More on atomic swaps and smart contracts

crypto251.0 Cryptocurrency and the Smileycoin

Gunnar Stefansson (editor)

November 29, 2020

The smart contract

Back to Nick Szabo

(**Copyright (c) 1994 by Nick Szabo**)

"A smart contract is a computerized transaction protocol that executes the terms of a contract."

With objectives:

"The general objectives of smart contract design 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, arbitration and enforcement costs, and other transaction costs[1]."

and from Wikipedia:

Implementations

https://en.wikipedia.org/wiki/Smart_contract

Byzantine fault-tolerant algorithms allowed digital security through decentralization to form smart contracts. Additionally, the programming languages with various degrees of Turing-completeness as a built-in feature of some blockchains make the creation of custom sophisticated logic possible.[4][12]

Notable examples of implementation of smart contracts include the following:

Smart contracts: Misunderstandings

- *Example of incorrect statement (more than one error here):*
  - *ethereum replaces bitcoin's more restrictive language (a scripting language of a hundred or so scripts) and replaces it with a language that allows developers to write their own programs – https://www.coindesk.com/information/ethereum-sm*
- *Note that*
  - *The Bitcoin scripting language* ***is limited*** *but so are all programming languages.*
  - *Developers can write their own programs in the Bitcoin scripting language!!*
  - *A more flexible language gives more flexibility :-)*
  - *A more flexible language is often more error-prone and less secure*

Tools for atomic swaps

Examples of tools and discussions

- Very good description with tool-box, Decred: `https://blog.decred.org/2017/09/20/On-Chain-Atomic-Swaps/`

"These tools were built for those who ... have ... transaction script and OP_CLTV support"

- Detailed example based on the Decred tools: `https://hackernoon.com/so-how-do-i-really-do-an-atomic-sw`

And recall that **"these tools do not address the issue of order book management"**

- for which you need Lightning or other tool for announcements of intent etc

Which coins are ready?

Nice overview: `https://swapready.net/`

Lightning

See https://www.forbes.com/sites/ktorpey/2018/03/15/bitcoins-h