A Blockchain Supported Solution for Compliant Digital Security Offerings

Andrew Le Gear

Abstract Ethereum launched in 2015 ushering a sea change over its predecessors in it's ability to tokenise an asset. This was a technical innovation and an *Initial Coin Offering* (ICO) boom ensued, peaking in 2017. The legal and compliance requirements of tokenisation failed to keep step in these early stages, but were eventually brought to bear after the ICO bubble burst, forcing technological liberalism to confront regulatory realities. The *Digital Security Offering* (DSO)—a name change intended to reflect full compliance—was coined. However, truly executing a fully compliant DSO remained elusive for many. In this chapter we navigate the regulatory landscape for DSOs and construct a compliant blockchain solution, using it to support the DSO capital raise for a product named *Talketh* in December of 2018. The journey discusses the key compliance concerns of *Know-Your-Customer* (KYC), *Anti-Money-Laundering* (AML), Custody, Tokenisation and onward secondary trading as part of a *Distributed Exchange* (DEX).

Keywords Blockchain · Initial public offering · IPO · Security token offering · STO · Digital security offering · DSO · Initial coin offering · ICO · Custody · Primary issuance · Secondary trading · Distributed exchange · DEX · Compliance

1 Introduction

A veritable tsunami of token offerings, exceeding $2.3 billion, washed through the initial coin offering (ICO) market in 2017 signalling the high watermark for this unregulated space (Zetzsche et al. 2018). By early 2018 it is estimated that half of these had already failed. A financial scandal of this scale did not go unnoticed by regulators. In the United States and Switzerland the respective agencies FINRA and FINMA brought existing securities legislation to bare on token offerings. The ICO space would no longer be the refuge from red tape and regulation for businesses

A. Le Gear (✉)
Horizon Globex Ltd, Zug, Switzerland
e-mail: andrew.legear@horizon-globex.ie

H. Treiblmaier and T. Clohessy (eds.), *Blockchain and Distributed Ledger Technology Use Cases*, Progress in IS, https://doi.org/10.1007/978-3-030-44337-5_6

raising investment that it once was. The *Securities and Exchange Commission* (SEC) officially declared Ether and Bitcoin as currencies, bringing the baggage of existing banking statutes in tow, and enforcement actions and subpoenas began to be served to non-compliant token offerings (Clayton 2018).

Out of necessity, a new breed of compliant token offerings have begun to emerge. Disassociating themselves from past scandals, the interchangable acronyms of DSO (Digital Security Offering) and STO (Security Token Offering) have come into parlance, whose names serve as an acknowledgement that token offerings are in fact subject to securities legislation and must be structured accordingly (Koverko and Housser 2018). This forces the issuer of a DSO or STO to acknowledge explicitly in their token contracts the roles of actors and processes that were gleefully ignored in the now archaically trivial business logic of an ERC-20. The roles of broker, issuer or transfer agent and processes for anti-money laundering (AML), know-your-customer (KYC) and dictated holding periods for tokens are mandated by law and must now be explicitly enforced in smart contracts. These requirements create as much overhead for a DSO or STO as there is experienced in a traditional initial public offering (IPO). Despite this, we quickly realise that there is no better innovation positioned to enforce the roles and procedures of an IPO/DSO/STO than a smart contract enabled blockchain solution.

Described in this chapter is such a platform and shows how the blockchain can be leveraged to support regulated requirements:

- *Notarisation*: Notarisation of the receipt of official documentation.
- *KYC*: The purpose of providing irrefutable proof of identity and source of investment funds.
- *AML*: Anti-money laundering procedures applied to KYC processes.
- *Regulation D 506c and Regulation S*: Non US offerings brought to the US market must be held by US citizens for one year post purchase.
- *Transfer Agents (Custody)*: A legally separate role whose responsibility is to move ownership of tokens between individuals, release securities in the event of an owners death and to enforce special holding periods where buyers or sellers of a token are registered affiliates of the issuing company.
- *Token Types—Utility Tokens versus Security Tokens (Primary Issuance)*: Depending on the categorisation of the token, it's primary function might be to provide a utility (e.g. gaining access to another platform), as opposed to representing an investment and legal ownership of an entity, as is the case with security tokens.
- *Bespoke Exchange (Secondary Trading)*: A means for onward, secondary trading, post-DSO, while also enforcing holding periods for US and non-US citizens.

Also described is a live executed example DSO, detailing the real world usage of an implementation of this platform. We use it to launch the DSO for a blockchain VoIP communications product called "Talketh" represented by a token with the exchange symbol "VOX." We explain the entire experience of executing this DSO including KYC, AML, custody, tokenisation and onward trading, all enabled and fully compliant as part of the blockchain solution platform on Ethereum.

For the issuer and other participating actors, the live example paints a picture of true success in forging compromise between the apparent utopian future of trustless solutions on the blockchain against the immovable regulatory institutions of old. We believe it provides a model for future adoption of blockchain solutions where existing legislation is embraced rather than subverted—disruptive technologies do not necessarily need to flirt with illegality.

2 The Security Lifecycle

First, let us expand upon the blockchain use case we are solving. Figure 1 presents a high-level view of the security lifecycle. Subtleties on a per jurisdiction basis exist as you drill into each of these steps. However, at this level of granularity, issuing a security will follow these steps the world over.

The actors involved include:

- *Issuer*: This the legal owner of the entity for which public ownership is being issued. This is the most accountable role in the process flow. All responsibility for breach of securities law ultimately resides with the issuer.
- *Reviewer*: A licensed professional who assesses KYC submissions. Relevant background checks are performed (AML) on a best effort basis and are approved accordingly to become investors in the primary issuance of the security. The role of the KYC reviewer is discussed further in the section "A Note on KYC Reviewers."
- *Transfer Agent*: The role can go by other names in other jurisdictions. We use the United States terminology here. A transfer agent is a form of "custodian" who, for various legal reasons, is empowered to hold the issued securities on behalf

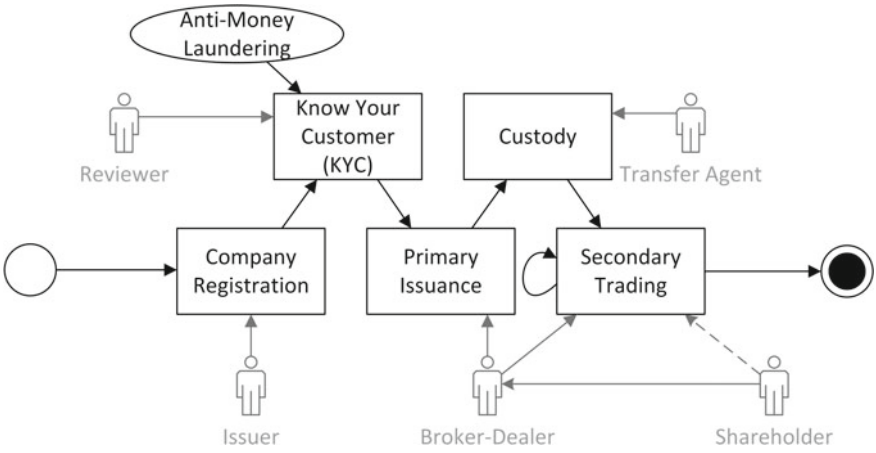

Fig. 1 The security lifecycle

of shareholders and the government. We discuss this role in more detail in the "Custody" section.

- *Broker-Dealer*: A licensed intermediary between the shareholders and all other actors in the process flow. Their role is especially pronounced where the securities are distributed, traded and investors are initially solicited.
- *Shareholders*: The owner of of an issued security. They may have gained ownership as part of the initial DSO, or later through a secondary trading venue.

The various actors then engage in the security lifecycle as follows (Fig. 1):

1. *Company Registration*: The lifecycle begins with a legal entity for which fractional ownership that will ultimately be distributed in the form of securities. The initial ownership, prior to public primary issuance, must be carefully recorded and stored. Where and how it is recorded is known as a "Good Control Location" in regulatory parlance (Ballard 1993). However, the means by which this is achieved is not explicitly stipulated—it must simply be "well known" and described in the company registration documents. The consequence of this is that an issuer may record the ownership of a company on the back of a napkin should they wish to. Obviously this is unwise, however, it is not uncommon to find private company ownership recorded on a single spreadsheet on a company hard drive. While beyond the scope of this chapter, it is worth highlighting yet another valuable blockchain use case opportunity here.
2. *KYC*: At this point, prospective investors are vetted for suitability. Reasonable effort must be employed to prove the identity of the investor. This can include, photographs, identity documents, live interviews and official payment documents from other utilities.
3. *AML*: Closely related to the KYC step, the Anti-money laundering step includes a legally required effort to exclude known criminals, politically exposed individuals and investors from sanctioned countries from the primary issuance.
4. *Primary Issuance*: The official distribution of the purchased securities to investors. The actual process often takes the form of a "closing call" where issuer, broker-dealer and custodian step through each approved investor, confirm payment and record in the good control location the new ownership of shareholder. Note, as emphasised in step 1, this is how the ownership is recorded and not, as is presented in popular culture, through a share certificate. Share certificates certainly exist. However, their role is more as a receipt for proof of purchase during dispute resolution, rather than a definitive legal demonstration of ownership. In fact, physical certificates are becoming increasingly rare and have been replaced with a digital representation for quite some time (Morris and Goldstein 2009). The opportunity for blockchain here is not to replace the share certificate, but to create a public, trusted, good control location for the company register of ownership.
5. *Custody*: This topic covers a wide range of functions performed on behalf of shareholders. We cover this in more detail in the "Custody" section. In the United States, as part of the securities lifecycle, a licensed individual known as a "transfer agent" performs this role. Key responsibilities include:

- Safe storage of physical share certificates.
- Preventing onward distribution of securities for legally required holding periods, post-primary issuance.
- Protecting investors from insider trading by preventing the onward sale of securities by affiliates of the issuing company.
- Reissuing certificates where a share certificate has been lost.
- Implementing court orders where securities must be transferred to the state in the event of a shareholder death or a criminal proceedings.

6. *Secondary Trading*: Finally, shareholders are now able to sell their issued securities onward in a licensed secondary market either directly or via a broker-dealer. We discuss blockchain supported options for this step in the section on "Secondary Trading".

3 The Talketh DSO

It is important to highlight that the blockchain supported solutions for the security lifecycle, that is described in the following sections, is not merely aspirational. It describes the real world implementation of live software and smart contracts, used to realise the Talketh VoIP DSO, which ran from November 2018 to February 2019.

Talketh is an optimised voice over IP (VoIP) smart phone app produced by Horizon Globex Ltd.[1] The app's value proposition was threefold:

- The patented optimised VoIP aspect of the product allowed the use of VoIP on 2G and Edge networks in parts of the world where other VoIP apps were unusable (Dantas et al. 2017).
- Competitive pricing for call minutes over traditional mobile carriers.
- The app could be topped up using cryptocurrency allowing up to 1 billion unbanked individuals access to the VoIP market.

The Talketh DSO was intended as a capital raise to fund expansion into it's intended markets. The DSO came under Swiss financial jurisdiction and was executed in compliance with regulations set out by FINMA (Thompson 2013).

To achieve regulatory compliance, we implemented the following products to execute the Talketh (and other future) DSOs:

- A "Know Your Customer" (KYC) solution called "KYCWare".[2]
- An Anti-Money-Laundering (AML) solution called "AML Cop".[3]
- A custody solution called "CustodyWare".[4]

[1] https://horizon-globex.com.

[2] https://kycware.com.

[3] https://amlcop.com.

[4] https://custodyware.com.

- A tokenisation solution called "Tokenetics".[5]

In the following sections we will explore the blockchain use cases employed in realising these solutions and specifically how they applied to the Talketh VoIP DSO.

4 Proposing a Blockchain Supported Solution for the Security Lifecycle

With our use case clearly defined we can now propose a blockchain supported software solution that adds value and trust to the process. Figure 2 summarises this proposal outlining key public blockchain hooks.[6] The following subsections will explore each of the components in detail:

- *KYC App + KYC and AML Web Service*: A white labeled smart phone application intended to be used by a prospective shareholder. The app will glean relevant KYC details, package them and submit them to the server. At the point of upload, the hash of the KYC pack is notarised to the blockchain to facilitate future dispute resolution and also to give the user confidence that the uploaded pack has remained untampered with throughout the process.
- *KYC Reviewer + KYC and AML Web Service*: A web client dashboard (Fig. 5) to be used by an approved KYC Reviewer. The KYC reviewer can review submissions

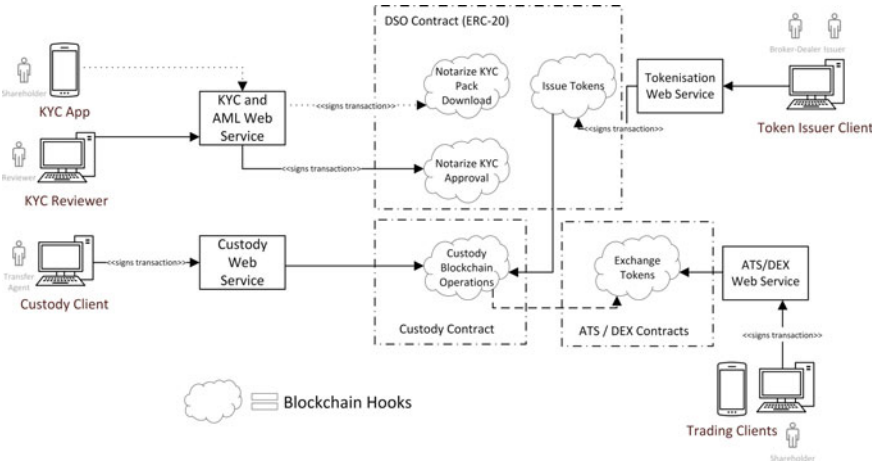

Fig. 2 A blockchain supported software solution for the security lifecycle

[5] https://tokenetics.com.

[6] Where a "blockchain hook" refers to an entry point on a smart contract that can be executed by traditional software.

and approve if appropriate. The approval is notarised to the blockchain to provide a verifiable chain of trust in the approval process.

- *Token Issuer Web Client + Tokenisation Web Service*: Once the issuer and broker dealer are satisfied with the suitability and identity of the prospective investor, the DSO is executed—security/utility tokens are minted and distributed to the wallets of shareholders on the blockchain. Depending on the local regulations or the type of shareholder, the tokens are deposited with a transfer agent who will custody the tokens on the shareholders behalf.
- *Custody Web Client + Custody Web Service*: A web front end intended to be used by a regulated transfer agent. Importantly, this solution makes the transfer agent responsible for maintaining their own private key for signing transactions to execute typical transfer agent tasks. This eliminates the potential that someone impersonated the transfer agent as part of the custody process. In the section "Custody" we discuss exactly what these "transfer agent tasks" are.
- *Trading Clients + ATS/DEX Web Service*: Finally, the custodian (transfer agent) releases the tokens to the shareholder for onward secondary trading. This can only be done if specific regulatory conditions are met (see the "Secondary Trading" section). An app and web service are provided to execute the exchange of tokens between shareholders. Shareholders sign transactions to execute this exchange, however centralised oversight is still needed to meet regulatory requirements. While this may be anathema to decentralised blockchain evangelists, it is a necessary step to ensure regulatory compliance. This can neatly be summarised for our system as "Decentralised trading, centralised control."

In the following subsections we will expand upon each of the subprocesses in Fig. 2 to demonstrate how they are implemented.

5 Know Your Customer and Anti-money Laundering

A KYC and AML process is stipulated by financial regulators to prevent criminal activity in the financial markets and to protect investors participating in those markets. The protections referred to may not be initially obvious. Many public offerings, while perfectly legitimate, can be deemed of high risk and not suitable for investors of lesser means. Effectively, the regulator's role here is to prevent individuals from being reckless with their own money, by only allowing individuals above a certain wealth threshold, known as "accredited investors" (Lee 2011), to participate.

Common KYC and AML requirements include:

- Identifying details such as name, address, phone number, photograph.
- Proof of address such as a utility bill.
- Proof of citizenship by way of passport or drivers license.
- Meeting the individual.
- The individual is not politically exposed or has a criminal history.

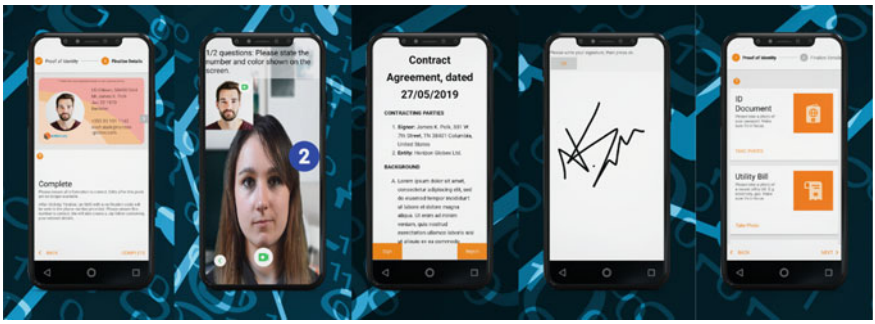

Fig. 3 Compliant KYC and AML app

- The individual has the financial means to participate in the investment.

Figure 3 shows several screen shots from our solution, implementing a compliant KYC solution, mapping to the "KYC App" from Fig. 2. However, in the context of this chapter we will only focus on how the solution integrates with the blockchain and adds value to a compliant KYC process.

5.1 A Note on KYC Reviewers

The role of reviewer in the KYC process is not simply an actor in a use case. It is an official, regulated role in many jurisdictions. The common structure is shown in Fig. 4. Residing at the top level is the financial regulator of the country. Taking the United States and Switzerland as examples, this maps to the SEC (Seligman 1982) and Swiss *Financial Market Supervisory Authority* (FINMA) (Thompson 2013) respectively. These regulators then in turn fund a non-profit entity to enforce these regulations—in our example this maps to the *Financial Industry Regulator Authority* (FINRA) (Black 2013) in the US and the *Financial Services Standards Association* (VQF) (Müller-Studer 2004) in Switzerland. The role of these authorities is to legally enforce the regulations in that jurisdiction and, importantly, to authorise any professionals who operate in this marketplace. This includes individuals who are authorised to review and approve KYC information, who must acquire a license from the enforcement agency.

5.2 A Compliant, Blockchain Supported KYC Platform

Our compliant blockchain supported solution for KYC and AML has three important blockchain hooks:

1. Ethereum wallets:
   - Token receiving wallet.

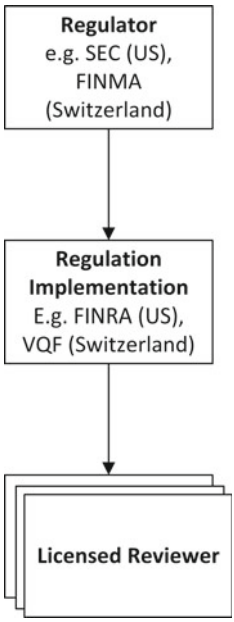

Fig. 4 KYC reviewer in a regulatory context

- Payment wallet.

2. Notarisations:
   - Hash of KYC pack upon upload.
   - KYC approval by the KYC reviewer.

Ethereum Wallets

Unlike a traditional KYC process, when operating within a blockchain and security tokenisation space, the opportunity for fraud is rampant (Fleder et al. 2015; Griffin and Shams 2018; Spagnuolo et al. 2014). If the investor wishes to pay in cryptocurrency[7] or has identified a wallet to receive security tokens, then those wallets must be subjected to a level of due diligence. Our solution provides for two blockchain supports to ease the KYC and AML assessment of these wallets (Fig. 5):

1. *Clean Wallet Creation*: Built into the process flow of the KYC app[8] is the option to create a new wallet, purely for the purposes of receiving tokens as part of the offering. A fresh wallet, with no pre-existing transactions, cannot by definition have any fraudulent transactions, thus dramatically easing the review process. Post-DSO, an investor can then move their tokens from this "hot wallet" to more secure "cold storage" in the form of a hardware wallet or printed key in a safe (Wong and Pocock 2018).
2. *Assisted Wallet Forensics*: The *public* wallet addresses, provided as part of the KYC process are uploaded to the server as part of the KYC pack for the reviewer

[7] Which, incidentally, is illegal in most jurisdictions as of July 2019.

[8] Visit https://kycware.com for further information.

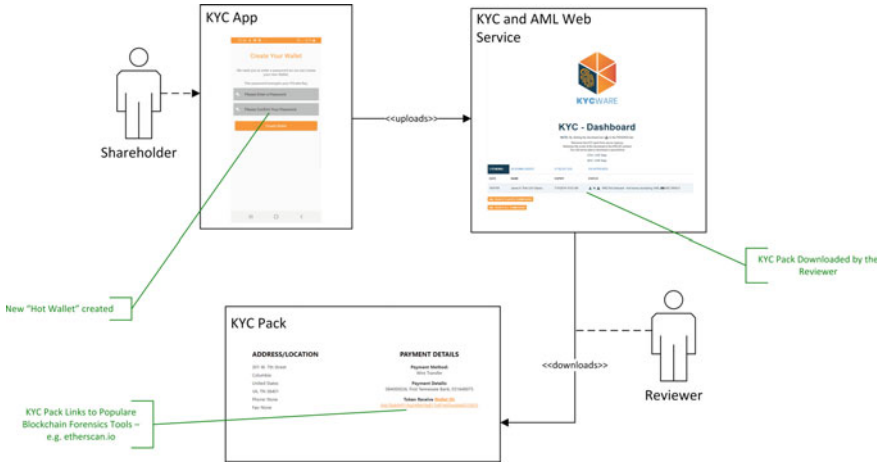

Fig. 5 Blockchain hooks for ethereum wallets

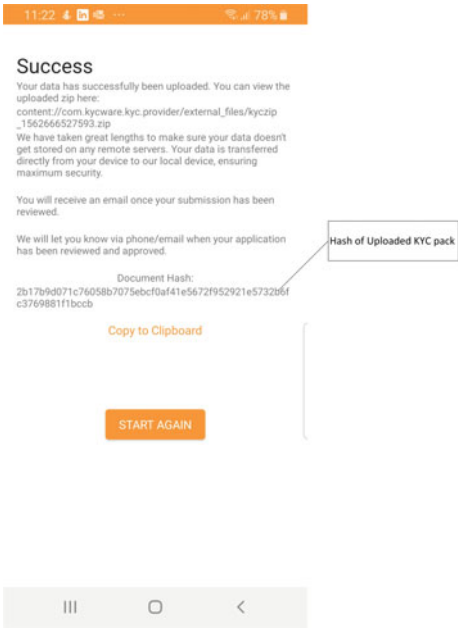

Fig. 6 Hash of KYC pack, post upload

to assess. We can then link the reviewer to popular blockchain forensic tools to aid in an AML assessment of these wallets.

Notarisations

We also leverage the Ethereum blockchain to provide providence at two steps of the KYC process. The KYC App uploads a zip file (the KYC pack) to the server. A hash of this file is provided to the user at the time of upload (shown in Fig. 6). The

KYC reviewer is also aware of this hash, while thirdly, the hash is also stored to the Ethereum smart contract, shown here:

Listing 6.1 Notarisation of Hash

```
function setKycHash(bytes32 sha) public onlyOwner {
    kycHashes.push(sha);
}
```

This is incredibly important where disputes arise, as a single byte change to the KYC Pack file will result in a drastically different hash. Both investor and reviewer can know with confidence that untampered KYC packs are being referenced when resolving disputes.

Finally, when a KYC reviewer is satisfied that a pack has passed KYC and AML checks, he will approve the pack to participate in the DSO. The new state of the KYC review—that it is now approved for the receiving wallet—is notarised to the Ethereum smart contract:

Listing 6.2 Notarisation of Approval

```
function kycApproved(bytes32 sha) public onlyKycProvider {
    kycValidated.push(sha);
}
```

Note the "onlyKycProvider" modifier in this case. This modifier is defined as:

Listing 6.3 Only KYC Provider

```
modifier onlyKycProvider {
    require(msg.sender == regulatorApprovedKycProvider, "Only the KYC Provider can call this function.");
    _;
}
```

It stipulates that only a specific nominated private key can approve submissions. The KYC provider must sign these transactions and only she possesses the private key of the nominated wallet. This enforces the securities regulations dictated at a blockchain smart contract level.[9]

6 Primary Issuance

Primary issuance refers to the initial creation of securities as part of a public offering (Gray et al. 1997). The security originates from the issuer and was not acquired through a third party, as you would when trading in a marketplace. In a blockchain context, "tokenisation" is a primary issuance where the issued securities are expressed within a smart contract and distributed to wallets owned by shareholders (Chen 2018). The act of tokenising an asset for the purposes of sale as part of a capital raise is a "Digital Securities Offering" (DSO)—The blockchain equivalent of an IPO (Kranz et al. 2019).

[9]For reference, a deployed example of this contract is here: https://kovan.etherscan.io/address/0x88e6f26a86caf47873e7c84bd43808f895b88b5a#contracts.

The most prevalent approach to creating a security token on the Ethereum blockchain is to implement the ERC-20 standard (Vogelsteller and Buterin 2018). At the time of writing, several other competing standards have been proposed, but none have achieved the same widespread adoption as ERC-20. These other ERC's include ERC-223, ERC-677, ERC-777, ERC-721 and ERC-827.[10] They attempt to solve various problems such as minting, fungibility and token loss, which were all vulnerabilities of the original ERC-20 specification.

The focus of the proposed solution in this chapter centers around compliance. Our approach has been to take a standard ERC-20 implementation and augment it to satisfy regulatory requirements including:

- Transfers can only occur between token holders approved through the KYC process.
- The definition of the DSO being complete, and then restricting transfers to the issuer only until the DSO is complete.
- Burning of tokens to reduce supply.

An example of these requirements deployed to Ethereum mainnet is here:

https://etherscan.io/address/0xbaf8f642e51e4dd275f1a4bdc960dcf14d9094b4#contracts—a contract used to tokenise the "Talketh VoIP" DSO. The specific blockchain hooks corresponding to the above list are:

Listing 6.4 Key ERC-20 Ammendments for Compliant Tokenisation

```
// (1)
    function _transfer(address from, address to, uint256 value) internal returns (bool) {
    require(isAuthorised(to), "Target of transfer has not passed KYC");

...

// (2)
   function icoTransfer(address to, uint256 value) public onlyOwner {
    require(!isIcoComplete, "ICO is complete, use transfer().");

...

// (3)
function _burn(address addressToBurn, uint256 value) private returns (bool success)
```

Earlier, the KYC reviewer possessed a separate key for signing transactions when notarising KYC approval. This now becomes more important as it creates a deliberate compliance barrier between the issuer, broker-dealer and regulated approver and, as will become evident in the following section, a divide between the custodian also. This provides clear and compliant separation of roles. To allow a broker-dealer to interact with these hooks as part of the tokenisation flow of a DSO we provide a web client for ease of use (Fig. 7). For this component, the web client is password protected and the private key of the issuer installed on the web server within a secure network, which is used to sign transactions needed to distribute the tokens. The

[10]The full list of Ethereum Request for Comment (ERC) is here: https://github.com/ethereum/EIPs/tree/master/EIPS.

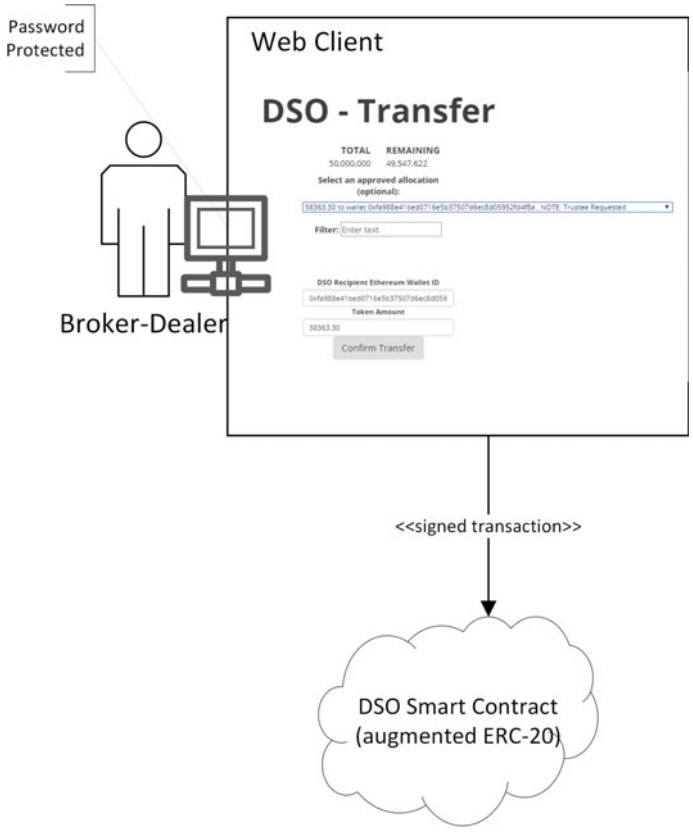

Fig. 7 Compliantly distributing tokens

broker and issuer, as part of the closing call, can then use the web client to distribute the tokens to complete the DSO. Figure 7 describes this flow. One important feature, that will be expanded upon in the next section, is that in certain circumstances, the regulations require that the tokens be transferred directly to a custodian and marked as "held" for shareholder. The web client described automatically handles this scenario, depending on the jurisdiction of the DSO.

7 Custody

Custody in the regulated securities markets is a core concept, and yet is one that, until recently, has been completely overlooked by the utopian, distributed token vision provided by blockchain. As part of the United States primary security issuances market, the role of the custodian is called a "Transfer Agent" (Loader 2013). Important functions performed by a transfer agent include:

- Foreign entities, performing public offerings on US financial markets, selling to US citizens are subject to Regulation D 506-c exemption (Freedman and Nutting 2015), which requires a transfer agent to hold the issued securities for a period of up to one year before onward sale by the shareholder.
- The closing call of an IPO first requires custody to be transferred to a transfer agent before onward distribution to shareholders.
- Affiliates of the issuing entity must deposit newly purchased securities to a transfer agent for a 3 month holding period to negate the potential of insider trading.
- Seized assets must be transferred to the state in the event of criminal suits.
- The security possessions of a deceased shareholder must be redistributed by transfer agents to new owners or the state.

The implication here for decentralised purists is, of course, grim. It is the law that some form of centralised oversight exists. When you own a security, you are not free to do with it as you please. In spite of this, it is important to note, that giving up some decentralisation does not equate to complete centralisation. In fact, earlier we discussed the restriction where transfers could only occur between individuals that had been subjected to KYC—This is another example of an incremental retrenchment towards centralisation—however, it is certainly not a complete abandonment of decentralisation in the process.

Figure 8 shows a dashboard we provide to transfer agents to perform common custody tasks to allow them support compliant DSO's. Each of the menu items is supported by a blockchain hook on a separate smart contract to manage custody:

- *Transfer*: Move tokens between two wallets.
- *Custody*: Pull tokens into custody from a token holder who has pre-approved a transfer.[11] This is intended to be used where secondary trading has already begun and tokens are being returned to custody.
- *Release*: Transfer control of tokens back to a shareholder. This moves tokens from the custody contract to the shareholders wallet.
- *Partial Release*: Same as previous, except only a portion of the tokens are released.
- *Holding Details*: Query the token quantities currently being held on behalf of a shareholder.
- *Add Time*: Increase or decrease the holding period assigned to a shareholder.
- *Set Affiliate Status*: Mark a shareholder as an "affiliate." Thus if they receive tokens they would be subject to a holding period before they could be released.

A complete code listing for the custody smart contract can be found here

https://etherscan.io/address/0xb966bb63027f82fcb8de4f07bc4084c5735d5112#contracts. We noted above, that the "Custody" function was one entry point to custody, post-DSO. The other entry point is part of the initial token distribution and was alluded to at the end of the previous section. We perform this transfer in an uncommon way, worth expanding on. First, tokens are transferred to the address of the custody smart contract. Then "hold()" is executed on the custody smart contract

[11] Used the "approve()" and "transferFrom()" operations on the standard ERC-20 interface.

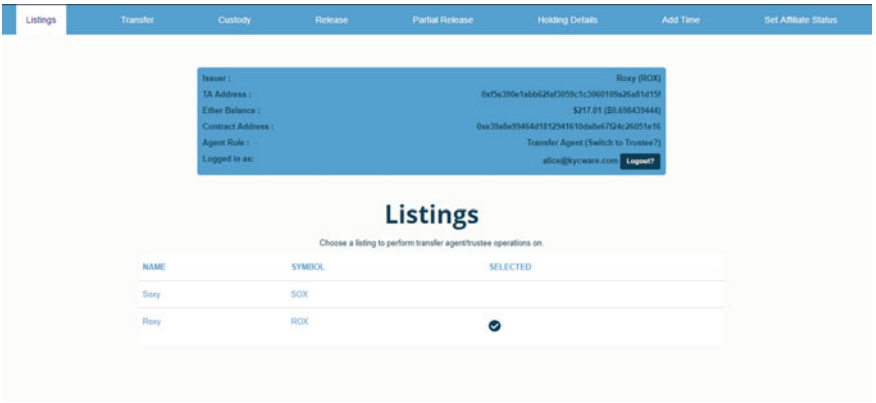

Fig. 8 Compliant custody dashboard for a transfer agent

to place a ledger entry that this custody contract is holding a portion of it's tokens for a specific shareholder. Note, that the transfer was not to the wallet address of the transfer agent, but to the actual smart contract address where the range of operations that can be performed with the tokens is strictly limited to clearly defined roles of a transfer agent. The transfer agents wallet is the only wallet permissioned to execute these functions on the custody smart contract, but equally the transfer agent is prevented from stealing the tokens for himself. Also, the semantic difference here is important—the transfer agent has the tokens in custody, but is never actually an owner of the tokens.

8 Secondary Trading

Technically, by this stage, the DSO is complete. For completeness we will discuss the secondary trading phase, however this topic is vast. A full discussion of blockchain distributed exchanges and secondary trading venues is beyond the scope of this chapter.

We will discuss a single secondary trading venue example, that is narrow in scope, yet compliant within it's jurisdiction. It is a simple DEX for the exchange of Talketh utility tokens and is deployed on the Ethereum Mainnet[12] here

https://etherscan.io/address/0x01e15429fedbc08dec25e127df09b4af17167f5e#contracts

At it's simplest, the DEX is an Ethereum smart contract which records bids and asks from token holders. A "bid" states the maximum that buyer is willing to pay, and the "ask" is the minumum a seller is willing to accept. If there is an overlap

[12]The name ascribed to the production network of Ethereum.

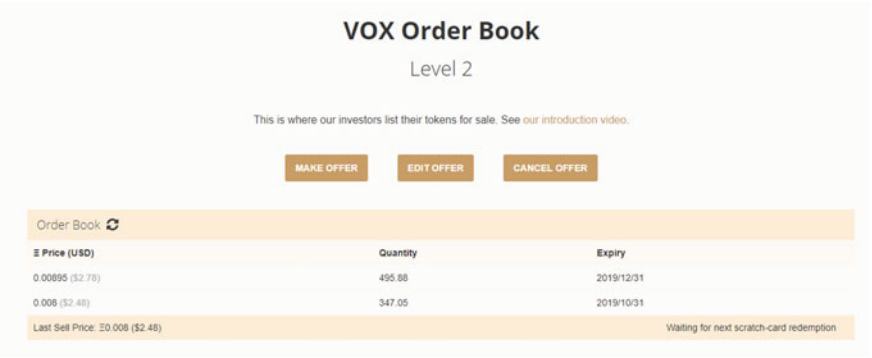

Fig. 9 Web client for the DEX

between these two prices a "cross" occurs and tokens are transferred, using the existing "transfer()" on the related ERC-20 an exchange, from seller to buyer. These DEX functions correspond to the following on the smart contract:

Listing 6.5 Bid/Ask and Cross on the DEX Interface

```
// Buy
function multiExecute(address[] sellers, uint256 lastQuantity) public payable returns (uint256 totalVouchers)
// Ask
function offer(uint256 quantity, uint256 price, uint256 expiry) public
// Execute
function execute(address seller, uint256 quantity, uint256 price)
```

Beyond these basic hooks, the DEX contract also offers support for cancels, price floors and ceilings, restricting trading to KYC'd individuals, fees, and specific calls where vouchers are being redeemed (discussed below). Asks can be placed on the DEX and the current order book viewed using a provided web client shown in Fig. 9. As with the other previous services provided, placing asks and cancels can only be achieved by the holder of the private key in order to sign the transactions. The transactions are signed locally and the private key never leaves the device of the user—in this sense it is a true distributed exchange.

The token economics needed to drive the liquidity of such a DEX emerges from the following business drivers:

- The minted tokens are "utility" tokens rather then "security" tokens. That is, their value is a utility that can be redeemed, rather than representing legal ownership of a company.
- In this case, the utility represented is discounted international call minutes.
- Large investors in the Talketh DSO would adopt the role of international wholesalers of call minutes, and thus would purchase the utility token at scale upon launch of the DSO.
- The capital raised as part of the DSO would then be deployed to fund sales and marketing of the platform internationally.
- Next, two mechanisms to provide an exit for the initial utility token purchasers are structured:

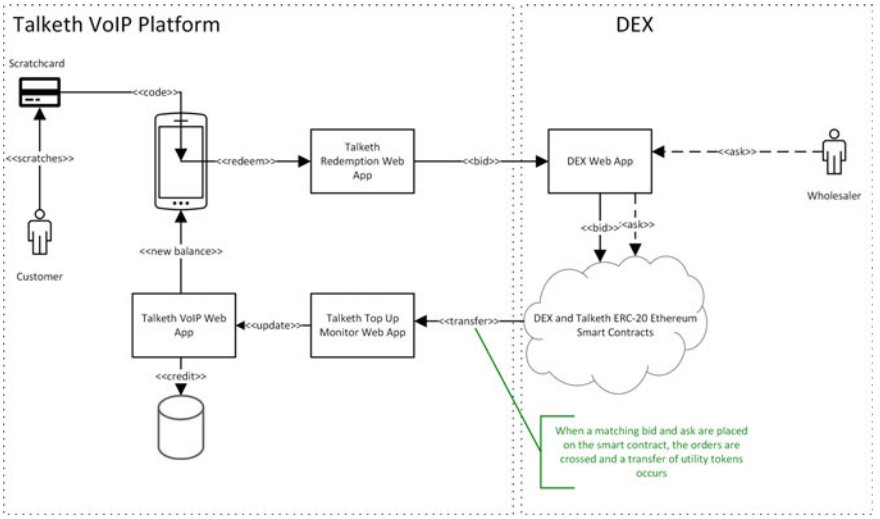

Fig. 10 Using a scratchcard to match an ask placed on the DEX

1. Local re-sellers[13] of call credit for Talketh can purchase minutes from the wholesalers on the DEX for onward distribution, with the wholesalers offering a typical markup on their ask price. Since the utility tokens were originally minted to redeem discounted minutes, the scope for profit margin lies in the difference between the face value of the minutes represented and the original token price.
2. Dealing with blockchain, wallets, signing transactions and acquiring cryptocurrency are quite significant technical barriers to entry for the average individual. As such, the Talketh platform has also rolled out a scratch card system for topping up. Scratch cards can be purchased with local currency and redeemed in the app. Instead of simply purchasing credit at full price, the scratch card redemption is linked to the DEX and will automatically attempt to purchase a discounted utility token from the market. The incentive here is clear: The customer has the opportunity to receive more credit than the apparent face value of the scratchcard, while also providing an exit with a margin for the wholesaler. This redemption mechanism is described in Fig. 10.

8.1 A Note on Blockchain Capacity for High Volume DEX Platforms

The capacity of a blockchain, like Ethereum, to scale is often cited as a looming problem (Gencer et al. 2018). As it currently stands, Ethereum can handle up to

[13] For example, the owner of a corner shop.

25 transactions per second (Buterin 2016c). The comparative use case that is often cited is that of the traditional platforms of Visa and Mastercard both handling 5000 transactions per second (Beck et al. 2016). Even choosing the much narrower use case of trading systems (as opposed to global transactions of all sorts), NASDAQ still requires 10 times the reported Ethereum maximum of 15 transactions per second. Arguably, some of these criticisms are unfair. Discounting the upcoming throughput gains promised by Ethereum 2.0 (Buterin 2016a, b), the comparative use cases of Visa, Mastercard and NASDAQ refer to the largest transactional systems of their kind on the planet. While an ambitious and worthy goal for blockchain technology, for which it currently falls short, there are many large traditional platforms that Ethereum currently has ample capacity to disrupt. For example, "OTC Markets" is the public home of over 10,000 listed American companies. By contrast, the NASDAQ has only 3300 listings. Yet, the OTC only requires a capacity of 180,000 trades per day. Ethereum could handle 10 times the volumes of the OTC as it currently stands (Domanski and Heath 2007)—Facts worth considering given the prevalence of counter arguments to this opinion.

9 Conclusion

Over the course of this chapter we have discussed the difficult blockchain use case of security offerings. This difficulty is not so much a technical, but a regulatory and compliance one. Navigating international securities regulation requires expert legal and professional input in lock step with a technical implementation team. Demonstrating with a live execution, in the form of the Talketh DSO, we have accomplished this goal, and produced a reusable implementation of the regulatory business logic, supported by the blockchain at its core. We are already applying this platform to more DSO's and future work will focus on compliant secondary trading in the United States to complement the platform. As a base technology, blockchain is now well positioned to add real value to complicated use cases like compliant security offerings and holds the real potential now to be at the center of one of the worlds most valuable technology genres.

References

Ballard, S. V. V. L. (1993). Memorandum of understanding between the United States. *SEC Docket, 54*(5).

Beck, R., Stenum Czepluch, J., Lollike, N., & Malone, S. (2016). Blockchain—The gateway to trust-free cryptographic transactions.

Black, B. (2013). Punishing bad brokers: Self-regulation and finra sanctions. *Brooklyn Journal of Corporate, Financial & Commercial Law, 8*, 23.

Buterin, V. (2016a). Ethereum 2.0 mauve paper. In *Ethereum developer conference* (Vol. 2).

Buterin, V. (2016b). Ethereum 2.0 mauve paper. In *Ethereum developer conference* (Vol. 2).

Buterin, V. (2016c). Ethereum: Platform review. *Opportunities and Challenges for Private and Consortium Blockchains*.
Chen, Y. (2018). Blockchain tokens and the potential democratization of entrepreneurship and innovation. *Business Horizons, 61*(4), 567–575.
Clayton, J. (2018). Chairman's testimony on virtual currencies: The roles of the sec and cftc. In *Testimony before the committee on banking, housing, and urban affairs, United States senate*.
Dantas, R., Exton, C., & Le Gear, A. (2017). Improving mobile voip quality through bandwidth optimisation.
Domanski, D. & Heath, A. (2007). Financial investors and commodity markets. *BIS Quarterly Review*.
Fleder, M., Kester, M. S., & Pillai, S. (2015). Bitcoin transaction graph analysis. arXiv:1502.01657.
Freedman, D. M., & Nutting, M. R. (2015). The growth of equity crowdfunding. *Value Examiner*, 6–10.
Gencer, A. E., Basu, S., Eyal, I., Van Renesse, R., & Sirer, E. G. (2018). Decentralization in bitcoin and ethereum networks. arXiv:1801.03998.
Gray, S., et al. (1997). Government securities: Primary issuance. Handbooks.
Griffin, J. M., & Shams, A. (2018). Is bitcoin really un-tethered? Available at SSRN 3195066.
Koverko, T., & Housser, C. (2018). *Growth*, 4, 5.
Kranz, J., Nagel, E., & Yoo, Y. (2019). Blockchain token sale. *Business & Information Systems Engineering*, 1–9.
Lee, S.-Y. (2011). Why the accredited investor standard fails the average investor. *Review of Banking and Financial Law, 31*, 987.
Loader, D. (2013). *Clearing, settlement and custody*. Butterworth-Heinemann.
Morris, V. B., & Goldstein, S. Z. (2009). *Guide to clearance & settlement: An introduction to dtcc*. Lightbulb Press, Inc.
Müller-Studer, L. (2004). The function of self-regulating organisations in the swiss money laundering control scheme. *Journal of Money Laundering Control, 7*(1), 69–74.
Seligman, J. (1982). *The transformation of wall street: A history of the securities and exchange commission and modern corporate finance*. Boston: Houghton Mifflin.
Spagnuolo, M., Maggi, F., & Zanero, S. (2014). Bitiodine: Extracting intelligence from the bitcoin network. In International conference on financial cryptography and data security (pp. 457–468). Springer.
Thompson, J. H. (2013). A global comparison of insider trading regulations. *International Journal of Accounting and Financial Reporting, 3*(1), 1.
Vogelsteller, F., & Buterin, V. (2018). Erc-20 token standard, 2015. https://github.com/ethereum/EIPs/tree/master/EIPS, 04–13.
Wong, S., & Pocock, A. (2018). Digital assets and their impact on wealth management. Available at SSRN 3367451.
Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Föhr, L. (2018). The ICO gold rush: It's a scam, it's a bubble, it's a super challenge for regulators.

Author Biographies

Andrew Le Gear received a B.Sc. 1st Class Honours Degree in Computer Systems from the University of Limerick in 2003. This was followed by a research scholarship with the Software Architecture Evolution Group at the same university until December 2006, when he received a Ph.D. in Computer Science entitled "Component Reconn-exion." Andrew is the author of numerous publications in the fields of software maintenance, architecture, analysis and more recently in blockchain analysis and reverse engineering. Since completing his Ph.D., Andrew has also worked as a professional software engineer in several of the worlds most software intense companies including Dell, IBM, QAD, Lehman Brothers, Nomura, and most recently as CTO at Horizon Globex Ltd. Andrew's main academic and professional interests now converge on blockchain technologies and applications.