Privacy & Identity Lab

Blockchain & Identity
(Why you should avoid the blockchain like the plague)

Jaap-Henk Hoepman
Radboud University
jhh@cs.ru.nl / @xotoxot

"The" blockchain does not exist

#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$14,869,611,619	$922.64	16,116,287 BTC	$117,128,000	3.68%	
2	Ethereum	$941,714,624	$10.69	88,109,527 ETH	$9,586,770	1.20%	
3	Ripple	$248,913,371	$0.006754	36,855,961,691 XRP *	$638,032	0.48%	
4	Litecoin	$193,138,772	$3.91	49,435,806 LTC	$3,150,530	1.20%	
5	Monero	$167,019,641	$12.11	13,789,714 XMR	$3,655,160	1.27%	
6	Ethereum Classic	$121,132,397	$1.38	88,070,028 ETC	$6,549,660	17.87%	
7	Dash	$106,400,325	$15.11	7,041,296 DASH	$2,065,660	-1.48%	
8	MaidSafeCoin	$54,399,063	$0.120205	452,552,412 MAID *	$401,398	2.58%	

Bitcoin: the first blockchain

- **Invented by 'Satoshi Nakamoto' in 2008**
- **Satoshi's goals**
  - Irreversible, immutable, transactions
  - Lower transaction costs
- **Satoshi's insight**
  - Secure, peer-to-peer, transaction processing is possible
  - Using 'proof-of-work' to create distributed **consensus**

Bitcoin:
A Peer-to-Peer Electronic Cash System
Satoshi Nakamoto
October 31, 2008
www.cryptoresearch.co.uk

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

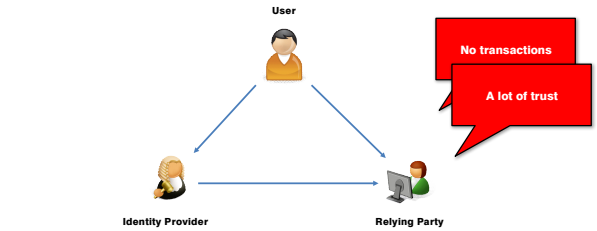
Why you should avoid blockchain like the plague

- **More centralised than you think**
  - Four largest (>75%) mining pools are from China
  - Developers decide (cf. Ethereum and Ethereum classic fork): transactions *are* reversible
  - *"fundamentally incompatible with democratic society"*
- **Poor scalability**
  - Max 7 transactions per second (cf 7000 for creditcards)
  - Blockchain grows rapidly (60 GB, 2x size of 2015)
- **Unsustainable: Mining consumes enormous amounts of energy**
  - 1tx can power 1 US household for a week (2017)
- **Incentives necessary**
  - To guarantee progress and keep nodes honest
- **Not privacy friendly**
  - Though altcoins that are exist
- **Security poorly understood**
  - Especially for "Proof-of-stake"
- **Still a middleman**
  - Consolidates centralized power of corporations and governments

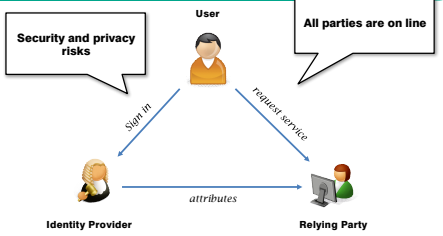
So should you use a blockchain?

- **Only when**
  - The order of (trans)actions matters
  - And there is no central authority you can trust
- **Otherwise**
  - Use a peer to peer network,
  - Or a distributed database, or …

So… what about identity?



Traditionally, a lot of stuff is wrong…



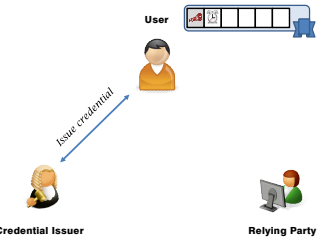
Self-sovereign identity?

- **Attribute based credentials!**

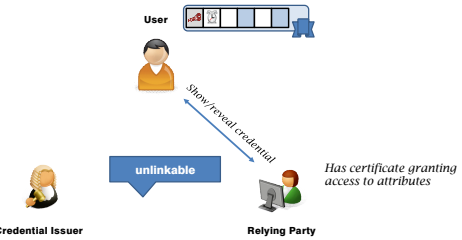
IRMA

https://privacybydesign.foundation

eID: ABC based : Issuing



eID: ABC based : showing



Questions / Discussion

[Monty Python's Argument Clinic sketch]

jhh@cs.ru.nl