CrushCrypto

# What is a smart contract?

## Educational Series

August 31, 2018

# Introduction

- First implemented in 2009 with the release of Bitcoin, a blockchain is a virtual ledger of data that functions as a distributed network.
- Computers across the globe called nodes store and update the ledger by reaching a consensus with all other nodes, meaning the data on the ledger is secured without needing third party verification.
- The Bitcoin blockchain is used as a ledger containing all wallet balances and transactional data, keeping records that are secure and immutable – effectively impossible to change once they exist.

# Overview

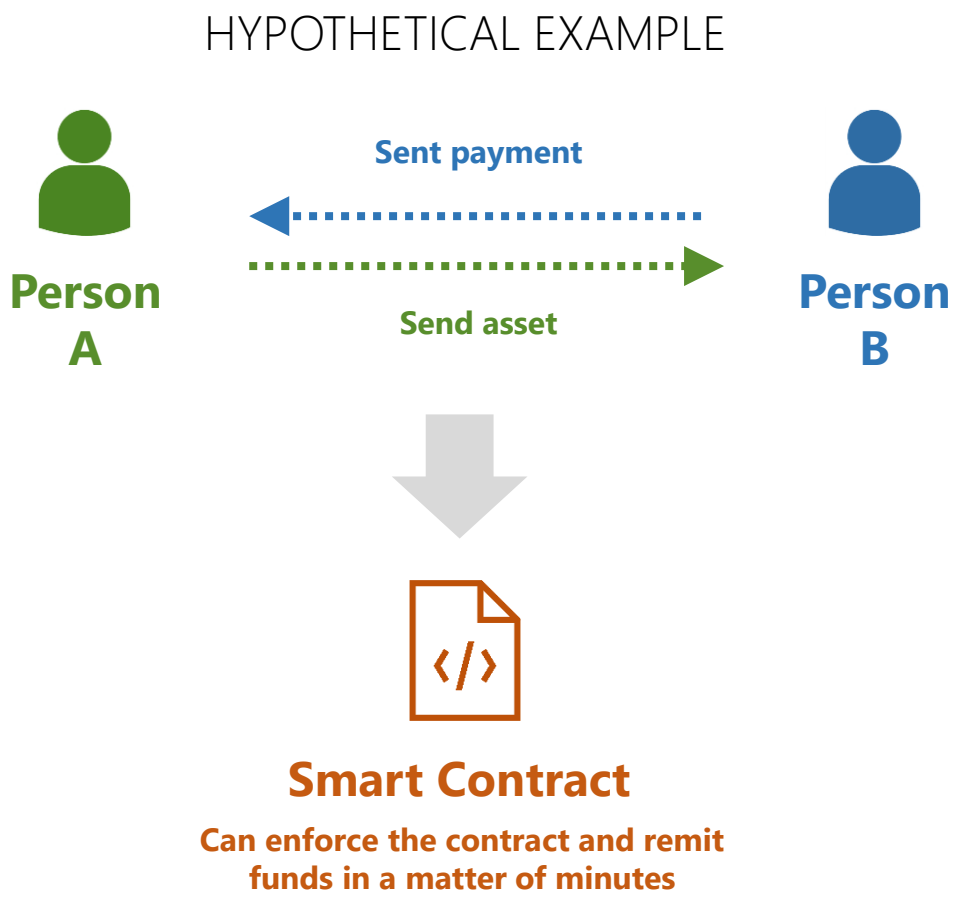
- A smart contract is **a piece of code stored on the blockchain that reads and writes data and is triggered by blockchain transactions**.
- Like a bitcoin transaction, the code for a smart contract is immutable once it's on the blockchain and can never be altered by a third party. The code will run exactly as programmed, forever (if the blockchain it's on still exists), which is a benefit and a weakness.

TRADITIONAL VS. SMART CONTRACTS

| Traditional Contracts | Smart Contracts |
|---|---|
| Paper / physical document | Software protocol |
| Requires trust in a third party (brokers, lawyers) | Trustless and no intermediaries |
| Days to weeks | Minutes |
| Higher administration and service costs | Cheaper and less prone to human error |
| Manual payment of funds | Automatic remittance |
| Escrow required | Escrow is not necessarily required |
| Physical signature | Digital signature |

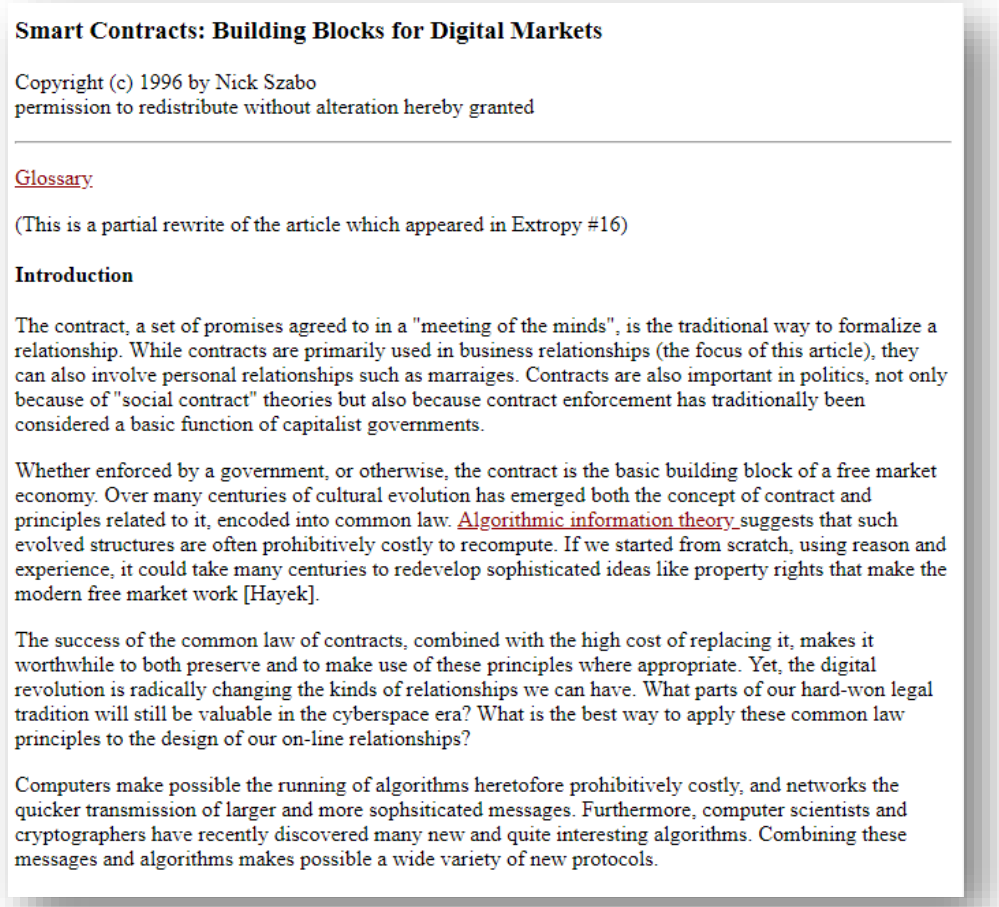
# Overview (continued)

- Example: A program receives an asset from Person A, waits for a condition, then automatically decides if the asset should be sent to person B or refunded to person A. This specific case could be used for betting or online payments as an automated escrow service.
- Smart contracts can be used to create decentralized applications (DApps) with a front end that allows users to interact with the smart contract directly from their wallet.
- web3, a collection of JavaScript libraries allowing for the connection to blockchain nodes, has made DApp development easier and more widespread.



# History

- Nick Szabo, a scholar and cryptographer, realized that a decentralized ledger could be used for self-executing, digital contracts. He announced his discovery in a 1994 paper called Smart Contracts, where he outlines his idea, digital cash protocols, and economic incentives.
- In 1996, he released a more detailed piece called Smart Contracts: Building Blocks for Digital Markets where he discusses traditional societal contracts, contracts embedded in the world, attack vectors, contract design, cryptographic building blocks, smart property, and more.



**Smart Contracts: Building Blocks for Digital Markets**

Copyright (c) 1996 by Nick Szabo
permission to redistribute without alteration hereby granted

---

Glossary

(This is a partial rewrite of the article which appeared in Extropy #16)

**Introduction**

The contract, a set of promises agreed to in a "meeting of the minds", is the traditional way to formalize a relationship. While contracts are primarily used in business relationships (the focus of this article), they can also involve personal relationships such as marraiges. Contracts are also important in politics, not only because of "social contract" theories but also because contract enforcement has traditionally been considered a basic function of capitalist governments.

Whether enforced by a government, or otherwise, the contract is the basic building block of a free market economy. Over many centuries of cultural evolution has emerged both the concept of contract and principles related to it, encoded into common law. Algorithmic information theory suggests that such evolved structures are often prohibitively costly to recompute. If we started from scratch, using reason and experience, it could take many centuries to redevelop sophisticated ideas like property rights that make the modern free market work [Hayek].

The success of the common law of contracts, combined with the high cost of replacing it, makes it worthwhile to both preserve and to make use of these principles where appropriate. Yet, the digital revolution is radically changing the kinds of relationships we can have. What parts of our hard-won legal tradition will still be valuable in the cyberspace era? What is the best way to apply these common law principles to the design of our on-line relationships?

Computers make possible the running of algorithms heretofore prohibitively costly, and networks the quicker transmission of larger and more sophsiticated messages. Furthermore, computer scientists and cryptographers have recently discovered many new and quite interesting algorithms. Combining these messages and algorithms makes possible a wide variety of new protocols.

# History (continued)

- Nick Szabo also mentions the objective of smart contract design is “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.”
- Szabo’s discovery of smart contracts was ahead of its time, as it could not be successfully implemented until the invention of a secure distributed ledger technology. The invention of blockchain was the first step towards smart contract development, while the release of Ethereum 6 years later is what popularized the idea.

# Benefits

- **Immutability**: The code of a smart contract is going to run exactly as programmed for as long as the blockchain is running. This is a benefit because people can now create truly censorship resistant, decentralized applications with no possibility of server downtime.
- **Autonomy**: Once certain conditions are met for a smart contract; its programmed functions will automatically execute. User input is not required, and data or assets can be automatically transferred or withheld.
- **Open source**: By nature of the blockchain, the code of all smart contracts is open source and available for anyone see. The transparency allows for community-based auditing and makes it difficult for anyone to hide malicious code in an application.
- **Disintermediation**: Smart contracts can remove a middleman from transactions in numerous industries.

# Weaknesses

- **Immutability**: Immutability is also a weakness of smart contracts as there is always potential for code to have errors. If a smart contract with a bug is deployed to the blockchain, it can never be fixed – unlike traditional programs. Since smart contracts often deal with assets, one error can cost millions of dollars.
- **Legal issues**: Considering smart contracts are a relatively new technology, there is no legal precedent for what they represent or how to handle issues. Hopefully there will be more clarity on the legal front soon, but the foreseeable future is uncertain.
- **Costs**: Storing data on the blockchain is expensive. Every computational task is run by each node on the network and requires data on the blockchain, meaning the costs can pile up quickly for a smart contract. Technologies such as IPFS are being developed to address this, but in the current state it is still a serious issue.

# Potential use cases

- There are lots of different uses for smart contract or programmable money that sets out the rules for payout. We are still at the early development stage for smart contracts or decentralized applications, so it is likely that the use cases that will eventually generate traction is still not yet discovered.
- Potential use cases include: digital ID, voting, supply chains, healthcare, real estate, ticketing, music/art licensing, etc.
- The above are examples of how smart contract could be used, not every method has been tested yet.

# Smart contract platforms

- Although Bitcoin has the potential to support smart contracts, it was not until the release of Ethereum in 2015 that the idea become popularized. The Ethereum Foundation created a Turing complete smart contract language called Solidity that made smart contracts easier to write and understand for developers.
- As of August 20, 2018, there are 1,793 DApps released on the Ethereum main-net, with 10,600 daily users, 78,400 daily transactions, and 13,700 ETH in 24hr volume.
- Other smart contract platforms such as NEO, Stellar, EOS, Cardano, and more have gained traction in recent years. Each has unique features, the most significant being different consensus mechanisms – some are focused on decentralization while others are more centralized but have faster transactions.

CrushCrypto