Academisch Schrijven opdracht 3

Yorick van Pelt - s4503678

Paper

Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”

Zie ook bijlage.

Doelgroep

De doelgroep van dit artikel was aanvankelijk een groep cryptografen (dit paper verscheen voor het eerst op een cryptografie mailing list). Nu bitcoin echter een stuk groter is geworden, is het paper echter ook prima geschikt voor mensen die meer willen weten over bitcoin. Er wordt niet te veel jargon gebruikt en onbekende concepten worden abstract uitgelegd zodat een lezer niet bekend hoeft te zijn met de implementatie.

Boodschap

Dit paper beschrijft een systeem om decentraal valuta te organiseren, en vergelijkt het met eerdere systemen en de huidige werkelijkheid.

Effectiviteit

De inleiding beschrijft de context van het werk en de problemen die worden opgelost met dit systeem. De informatiedichtheid is erg hoog, maar het verhaal is vrij onsamenhangend. Er zijn twee primaire problemen met het huidige systeem, maar de overgang ertussen zit midden in een zin. Informatie wordt wel herhaald, maar vaak niet op de plek in de zin die de lezer verwacht. De schrijver kan niet wachten met het introduceren van nieuwe concepten, maar er wordt wel gelet op het zetten van context.

Een interessant aspect van dit schrijfwerk is dat de schrijver anoniem wilde blijven, en zich waarschijnlijk bewust was van het begip ‘stylometrie’; de schrijfstijl

wordt hierbij vergeleken met andere werken om zo de schrijver te identificeren. Verscheidene mensen hebben al geprobeerd om dit toe te passen, maar de auteur is nog niet met zekerheid gevonden. Het kan dus heel goed zijn dat dit artikel onnatuurlijk geschreven is om mensen voor de gek te houden.

De samenvatting is duidelijk als laatst geschreven, en bevat 1 of twee zinnen per hoofdstuk. Het hoofd-idee zal niet meteen duidelijk worden, maar de scope en toegepaste technieken zeker wel. Dit stuk is dus niet geschreven als een lopend stuk tekst; lezers krijgen echter een goed idee van de inhoud van dit paper.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.