Smart Contracts

Contents

1. Overview

Smart contracts present a way of encoding software into a blockchain transaction. In doing so, the software becomes available for execution by other peers on the network, and can act as a node would to make transactions, create contracts, or hold a balance.[1] In practical applications, a secondary currency is traded to handle processing of smart contracts. In the Ethereum model this currency is referred to as Gas. [2] This is only a brief primer summarizing the current state of this technology, so please be sure to peruse the citations for more detailed information, or contact us by email to request a deep dive whitepaper.

2. Background

The premise of a smart contract actually predates blockchain. In 1996, Nick Szabo proposed a peer-to-peer network for validating events and processing requests in "Smart Contracts: Building Blocks for Digital Free Markets". His primary definition of a true smart contract is that one which is robust against both naïve and sophisticated attacks, meaning that the system must be self-securing and distributed. [1]

2.1. The Four Objectives

Szabo outlined four constraints which must be satisfied to create a decentralized trust system which still hold true today.

2.1.1. Observability

All concerned parties must be able to view the contract in its entirety and monitor the execution thereof.

2.1.2. Verifiability

All parties must be able to verify participation and execution of the contract.

2.1.3. Privity

Only relevant information should be made public in order to maintain the informational integrity of the participants.

2.1.4. Enforceability

All parties must have a pre-defined recourse in the event of a breach of contract, and some form of trusted third party must be available to enforce the action.

2.2. Blockchain Smart Contracts

In Ethereum, smart contracts can be encoded into the common blockchain. This application satisfies all four of Szabo's requirements by storing both the value and the application logic in a common forum, and using private keys to secure access and information. The Ethereum platform has provided a new network which is designed to act as a payment trust system for smart contracts and distributed applications. [3]

3. Technical Review

Because Smart Contract is a term for a procedure and not a particular technology, the true nature of the contract can be hard to define.

> *"There exists no universally accepted definition of a smart contract. Generally, smart contracts are computer protocols that implement the terms of a negotiated contract in a self-executing manner." [5]*

Despite this, there are a set of technologies currently being applied, and so the true limitation of the field can be understood from an analysis of these underlying constructs.

3.1. Automatic Evaluation & Execution

In a traditional contractual arrangement, the rules are set, but the execution must be triggered by a participating party. In a smart contract, execution is triggered by an impartial factor such as a combination of external data from reliable sources. [1]

3.2. Escrow Capability

Key to any contract is the ability to hold collateral and process the exchange of goods and services. Smart contracts present a means of automating this component of a contractual obligation and linking execution to commonly trusted sources such as stock exchange data, account balances, or even sports events. [3]

3.3. Multiple Signature Authentication (MultiSig)

Hashing systems allow participating parties to sign an event with a private key, which is never displayed publicly. This reduces fraud by providing a system which is nearly impossible to subvert. [7]

3.4. Network Scale and Distribution (Immutability)

In the blockchain context, smart contracts are privately signed and publicly noted, so once a contract is signed by all parties it cannot be changed without control over more then 50% of the network. [8] (See Glossary: 51% Attack)

For a smart contract to be truly secure, it is necessary that the execution be processed simultaneously across a wide network of devices. This not only reduces the risk of fraud, but also prevents attacks such as ransomware from preventing access.

4. Present Applications

Transparency and trust are at the core of all businesses, so naturally the adoption and application of smart contracts has already been rapid. Cap Gemini Consulting Group is currently predicting widespread adoption by 2020. [3] While smart contracts will never fully replace the legal system, they provide a means of monitoring complex systems with high degrees of granularity, and pre-authorizing responses to system events.

4.1. Financial Technology

Due to the contractual nature of most financial technologies, smart contracts, specifically when combined with a blockchain, have a number of applications. This is just a brief example, but please see our upcoming release "Blockchains for Financial Services" for more information.

4.1.1. Simplified Escrow Accounting

The most obvious and perhaps most powerful quality of a smart contract on a blockchain such as Ethereum is that it can hold value without any autonomy of it's own. This means that two parties can pay into a fund, and the contract will execute per the agreed-upon rules without any possibility of interference.

4.1.2. Investments / Options

In banking, an option refers to an agreement to be evaluated on a predefined date. One example is the case where an investor believes a stock will decrease in value and offers to sell another investor the stock at a lesser value in the future, with the hope of making a return on the margin. Presently these options are handled by large brokerages with major overhead costs.

In smart contracts, any two members of the blockchain can generate an option contract in minutes. The contract can pull data from a particular stock exchange on the public internet, and execute the value transfer as necessary. [16] Likewise smart contracts can also be applied to define ownership of a corporation, which can reduce overhead related to initial public offerings of stocks. [3]

4.1.3. Insurance

Smart contracts have the potential to expedite processing and payment of claims, as well as to handle premiums and manage funds. [3]

In addition, several firms have already launched ICOs for new currencies which will act as insurance utilities on the public blockchain. [15]

4.1.4. Total Decentralization

The final, and quite substantial, benefit of smart contracts for finance is that they are stored in the public blockchain record, meaning that they cannot be lost without the entire network being subverted. Since financial industry assets are essentially a matter of public record and not able to be physically protected in any way, the blockchain and contracts built on it present a wide range of opportunities for improvement to asset security.

4.2. Government

In the government sector, smart contracts have the potential to reduce fraud and increase transparency through the use of signing keys and blockchain ledgers.

The Cook County of Chicago has recently (May 2017) been investigating the use of blockchain as a title and deed management system.[10] Under this orientation, title transfers, property taxes, and any other related processes would be handled with smart contracts. The key in this case is that the signing keys in each event are able to be tracked over the history of the system, and records cannot be updated once they are committed. This process ensures that the entire public record is open and transparent.

4.3. Healthcare

Privacy is a primary concern for healthcare providers and insurers alike. Separately, detailed and accessible medical records are also key to improving quality of care. This contrast provides a wide realm of possibilities for smart contracts that control access to information, as well as those that trigger transactional events in exchange for services. [11]

4.4. Logistics

Logistics and supply chain management provide additional industries where transparency and automation have major potential. Supply chain adoption of blockchain has already been growing due to the benefits of signing keys and record transparency, but additional smart contract services are now being developed to automate notification events from shipping manifests and weigh-in station recording. In short, bringing all of the data into a single platform means that the oversight of business processes and even payment processing can be built into the contracts themselves. [12]

4.5. Manufacturing

The future of the internet of things presents wide ranging applications for smart contract technology. Internet of things devices have internal processing power, as well as data gathering capabilities, which makes them ideal nodes for a blockchain network. Through connecting wide networks of such devices it is possible not only to ensure data redundancy and overall connectivity, but to also built in live time management of control systems based on first hand data. [13]

A number of firms are already developing systems for recording everything from maintenance information to production output to create smart contracts which can execute replacement orders and even respond to supply chain disruptions. [14]

4.6. Consumer Goods

In addition to the potential for the internet of things in manufacturing, there now exist a wide range of devices such as smart fridges, appliances, and entertainment systems which now track a wide range of data and can be authorized to make decisions. Key signing and authorization present a substantial increase in security as homeowners begin to integrate automated products into their lives.

Citations

1. Nick Szabo, “Smart Contracts: Building Blocks for Digital Markets”, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

2. Ethereum Whitepaper, https://coss.io/documents/white-papers/ethereum.pdf

3. CapGemeni Consulting, “Smart Contracts in Financial Services: Getting from Hype to Reality”, https://www.capgemini-consulting.com/resource-file-access/resource/pdf/smart-contracts.pdf

4. Quinn DuPont, University of Toronto, “Experiments in Algorithmic Governance: A history and ethnography of ‘The DAO’, a failed Decentralized Autonomous Organization”, http://iqdupont.com/assets/documents/DUPONT-2017-Preprint-Algorithmic-Governance.pdf

5. Jenny Cieplak and Simon Leefatt, “SMART CONTRACTS: A SMART WAY TO AUTOMATE PERFORMANCE”, https://perma.cc/EUT6-RL6P

6. Alan Cohn, Travis West, & Chelsea Parker, “SMART AFTER ALL: BLOCKCHAIN, SMART CONTRACTS, PARAMETRIC INSURANCE, AND SMART ENERGY GRIDS”, https://perma.cc/TY7W-Q8CX

7. Francisco Javier Buenasmananas Domıguez, Luis Hernandez Encinas, “Digital identity-based multisignature scheme implementation”, http://digital.csic.es/bitstream/10261/42901/1/infocomp_2011_2_40_10176.pdf

8. Alex Potanin, Johan Ostlund, Yoav Zibin, and Michael D. Ernst, “Immutability”, https://homes.cs.washington.edu/~mernst/pubs/immutability-aliasing-2013-lncs7850.pdf

9. Gideon Greenspan, “The Blockchain Immutability Myth”, https://www.coindesk.com/blockchain-immutability-myth/

10. John Mirkovic, Cook County Recorder of Deeds, May 30, 2017, “BLOCKCHAIN PILOT PROGRAM FINAL REPORT”,

http://cookrecorder.com/wp-content/uploads/2016/11/Final-Report-CCRD-Blockchain-Pilot-Program-for-web.pdf

11. RJ Krawiec, Dan Housman, Mark White, Mariya Filipova, Florian Quarre, Dan Barr, Allen Nesbitt, Kate Fedosova, Jason Killmeyer, Adam Israel, Lindsay Tsai, Deloitte Consulting, "Blockchain: Opportunities for Health Care", https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-blockchain-opportunities-for-health-care.pdf

12. Cognizant, "Blockchain's Smart Contracts: Driving the Next Wave of Innovation Across Manufacturing Value Chains", https://www.cognizant.com/whitepapers/blockchains-smart-contracts-driving-the-next-wave-of-innovation-across-manufacturing-value-chains-codex2113.pdf

13. Arshdeep Bahga, Vijay K. Madisetti, Georgia Institute of Technology, "Blockchain Platform for Industrial Internet of Things", https://file.scirp.org/pdf/JSEA_2016102814012798.pdf

14. IOTA.org, https://iota.org/

15. Joshua Davis, "PEER TO PEER INSURANCE ON AN ETHEREUM BLOCKCHAIN", http://dynamisapp.com/whitepaper.pdf

16. EBA Working Group on Electronic Alternative Payments, "Applying cryptotechnologies to Trade Finance", https://www.abe-eba.eu/downloads/knowledge-and-research/EBA_May2016_eAPWG_Applying_cryptotechnologies_to_Trade_Finance.pdf