) model offers the best potential for a solution.

5.2 PKI or public key infrastructure is the model for managing SSL certificates for websites. It has the following elements:[15]

(a) **Certificate Authority**: entity that stores, issues, and signs the digital certificates.

(b) **Registration Authority**: entity that verifies the identity of the entities requesting their digital certificates to be stored at the certificate authority.

(c) **Central Directory:** a secure location in which to store and index keys.

(d) **Certificate Management System**: to manage things like the access to stored certificates or the delivery of the certificates to be issued.

(e) **Certificate Policy:** stating the PKI's requirements concerning its procedures so outsiders can analyse the PKI's trustworthiness.

5.3 Our proposed DPKI model would implement a variation of this structure, as summarised in Table 1, replacing various centralised elements with blockchains, smart contracts, and non-fungible digital assets as follows:

(a) **Smart Contract as Certificate Authority:** The Certification Authority functions would be replaced by a smart contract issuing non-fungible ID tokens on a public blockchain.

(b) **Registration Authorities Retained:** The smart contract would send their application a to Registration Authority (RA) to verify the identity claims. If all claims are verified, the smart contract would issue the ID Token to the User's blockchain address.

(c) **Self-Sovereign Key Registry:** Users would control the private keys to their accounts and identity documentation on their phones.

(d) **Self-Sovereign Certificate Management System:** the certificate management system would be replaced by a smart contract that allows Users to grant third parties access to the identity documents through single use keys issued solely at the User's discretion.

(e) **Open-source Code as Certificate Policy:** A GitHub or similar repository would store the open-source code of the smart contract and App

[14] Benedict Faber et al, 'BPDIMS: Blockchain-Based Personal Data and Identity Management System' (Proceedings of the 52nd Hawaii International Conference on Systems Science, 2019) 6859-6860

[15] Wikipedia, *Public Key Infrastructure* (Web Page) <https://en.wikipedia.org/wiki/Public_key_infrastructure>

allowing anyone to review the quality of the code and analyse the DPKI's trustworthiness.

Design Element	Traditional PKI Features	Proposed DPKI Features
Certification	Certification Authority	Smart Contract
Verification	Registration Authority	Registration Authority
Key Directory	Centralised storage	User's Phones
Rules	Management system	Smart Contract
Transparency	Published policies	Open-source code

Table 1-PKI vs DPKI Design Elements

5.4 This model appears to ameliorate the problems associated with the centralised PKI model while retaining a role for registration authorities, which is essential for trust and KYC compliance. We think it has a reasonable chance of delivering a system that meets our design principles.

6. Choice of Blockchain and Smart Contract Technology

6.1 Our DPKI solution requires a blockchain and a smart contract platform. We chose the XRP Ledger and HotPocket, our recently developed layer 2 smart contract solution.

XRP Ledger

6.2 The XRP Ledger is a public blockchain that uses a consensus protocol to prevent double spending. In our opinion, the features that make the XRP Ledger ideal for self-KYC include:[16]

(a) **Fast and Cheap:** This protocol is fast and cheap. It takes ~3 seconds and costs factions of a penny to process a transaction.

(b) **Permissionless:** Anybody can use the XRP Ledger, and nobody controls access to it.

(c) **Reliable:** Since launch, the XRP Ledger has successfully closed over 64 million ledgers.

(d) **Secure:** Secure: In addition to standard public blockchain features, the XRP Ledger offers native multi-signing and ED25519 support.

(e) **Tokenisation:** The XRP Ledger natively supports non-XRP tokens, which can be used to create account-bound non-fungible Identity Tokens.

HotPocket Consensus Engine

6.3 HotPocket is a UNL (unique node list) consensus engine that converts any number of Linux machines into a mini-blockchain capable of cheaply and

[16] These stats taken from 'Your Questions About XRP, Answered', *XRP Overview* (Web Page) <https://xrpl.org/overview.html>

speedily running any dApp in any language at almost any scale on almost any blockchain, including the XRP Ledger.

6.4 HotPocket dApps don't run on blockchains, they are blockchains. Each dApp is its own blockchain with its own chain history and dedicated nodes, making them incredibly flexible.

6.5 DApps may be public or private. DApps may call external services, read and write data directly to disk and the web, and generally perform any task a regular program can, without centralisation or trusted third parties and without requiring the programmer to implement their own consensus mechanisms.

6.6 This flexibility has many benefits that makes HotPocket ideal for a tokenised digital identity solution using a DPKI, including:

(a) **Privacy Compliance:** dApps can encrypt data, run only on hosts in a specified jurisdiction, or only on hosts that have agreed to meet privacy regulations.

(a) **Scale & Flexibility:** dApps can run on as few or as many hosts as the dApp developer desires from a cost and security perspective.

(b) **On-Demand Oracles:** HotPocket dApps can elect a sub-set or jury of their own nodes to get data from off-chain, agree on the truth, and report to the rest of the chain as a bespoke, on-demand oracle.

(c) **Enhanced Security:** dApps can detect when a host has become compromised or untrustworthy, shut down that instance of the dApp, and reload it on another, more trusted Node.

6.7 With the XRP Ledger and HotPocket we can build a DPKI solution that meets our design principles and is fast, cheap, and convenient to use.

7. Next Steps

7.1 Nick Szabo, the father of smart contracts[17], maintains that blockchain identity is a graveyard of failed projects because the problem and the technology are relatively incompatible.

> *Identity is local, insecure, and labour-intensive. Blockchains are global, secure, automated.* [18]

7.2 Our ambition is to build a form of digital identity that can scale, that takes what is local, insecure, and labour-intensive and "tokenises" it so that it can be global, secure, and automated.

7.3 To this end, our most immediate next step is to build a working proof concept.

[17] Nick Szabo, 'Formalizing and Securing Relationships on Public Networks' *Satoshi Nakamoto Institute* (Web Page, 1997) <https://nakamotoinstitute.org/formalizing-securing-relationships/>

[18] @NickSzabo4, (Twitter, 18 June 2017, 11:01am) <https://twitter.com/NickSzabo4/status/876243371534057472>