PROVORMA: A Blockchain for Regulated and Exempted Private Placement Tokens

Oscar Pacey
oscar@tranquilitynode.com
www.provorma.com

Abstract: An implementation of the Prova[i] blockchain software designed to facilitate the distribution and transfer of regulated and exempted tokens used for capital raising purposes. Most jurisdictions have rules governing capital raising activity which are in place to protect investors by restricting higher risk investments to defined demographics. These demographics are often termed Accredited Investors, Sophisticated Investors, Professional Investors, Institutional Investors and Eligible Counterparties. Initial coin offerings can easily fall foul of these laws by nature of their tokens' private, borderless and highly transferrable nature. Provorma is a bitcoin[ii] like blockchain which restricts all addresses to those managed by authorised wallet service providers only. Obtaining a wallet will require validation of the investor's regulatory status. Once validated the investor will be free to hold their tokens and transfer them to other eligible investors. The rules incumbent on any particular token are embedded in the blockchain by the issuer in a manner akin to covenants embedded within property contracts. Provorma tokens may include complex equity and debt like characteristics.

1. Introduction

Financial markets regulators are obliged, within their jurisdiction, to protect investors from the risks inherent in capital raising. Part of their frameworks usually includes some exemptions that allow capital raising to occur outside of the usual controls and obligations so long as the investments are made only by backers whom have the knowledge, experience and wealth to understand and weather the associated risks. Such events are referred to as private placements. If an organisation is willing to raise from such investors only and abide by the associated marketing and solicitation restrictions, then they are afforded exemptions from the usual costs and obligations of a fully regulated securities offering. Private placement rules typically mandate that such securities may only ever be held by eligible investors, thus prohibiting free trade within an open secondary market. In some cases, secondary markets and transfers are expressly prohibited within a defined lock-up period after issuance.

Blockchains offer a means of managing the ownership register of digital assets and a mechanism for facilitating free exchange of ownership. Companies are using blockchain, via ICOs, as a mechanism with which they can issue something equivalent to an unregistered security to a global market of investors. Investors are keen on the liquid secondary market made possible by the tokens and the exchanges which support them. Many ICOs are however in breach of regulations, often in multiple jurisdictions.

Capital raising tokens issued so far have not tended to reflect the complex attributes embedded in traditional equity and debt securities including dividends, voting rights and coupons.

Provorma is a permissioned blockchain standard which offers a compliant means of distributing security tokens and a means to offer more complex rights and profit distribution attributes than has been the norm thus far.

2. Blockchain specification

The open source Prova blockchain software was developed by BitGo[iii] originally to meet the needs of the Royal Mint Gold[iv] project (RMG) in collaboration with Cryptonomy Ltd.[v] RMG may only be held by known individuals who have passed through a know-your-customer (KYC) check. Prova achieves this restriction in a non-custodial way by means of a multi-party, multi-signature addressing scheme. The issuance of gold tokens on to the RMG blockchain is managed by the Royal Mint who hold authorised issuance keys which only they have access to. Prova is therefore well adapted to the needs of private placement securities issuers, their regulators and their investors.

Each capital raising organisation will launch their own security tokens on the Provorma blockchain using the client software. This blockchain will encode the capital attributes and legal restrictions incumbent upon its token by means of an administrative thread known as the 'rules thread', which can be written to using the administrator keys. Transactions made on the rules thread will update an extensible data structure of the following standardised form:

```
{
        Permitted Holder Types: {
                US Accredited Investor SA 1933 Reg D 506,
                EU Professional Investor MiFID 2004,
                UK High Net-worth Individual FSMA 2000,
                AUS Sophisticated Investor CA 2001 6D,
                Etc
        },

        Transferable: {
                Trigger type: block height | time offset | date,
                Trigger: 500,000 | 12 months | 30-Jul-2020
        },

        Voting rights: {
                AGM: {
                        Trigger type: block height | time offset | date,
                        Trigger: 500,000 | 12 months | 30-Jul-2020
                }
                EGM: {
                        Trigger type: block height | time offset | date,
                        Trigger: 500,000 | 12 months | 30-Jul-2020
                }
        }

        Dividend: {
                Type: Variable | Fixed | None,
                Fixed Rate: x%
```

```
                    Asset: Native | External | Scrip
                    Convertible: {
                            Convertible To: Variable | Fixed | FALSE,
                            Trigger Type: block height | time offset | date,
                            Trigger: 500,000 | 12 months | 30-Jul-2020



                    }
            }

            Duration: {
                    Trigger type: block height | time offset | date, FALSE,
                    Trigger: 500,000 | 12 months | 30-Jul-2020,
                    Right: Redemption | Expiry | Etc
            }

            Coupons: {
                    Quantity: 0 | 1 | 2 | … | n,
                    Rate: x%
                    Trigger type: block height | time offset | date,
                    Trigger schedule: {
                            100,000,
                            200,000,
                            300,000,
                            400,000
                            |
                            3 months,
                            6 months,
                            12 months,
                            18 months,
                            |
                            01-Jun-2018,
                            01-Sep-2018,
                            01-Dep-2018,
                            01-Mar-2019
                    }

            }

            Collateral: {
                    Description: Early versions can include a natural language
    description of the type and conditions of collateral. Later versions may
    include automated scripts and references to other blockchains.
            }
    }
```

Early versions of Provorma will rely on the wallet service providers to enforce these rules. Later versions will migrate control to the consensus rules of the Provorma software run by the nodes and block generators.

3. Wallet Service Provider

A Wallet service provider (WSP) will provision an administrative wallet service dedicated to the tokens their client, the issuer, wishes to launch.

Investors in the capital raise will apply for a wallet with the WSP of their choice from the range available. For each investor, the WSP will keep on record the KYC information and regulatory status at the time of verification. The investor will be permitted to hold wallets only for tokens which match their profile.

4. Exchanges

Where transfer of ownership is permitted by law, a token secondary market place may run books for their customers. Such activity will be off-chain and therefore only exchanges compliant with the given rules may be given wallets.

At the time of writing there are a number of exchanges investing in the regulated and exempted security token concept.

5. Investor validation service

Every investor will require validation with each WSP and Exchange they hold a relationship with. Each investor must apply to a centralised Investor Validation Service (IVS) via their WSPs and Exchanges. The IVS will house compliance expertise over all major investor jurisdictions and outsource for minor jurisdictions. Records will be help in accordance with the rules in force over the private placement.

7. Conclusion

Provorma and the ecosystem of IVS, WSPs and Exchanges create a modern, blockchain based infrastructure for encoding security tokens and enabling liquid secondary markets where permitted by law. Capital raising organisation will have access to a global pool of eligible investors via the IVS and the participating WSPs and Exchanges. The capital raising tokens may expire after a period of time to be replaced by unregulated utility tokens on another network or persist in the form of equity and debt tokens perpetually.

---

[i] Prova: https://www.provachain.com
[ii] Bitcoin: https://bitcoin.org/bitcoin.pdf
[iii] BitGo: https://www.bitgo.com/
[iv] RMG: https://www.royalmint.com/invest/bullion/digital-gold/
[v] Cryptonomy: https://www.cryptonomy.com