ABCDE: A BlockChain Derivatives Exchange

Christopher Hannon

Abstract

Blockchain technology offers many promising improvements to existing computation systems. Many industries and sectors are seeing promising new proposals utilizing BlockChain to improve and capitalize on the decentralized nature of BlockChain including industries such as insurance, internet of things, finance, advertisement, entertainment, and many more. While many of these proposals and projects launched have seen early success, one of the largest barriers of entry is the lack of interoperability of Blockchain applications to their traditional counterparties. In this document we propose a Blockchain derivatives exchange (ABCDE) designed to be backwards compatible to the existing financial industry, while utilizing BlockChain properties of decentralization, immutability and transparency to take financial securities into the 21st century.

Specifically, this proposal overviews the design of a BlockChain exchange including advantages gained by Blockchain, interopperability to existing financial systems, and security designs and models. The ABCDE will support traditional derivatives such as futures, and options on underlying such as AAPL or GOOG marked to market daily, as well as new Blockchain based derivative contracts on ERC20 tokens which operate similarly to stock of decentralized BlockChain applications.

Summary

1 Introduction

Electronic currency has a long and seemingly fruitless history until recently with the emergence of Satoshi's Bitcoin Nakamoto [2008]. The Blockchain, the essence of electronic cryptocurrency, is poised to disrupt many domains including the financial industry, internet of things (IoT), energy, healthcare, utilities, and insurance to name a few. Blockchain gets its name from the consensus protocol of electronic currency that mediates transactions, and establishes a universally agreed upon transaction history. This document proposes Blockchain support for existing traditional financial derivatives as well as crypto derivatives. More abstractly, it addresses the following problem: How can we integrate existing financial markets into the cryptocurrency ecosystem? Specifically we propose a decentralized derivative exchange with support for contracts on traditional commodities through immutable programmable smart contracts on the Blockchain. Additionally, the exchange aims to support a new age of Blockchain securities built on top of cryptocurrency tokens of which can bleed the lines between stock and currency. Our Blockchain based platform leverages the advantages of the cryptographically secure Blockchain, purely transparent financial contracts, and the decentralized nature of the Blockchain, and applies them to traditional financial derivatives markets. The advantage of a Blockchain based exchange can be expressed in reduced fees due to programmable smart contracts, increased transparency through the universal public ledger that Blockchain offers making the ABCDE's orderbook completely public and auditable and facilitates. Additionally the turing-complete smart contract programming language reduces counterparty risk while the ABCDE is able to perform the same functions as traditional exchange components.

2 Motivation

We are proposing a Blockchain derivative exchange based in the cryptocurrency and Blockchain ecosystem with the following motivation.

- Maximize financial transparency and immutability.
- Financial decentralization
- Programmable automatic derivative contracts to reduce middlemen payments
- Cross-chain (cryptocurrency independent) order matching to maximize exchange volume

3 Components

- User interface
- Contract setup
- Orders matching contract
- External data source contract
- Clearinghouse contract

Figure 1 illustrates the interaction at a high level of the system components. The following sections go into details of the listed components.

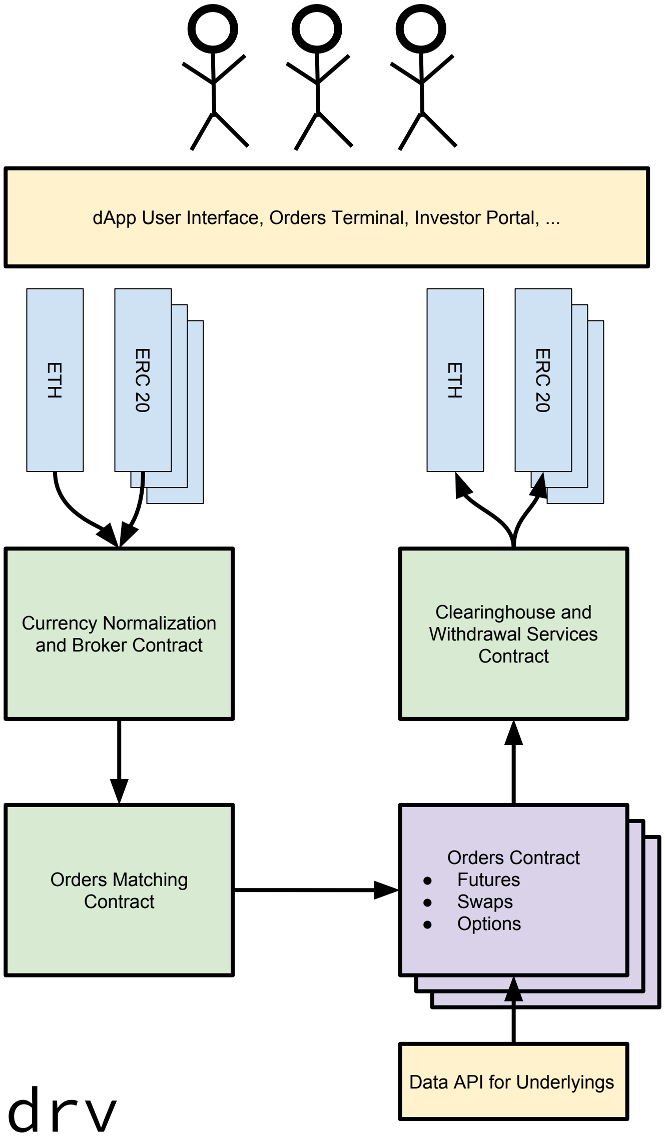
dApp User Interface, Orders Terminal, Investor Portal, ...
ETH
ERC 20
ETH
ERC 20
Currency Normalization and Broker Contract
Clearinghouse and Withdrawal Services Contract
Orders Matching Contract
Orders Contract
Futures
Swaps
Options
Data API for Underlyings
drv

Figure 1: The core components of ABCDE.

3.1 User Interface

The user interface for BCDE will have the following components:

- Registration: required for legal purposes
- Trader Terminal: will display information regarding derivative types, prices, volumes, etc.
- Investor Portal: the point of contact for ICO backers

A common misperception of Blockchain is its use for illicit behavior. However Public-Private key infrastructure, the underlying technology for Blockchain identities, is also widely used for authentication such as in PGP or internet certificates. In order to comply with regulations and restrictions ABCDE will utilize Know Your Customer (KYC), Anti-money Laundering (AML), and Counter-Terrorism Financing (CTF) through Cynopsis-Solutions. A registration process will enable us to authenticate users allowing us to comply with any regional regulations.

Additionally, perhaps the most important component for a trader is a terminal that would allow a user to place orders, and see information such as trade volume. The terminal would also provide a way for traders and investors to manage and settle their existing positions. The trader terminal provides the trader information on how to convert between currencies during contract settlement and creation which can add utility.

Finally, in order to maximize transparency of the exchange, an investor portal will allow the public to view and audit company operations, business directions, and request features.

3.2 Contract Setup

Because there are an ever expanding construction of new Blockchain services and tokens, and a large variety of popular cryptocurrencies, all underlying contracts are done with Ethereum.

3.3 Order Matching

All underlying derivative contracts are created with DRV tokens, thus orders are easier to match as there would be greater trade volume when compared to a separate order book for each currency. The implementation of the order matching contract is centralized, however the matching is done on top of the Ethereum blockchain which makes the verification process of the contract decentralized. Thus, the Blockchain can enforce transparency, immutability, fairness, and auditability properties which motivates our design of ABCDE. Additionally, all fees for matching are actually given(required) to the Blockchain miners which verify the previously mentioned properties.

3.4 External Data Source Contract

In order to settle a contract and to complete the margin changes, the spot price of the underlying asset is required. For both traditional derivatives and crypto derivatives, there will be a spot price required. Therefore the smart contract will need to have a connection to the data source an existing stock exchange or a cryptocurrency exchange in the latter case.

There also exists many other uses for integrating off-chain data into the Blockchain. For example, automatic insurance payouts in the case of natural disasters, connection IoT device actuation, and prediction markets such as Augur Peterson and Krug Sztorc [2014], and Gnosis Koppelmann et al. [2017] to name a few. Therefore this is not a new problem and there exists multiple solutions we can leverage.

The main challenge is then how to trust someone to inject these values into various smart contracts. *Oracles* are a name given for the party or service that is trusted to introduce external data into the Blockchain. The idea of a centralized trusted party is contrary to Blockchain however. There has been various work recently on solutions. One such proposal is called ChainLink Ellis et al. [2017] which is a decentralized oracle service. However even if a oracle service is distributed and decentralized there remains the challenge of trust in the service. Additionally the complexity associated with ChainLink increases the fees required. Another service, Oracalize **?** is a centralized data service that provides the ability to run authenticity proofs which the service can offload the trust to well-known and widely used services such as intel SGX, Android and Google's SafetyNet, Qualcomm's TEE, Amazons TLS Notery, and more. The authenticity can also be proven on the Blockchain which would allow the existing decentralized infrastructure to validate the authenticity and correctness of the input data. Since the data validation is critically important in financial contracts the design of our system revolves around verifying the data.

3.5 Clearinghouse Contract

While traditional financial clearing houses operate between two parties engaged in a contract for facilitating payments and reducing counterparty risk, our smart contract based system progmatically enforces counterparty payment which in turn reduces risk for .

While a centralized counterparty clearing is still needed in out platform, its roll transitions to picking up one end of the transaction if a party defaults on a margin call since all derivatives are marked to market daily.

TODO Does this reduces the need for centralized counterparty clearing. Or maybe just the risk?

4 Summary

4.1 Conclusion

This proposal highlights the research challenges of integrating financial derivatives into a Blockchain based system and provides motivation for such integration. It also overviews the existing state of connecting external data into the Blockchain, as well as connecting Blockchains together for more robust intracurrency exchange. The proposed research direction can be summarized as follows: investigation into cross-Blockchain contracts for the creation of a Intra-Blockchain currency market, the integration of off-chain data into the Blockchain to create transactions that utilize external data sources, and the modeling of proposed research problems and solutions through simulation.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Suspendisse accumsan magna est, quis elementum leo laoreet eu. Donec sollicitudin elit non massa venenatis, in viverra dolor sagittis. Maecenas ac justo pulvinar, consectetur mauris hendrerit, vulputate lacus. Etiam tristique sapien quis sem commodo, et eleifend tortor viverra.

References

S. Ellis, A. Juels, and J. Nazarov. ChainLink: A Decentralized Oracle Network. 09 2017.

M. Koppelmann, S. George, and F. Ernst. Gnosis. 2017.

S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

J. Peterson and J. Krug.

P. Sztorc. Truthcoin: Peer-to-Peer Oracle System and Prediction Marketplace. 2014.