

DESKTOP RESEARCH

A REVIEW OF CURRENT SMART CONTRACT PLATFORMS

July 9, 2016

Resilience Partners Ltd
Mo Afshar

Contents

1	Introduction	3
2	Blockchain and Bitcoin	4
3	Smart Contract Software Platforms	5
3.1	Ethereum	5
3.2	Eris industries	5
3.3	Codius	6
3.4	Counterparty	6
	References	7

1 INTRODUCTION

According to wikipedia Smart contracts are computer protocols that facilitate, verify, or enforce the negotiation or performance of a contract, or that make contractual clause unnecessary. They usually have a user interface and often emulate the logic of contractual clauses. They aim to provide security better than traditional contract law and reduce transaction costs associated with contracting.

The phrase "smart contracts" was coined by legal theorist computer scientist Nick Szabo and his description was: "A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs."

However as Josh Stark a lawyer and head of operations and legal at Ledger Labs has stated if we are talking about to identify a specific technology - code that is stored, verified and executed on a blockchain, we can call this definition "smart contract code". Other time if we are talking about specific application of that technology, as a complement or a substitute for legal contracts then we can name these smart legal contracts. By doing so we can easily answer questions like: what are the capabilities of a smart contract? By doing so we are able to answer these questions in a more suitable manner.

2 BLOCKCHAIN AND BITCOIN

Blockchain is a distributed database that maintains a continuously growing list of data records hardened against tampering and revision. It is a data structure that makes it possible to create a digital ledger of transactions and share it among distributed network of computers. It uses cryptography to allow each participant on the network to manipulate the ledger in a secure way without the need for a central authority. Once a block of data is recorded and stored it is very difficult to change or remove it, if for example someone wants to add to the data, the people in the network run algorithms to evaluate and verify the proposed transaction. If the majority agree then the transaction is valid and the new transaction will be approved and added.

The blockchain is seen as the main technical innovation of bitcoin, where it serves as the public ledger of all bitcoin transactions. Bitcoin is a form of digital currency created and held electronically, no one controls it. They are transferred directly from person to person via the net, without using a bank, which means the fees are much less, you can use it in any country, your account wont be frozen and there are no arbitrary limits which can affect you.

3 SMART CONTRACT SOFTWARE PLATFORMS

Below I will be looking at some of the software platforms that companies are using in conjunction with smart contracts.

3.1 Ethereum

According to www.ethereum.org Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference. The apps run on a custom built blockchain as this enables developers to create markets, store registries of debts or promises, move funds all without a middle man. Using this platform anyone can set up a node that replicates the necessary data for all nodes to an agreement and be compensated by user and app developers. This allows user data to remain private and apps to be decentralized.

Ethereum introduces Mix IDE for the blockchain era. Mix is a full IDE for the Ethereum network. You are able to develop and write smart contracts and closely inspect the compiled code. Furthermore, Ethereum introduces Solidity which is a high level language whose syntax is similar to that of Javascript and it is designed to compile code for the Ethereum Virtual Machine. You are able to create contracts for voting, multi signature wallets and more. An extensive documentation can be viewed at: <https://solidity.readthedocs.io/en/latest/index.html>

3.2 Eris industries

Eris is a free software that allows you to build your own secure, low-cost, run-anywhere application using blockchain and smart contract technology. Eris enables you to Install the complete platform and deploy your own custom blockchain or connect to an existing one to develop sophisticated financial or legal applications. You can also build and run the application using smart contract templates and a simple, web-based user interface. An extensive documentation can be viewed at: <https://docs.erisindustries.com/>

The documentation includes a wide variety of tutorials explaining the Eris Stack, Eris Platform and its components, Using Eris such as interacting with your own smart contracts and more in depth tutorials such as writing your own smart contracts.

3.3 Codius

Codius is an open hosting protocol, it makes it very easy to upload program, whether you want it to run on one host or thousands. It lets you turn your service into a peer-to-peer network and it can work with decentralized apps. Furthermore, when two people transact, they could write the terms of their transaction into code but neither of them might trust the other to run it, Codius allows a third party to run it and attest to the integrity of the exact code it received.

Smart contracts run on Codius can hold assets in one or multiple math-based distributed ledgers, such as Bitcoin and Ripple, it can collect information from any source connected to the Internet and be written in standard programming languages. Depending on the security model required for a particular smart contract, the contracting parties can select the host. An extensive documentation can be viewed at: <https://codius.org/docs/using-codius/getting-started>

3.4 Counterparty

The Counterparty protocol is open source and extensively tested platform allowing users to create and trade any kind of digital token, it also enables you to write specific digital agreements (smart contracts) and execute them on the Bitcoin blockchain.

By implementing Ethereum's entire smart contract platform Counterparty enables users to write Turing Complete smart contracts into the Bitcoin blockchain and execute those in a completely decentralized manner. Counterparty supports both the languages Solidity and Serpent which can be used to write smart contracts. An extensive documentation can be viewed at: <http://counterparty.io/docs/>

REFERENCES

<https://en.wikipedia.org/wiki/Smart_contract> [Accessed July 2016]

Josh Stark 2016. *making sense smart contracts*, [online] Available at: <<http://www.coindesk.com/making-sense-smart-contracts/>> [Accessed July 2016]

Wikipedia *Blockchain (database)* [online] Available at: <[https://en.wikipedia.org/wiki/Blockchain_\(database\)](https://en.wikipedia.org/wiki/Blockchain_(database))> [Accessed July 2016]

Ethereum [online] Available at: <<https://www.ethereum.org/>> [Accessed July 2016]

Codius [online] Available at: <<https://codius.org/>> [Accessed July 2016]

Counterparty [online] Available at: <<http://counterparty.io>> [Accessed July 2016]