Improving OTC: Modeling Non-Deliverable Cryptoasset Perpetual Contracts

Justin Smith[1]

[1] *Swisscom Blockchain, Zürich, Switzerland*

January 25, 2019

Over-the-counter (OTC) markets such as the ~450 trillion USD interest rate derivatives market[2] can benefit greatly from cryptofinance technology, which combines the benefits of both traditional OTC and centralized trading. Creating financial products in the form of cryptoassets and trading them algorithmically through Hashed Time-Locked Contract Transactions (HTLC)[3] eliminates counterparty risk, enables uniform trade execution, provides confidentiality in trading without sacrificing auditability, and removes nearly all non-informational barriers that may exist between primary and secondary markets. Fraudulent activity commonly found on centralized platforms, such as front-running, is impossible. However, issuing financial products using cryptofinance technology is a new and not well understood activity. In this article we introduce a model for a simple financial product primitive and suggest how to create and deploy this primitive using free and open source software.

1 Introduction

Financial products (e.g. interest rate swaps, credit default swaps, equities, bonds, bank notes, cash) are contracts between two parties which specify transfers of money now and in the future. In this article we examine a generic model for creating financial products: the **non-deliverable cryptoasset perpetual**, or **NDCP**, where the stated beneficiary of a contract can transfer their right to (perhaps) receive contractually-specified future benefits to another party by transferring control of cryptographic tokens ("tokens"), while the state of any associated off-chain agreement remains unchanged. This is in essence a way to make promises more tangible and tradeable, and removes barriers between primary and secondary markets. Due to the properties of cryptographic tokens, NDCPs may have significant and surprising effects on markets previously believed to be inherently inefficient, such as the secondary market for radio spectrum[8].

In the NDCP model a contract is created specifying buyer, seller, and the terms of the agreement. This contract is executed, validated, and recorded using traditional methods i.e. notarized paper triplicates. To fulfill the contract, the buyer provides consideration and in return receives from the seller a cryptographic token or tokens, which may represent the beneficiary's whole or fractional ownership interest in the underlying paper contract. The buyer may sell or otherwise transfer the cryptographic tokens at any time after taking delivery. However, the *underlying paper contract is never updated*.

2 Cryptographic Token Deployment

In the context of Bitcoin[6], a cryptographic token is simply a Bitcoin transaction which carries some unique data that the contracting parties have agreed to recognize. This allows the contracting parties to benefit from Bitcoin's strengths, such as immutability, non-counterfeitability, ease of transfer, robustness and transparency[4], but also Bitcoin's variable transaction costs. We assume that the highest and best use of the Bitcoin network is Bitcoin transactions, and therefore recommend a very similar and compatible open-source technology to issue cryptographic tokens, an Elements sidechain[5]. This technology allows for rapid transaction speeds and low or even zero transaction costs to the end user. We assume NDCPs are regulated instruments and issued in a legal context; therefore Bitcoin's robust governance and "indestructible" persistence would be superfluous. Credible public or private organizations such as Telecoms are well-suited to maintain NDCP dedicated sidechains, giving traders of the NDCP predictable transaction speed and costs without sacrificing any of the other beneficial properties of Bitcoin.

2.1 Introduction to the Provisioning Process

The sidechain on which the NDCP token is to circulate must always have an appropriate count of nodes in order to ensure the expected level of network security is maintained. A satisfactory distribution of nodes is likely to happen organically, correlated to the number of traders who are using compatible software. Traders will normally operate their own nodes in order to validate incoming transactions, although this validation process may be outsourced to a trusted entity which specializes in IT infrastructure. Such an entity may manage the entire blockchain infrastructure on which NDCPs "run" and provide access or uptime guarantees under a generic Service Level Agreement (SLA).

2.2 Issuance

Issuance is the first step in the provisioning process1. An administrator will specify the quantity of tokens to be issued, and unique hex is generated for the token. This hex is used to track the token on the network. Local clients may label the hex however they like.

2.3 Initial Distribution

After tokens are created, they must be distributed. This process can be administered by a human, or it can be automated. The receiving address(es) belonging to the contract buyer must be known beforehand.

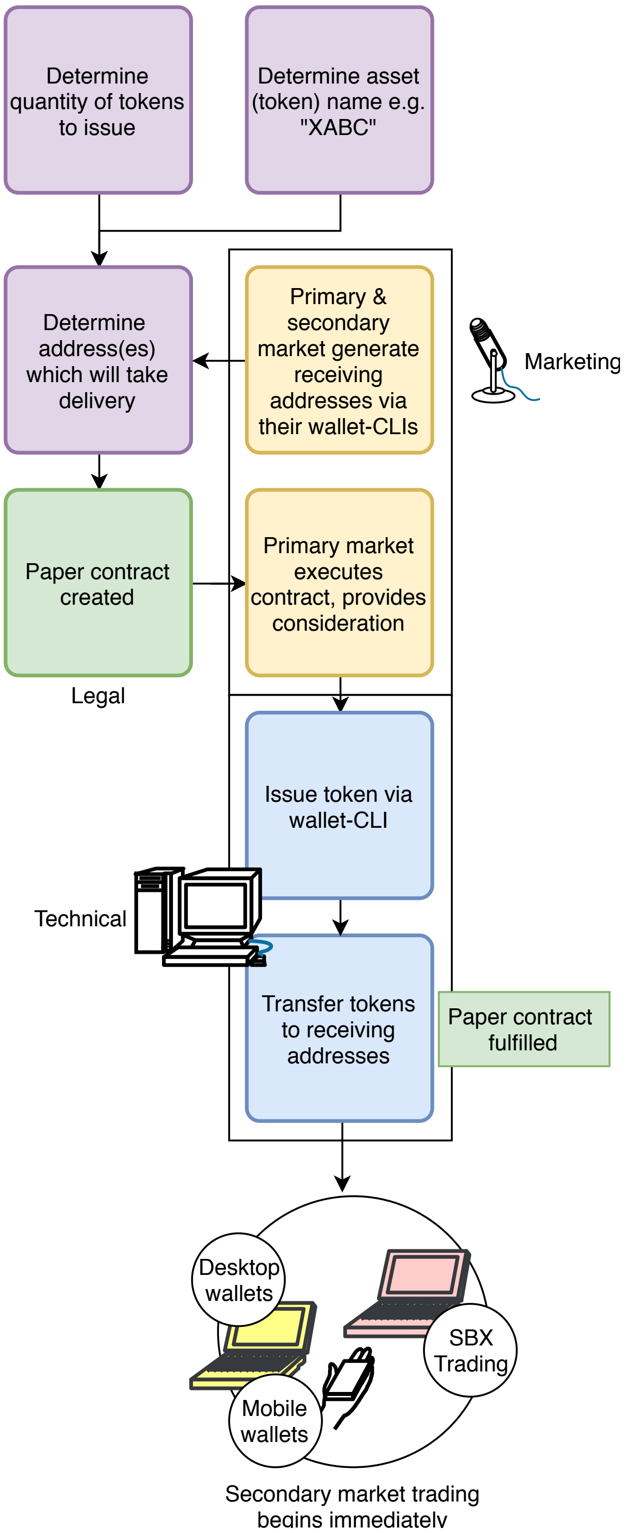
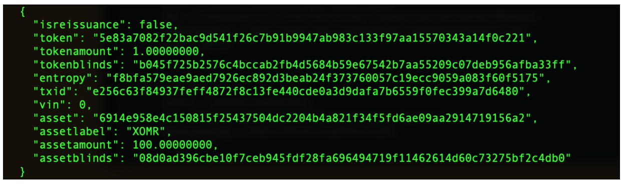

Determine quantity of tokens to issue
Determine asset (token) name e.g. "XABC"
Determine address(es) which will take delivery
Primary & secondary market generate receiving addresses via their wallet-CLIs
Marketing
Paper contract created
Primary market executes contract, provides consideration
Legal
Issue token via wallet-CLI
Technical
Transfer tokens to receiving addresses
Paper contract fulfilled
Desktop wallets
SBX Trading
Mobile wallets
Secondary market trading begins immediately

Figure 1: *A generic process diagram for an NDCP.*



```
{
  "isreissuance": false,
  "token": "5e83a7082f22bac9d541f26c7b91b9947ab983c133f97aa15570343a14f0c221",
  "tokenamount": 1.00000000,
  "tokenblinds": "b045f725b2576c4bccab2fb4d5684b59e67542b7aa55209c07deb956afba33ff",
  "entropy": "f8bfa579eae9aed7926ec892d3beab24f373760057c19ecc9059a083f60f5175",
  "txid": "e256c63f84937feff4872f8c13fe440cde0a3d9dafa7b6559f0fec399a7d6480",
  "vin": 0,
  "asset": "6914e958e4c150815f25437504dc2204b4a821f34f5fd6ae09aa2914719156a2",
  "assetlabel": "XOMR",
  "assetamount": 100.00000000,
  "assetblinds": "08d0ad396cbe10f7ceb945fdf28fa696494719f11462614d60c73275bf2c4db0"
}
```

Figure 2: *100 tokens issued using a wallet-cli software. The label provided by the local client is "XOMR". This label does not travel on the network.*

2.4 Re-Issuance

It is possible to create more of the same token through the process of re-issuance. This activity is hidden from users by default, but the issuer can give full access to an auditor on request. In fact, the issuer can even give control of re-issuance to another party at any time, perhaps an auditor or regulator.

2.5 Validating Transactions

Valid token transactions are included in *blocks*. These blocks can only be produced by special node operators, which may operated by a trusted and well established entity which is impartial, e.g. a telecom. The exact requirements of the quorum required to produce a block will vary depending on the trust model required for the NDCP. It is critical that these special node operators act with absolute impartiality and enforce consensus rules, remaining completely impartial to transactions included in each block, or else trust in the system and the value of any NDCPs on the chain will be damaged or destroyed.

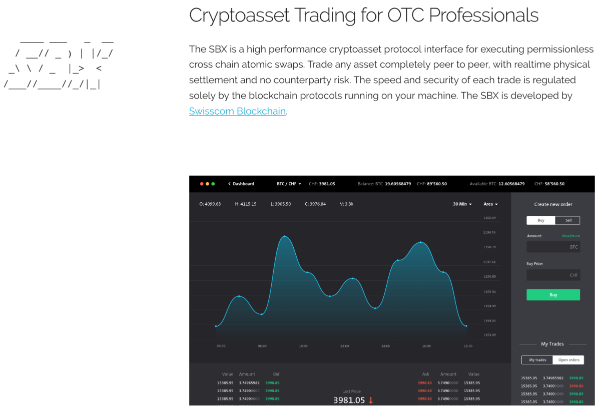
3 Secondary Market Development

In the simplest NDCP cases, no future benefits are promised to the NDCP contract buyer. This means that after the seller delivers the tokens to the buyer during the initial sale, the contract seller has no outstanding obligations.

If the paper contract specifies that some benefits will be given to token holders at some point in the future, any token holder (contract buyer, or beneficiary) wishing to claim their benefits must prove that they control some number of tokens. A proven way of completely automating delivery of a precise amount of money to the correct beneficiary is via Bitcoin[7]. The beneficiary signs a message in their Bitcoin wallet which includes their token receiving address, then present the resulting signature to the contract seller.

3.1 Secondary Market Infrastructure

Secondary market participants need at a minimum 1) a means to take delivery of their cryptographic tokens and 2) a means to trade their cryptographic tokens for other tokens and cryptocurrencies Over the Counter, or in computer networking terms *peer to peer*. Normally, anyone with a modern computer and stable network connection should be able to download free and use free and open source software which enables them to take delivery of tokens. But trading cryptographic tokens OTC requires the use of special algorithm(s) and management of communication between network peers, which can be automated by computer software such as Swisscom Blockchain's SBX[1] shown in figure 3.



Cryptoasset Trading for OTC Professionals

The SBX is a high performance cryptoasset protocol interface for executing permissionless cross chain atomic swaps. Trade any asset completely peer to peer, with realtime physical settlement and no counterparty risk. The speed and security of each trade is regulated solely by the blockchain protocols running on your machine. The SBX is developed by Swisscom Blockchain.

Figure 3: *The SBX is software for trading cryptoassets OTC.*

4 Summary

The non-deliverable cryptoasset perpetual is a new financial product primitive which offers many benefits over traditional OTC and custodial trading methods. When deployed properly and used with appropriate infrastructure, stakeholders can realize significant benefits over using legacy technology which relies on trusted third parties. Blockchain technology is used to disintermediate third parties, reducing costs, counterparty risk, time to settlement, and overall complexity.

References

[1] Swisscom Blockchain AG. *SBX Webpage*. http://157.230.100.51/. 2019.

[2] Marco Avellaneda and Rama Cont. *Transparency in Over-the-counter Interest rate derivatives Markets*. https://www.isda.org/a/8eiDE/irmarkettransparency.pdf. 2010.

[3] Sean Bowe and Daira Hopwood. *Hashed Time-Locked Contract transactions*. https://github.com/bitcoin/bips/wiki/Comments:BIP-0199. 2017.

[4] *Colored Coins*. https://en.bitcoin.it/wiki/Colored_Coins. 2015.

[5] Blockstream Corp. *Elements: An open source, sidechain-capable blockchain platform*. https://elementsproject.org. 2019.

[6] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf.

[7] *Obyte Wiki*. https://wiki.obyte.org/Airdrop#Proving_ownership. 2016.

[8] Jon Peha and Sooksan Panichpapiboon. *Real-time secondary markets for spectrum*. http://ntrg.cs.tcd.ie. 2004.