Faculty of Law, Economics and Finance of the University of Luxembourg

Competing Claims to Crypto-Assets

Dr. Jannik Woxholth
ADA Chair in Financial Law (Inclusive Finance)

ada

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère des Affaires étrangères
et européennes

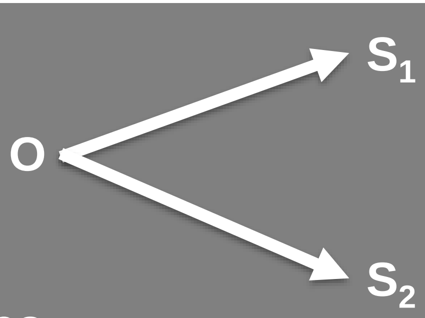
uni.lu
FACULTY OF
ECONOMICS
AND FINANCE

Introduction

O = Owner (title holder)
S = Successor
RO = Real Owner (real title holder)
AO = Apparent Owner (apparent title holder)

Competing claims

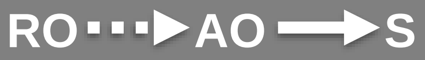
“Double spending” problem



Examples:

- O sells the same asset first to S_1 and then to S_2
- O goes into bankruptcy proceedings and transfers assets to S_2 to shield them from creditors (S_1)

“Apparent owner” problem



Examples:

- AO steals assets from RO and transfers them to S
- RO’s assets are somehow registered in the name of AO who goes into bankruptcy proceedings

Table of content

I. Introduction

II. Competing claims unsolved by technology

A. What problem did Nakamoto set out to solve?
B. Remaining issues unaddressed by technology
C. Competing claims *facilitated* by technology

III. Competing claims unsolved by law

A. Property rights
B. The *nemo dat* rule for on-chain transfers
C. Registration, possession, and negotiability

IV. Three principles to address competing claims

A. Acknowledge property rights
B. Establish negotiability
C. Reduce cost of enforcement

V. Conclusion

Table of content

I. Introduction

II. Competing claims unsolved by technology

- **A. What problem did Nakamoto set out to solve?**
- **B. Remaining issues unaddressed by technology**
- **C. Competing claims *facilitated* by technology**

III. Competing claims unsolved by law

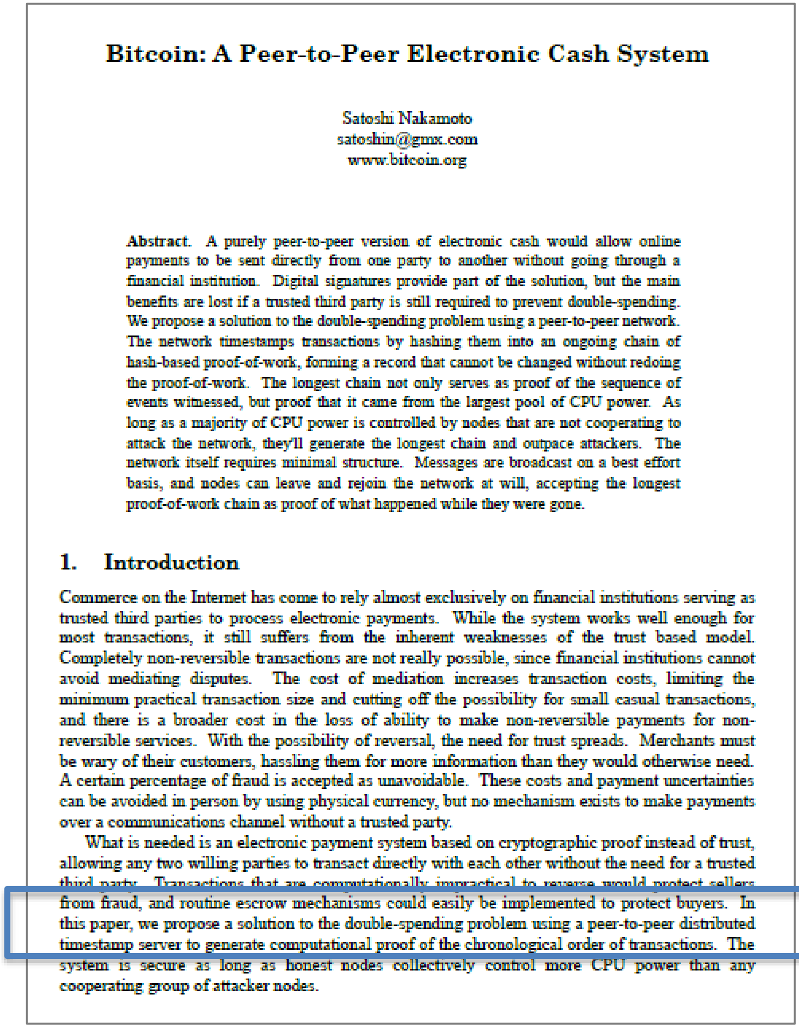
- A. Property rights
- B. The *nemo dat* rule for on-chain transfers
- C. Registration, possession, and negotiability

IV. Three principles to address competing claims

- A. Acknowledge property rights
- B. Establish negotiability
- C. Reduce cost of enforcement

V. Conclusion

A. What problem did Nakamoto set out to solve?



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.

> “In this paper, we propose a solution to the double-spending problem …”

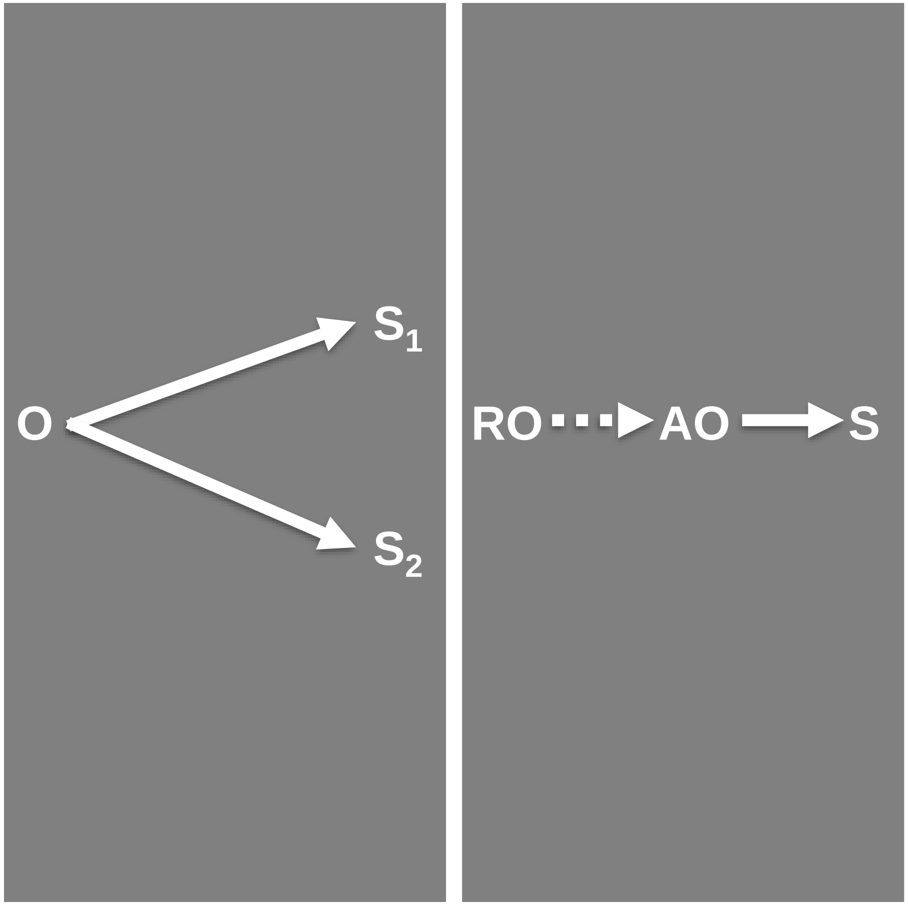
SOURCE: S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System» (2008)

B. Remaining issues unaddressed by technology

O = Owner
S = Successor
RO = Real Owner
AO = Apparent Owner

Type of problem

Double spending | Apparent owner



B. Remaining issues unaddressed by technology

Type of claim	Transfers	E.g., sale, gift, or succession
	Creditor claims	Individual or collective creditor claims, e.g., insolvency

B. Remaining issues unaddressed by technology

		Type of problem	
		Double spending	Apparent owner
Type of claim	Transfers	(✓)	✗
	Creditor claims	✗	✗

DLT provides a solution ✓

DLT provides no solution ✗

C. Competing claims *facilitated* by technology

DLT side-effects:

- Cyber-attacks (theft)
- Anonymous accounts:
  - Transferor lacks legal capacity?
  - Hidden from creditors?
  - What jurisdiction?
- Designed to be immutable

$1.9B

worth of crypto-assets stolen or obtained by criminals in 2020*

* https://www.securitymagazine.com/articles/94627-19b-in-crypto-currency-stolen-by-hackers-last-year

Table of content

I. Introduction

II. Competing claims unsolved by technology

A. What problem did Nakamoto set out to solve?
B. Remaining issues unaddressed by technology
C. Competing claims *facilitated* by technology

III. Competing claims unsolved by law

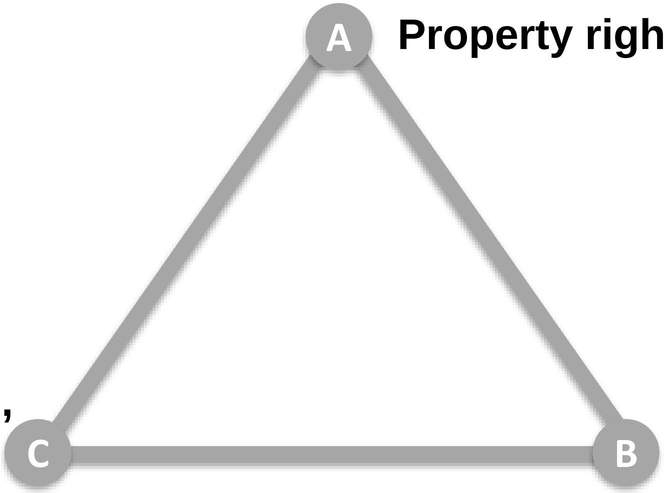
A. Property rights
B. The *nemo dat* rule for on-chain transfers
C. Registration, possession, and negotiability

IV. Three principles to address competing claims

A. Acknowledge property rights
B. Establish negotiability
C. Reduce cost of enforcement

V. Conclusion

Comparative legal analysis



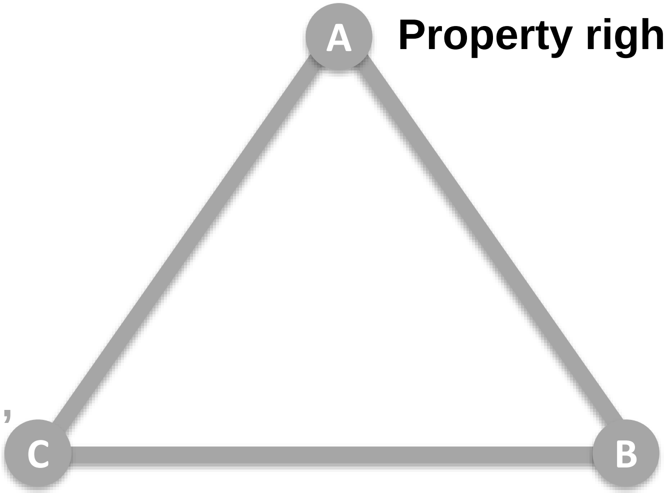
Property rights

Registration, possession, and negotiability

The *nemo dat* rule for on-chain transactions

A. Property rights

- Most crypto-assets: contractual rights / things in action
- Typical cryptocurrency: neither corporeal nor contractual – can they be owned at all?
- Typically no ownership in data / information

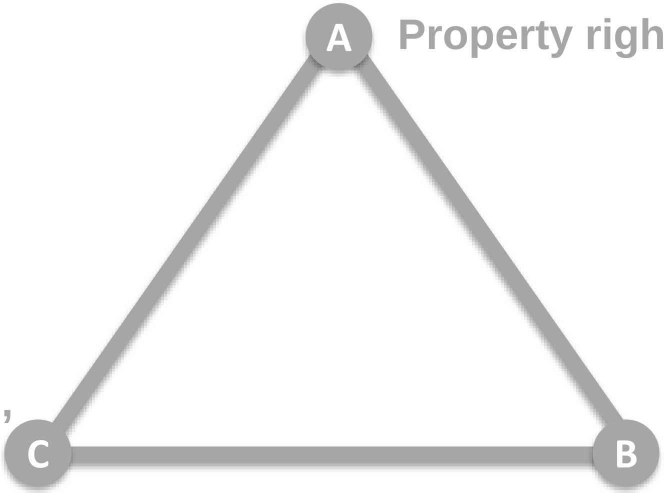


Property rights

The *nemo dat* rule for on-chain transactions

Registration, possession, and negotiability

B. The *nemo dat* rule for on-chain transfers



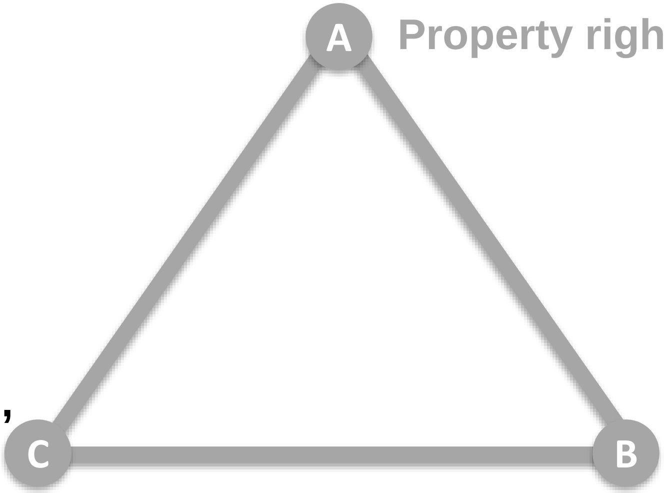
Property rights

Registration, possession, and negotiability

The *nemo dat* rule for on-chain transactions

- Starting point: *nemo dat quod non habet / prior tempore, potitur jure*
- Assumption: multiple parties have competing claims in the same asset
- Crypto-assets: unspent transaction output (UTXO)

C. Registration, possession, and negotiability



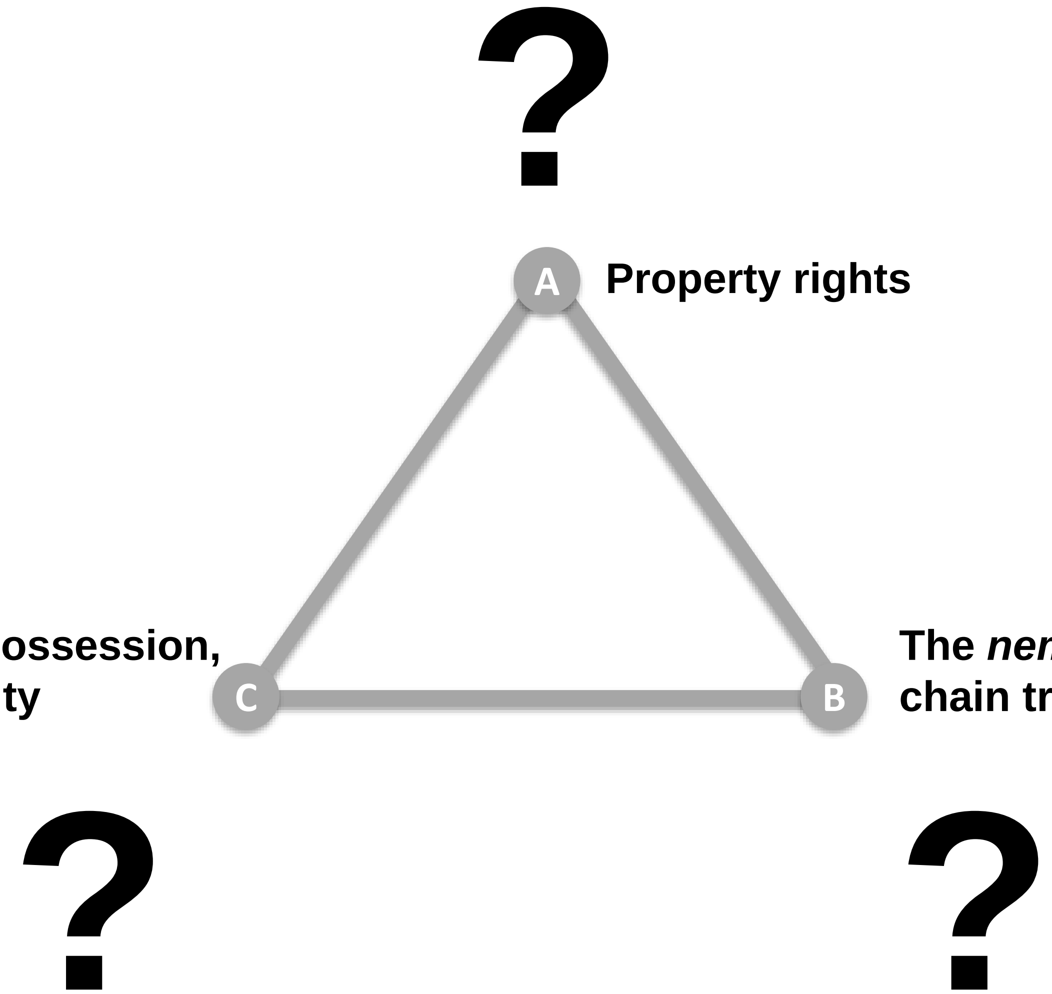
Property rights

The *nemo dat* rule for on-chain transactions

Registration, possession, and negotiability

- Wide exceptions from the *nemo dat* rule, both for transfers and creditor claims
- Example: negotiability
  - By statute?
  - By mercantile usage?
  - By consent?

Competing claims unsolved by law



Property rights

Registration, possession, and negotiability

The *nemo dat* rule for on-chain transactions

Table of content

I. Introduction

II. Competing claims unsolved by technology

- A. What problem did Nakamoto set out to solve?
- B. Remaining issues unaddressed by technology
- C. Competing claims *facilitated* by technology

III. Competing claims unsolved by law

- A. Property rights
- B. The *nemo dat* rule for on-chain transfers
- C. Registration, possession, and negotiability

IV. Three principles to address competing claims

- **A. Acknowledge property rights**
- **B. Establish negotiability**
- **C. Reduce cost of enforcement**

V. Conclusion

Competing claims as issue unsolved

Options include:

- Not recognising property rights
- Adhering to the *nemo dat* rule
- Acknowledging negotiability
- Bypassing the problem

Three principles to address competing claims

A **Acknowledge property rights**

- Market participants believe that they ‘own’ their crypto-assets: should be supported by law

B **Establish negotiability**

- Negotiability by asserting ‘control’ over private keys
- Treat different crypto-assets like their negotiable document equivalents

C **Reduce cost of enforcement**

- Restore legal title by reverse-transfer or return of the private key
- Adjust KYC and procedural rules

C. International collaboration required to reduce cost of enforcement

- Problem: libertarian ‘free havens’
- Need for international KYC-rules
- Need some consensus around the three principles
- Ongoing efforts deserve support: UNIDROIT, European Law Institute

Table of content

FACULTY OF LAW, ECONOMICS AND FINANCE

I. Introduction

II. Competing claims unsolved by technology

A. What problem did Nakamoto set out to solve?
B. Remaining issues unaddressed by technology
C. Competing claims *facilitated* by technology

III. Competing claims unsolved by law

A. Property rights
B. The *nemo dat* rule for on-chain transfers
C. Registration, possession, and negotiability

IV. Three principles to address competing claims

A. Acknowledge property rights
B. Establish negotiability
C. Reduce cost of enforcement

V. Conclusion

Conclusion

- Issue solved neither by technology nor law
- Solution underpinned by three principles:
  1. Acknowledge property rights
  2. Establish negotiability
  3. Reduce cost of enforcement

Thank you!

Dr. Jannik Woxholth

ADA Chair in Financial Law (Inclusive Finance),

University of Luxembourg

jannik.woxholth@uni.lu

Forthcoming publication:

“Competing Claims to Crypto-Assets”