Universiteit Leiden
The Netherlands

Insolvency of crypto-custodians and implications for crypto-investors

Ilya Kokorin

Digital Assets Project

Leiden, 19 September 2019

AGENDA

1. Introduction: research questions
2. How bitcoin transactions work?
3. Crypto-exchanges and ways to “store” bitcoins
4. Insolvency of crypto-custodians: 2 scenarios
5. Insolvency of a crypto-custodian: Dutch law perspective
6. Conclusions and recommendations

Insolvency of crypto-custodians and position of investors

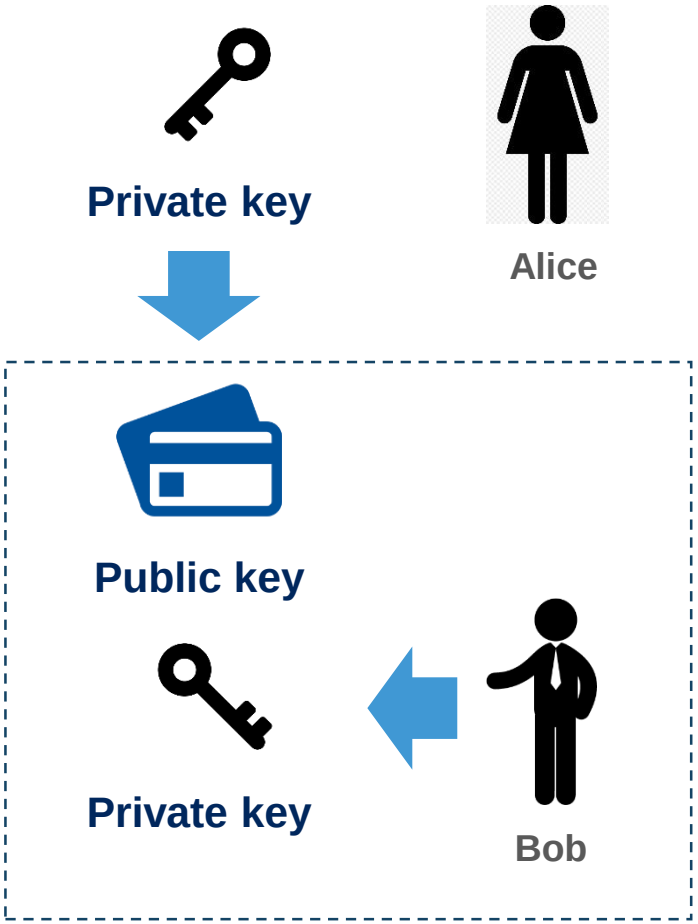
Which rights can crypto-investors assert in the crypto-custodian's insolvency?

1. Do the investors' bitcoins become part of the insolvency estate?
2. Are the investors' rights contractual or property?
3. If these rights are property rights, can the investor (quasi-)revendicate deposited bitcoins?

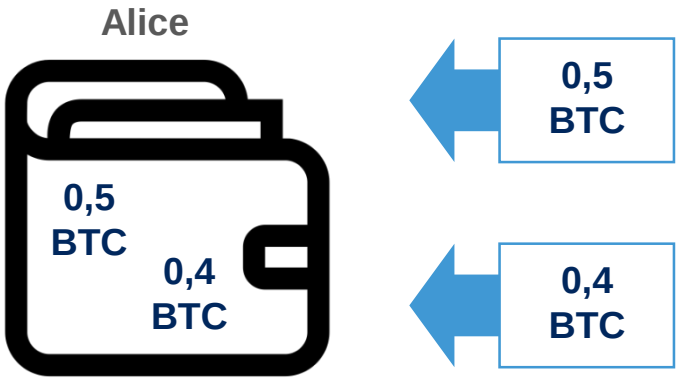
→ What recommendations follow?

How transactions on (bitcoin) blockchain work

Public/private key encryption



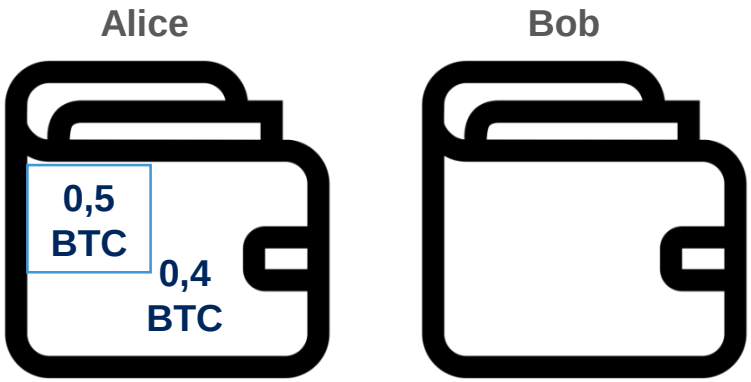
Bitcoin transaction inputs and outputs



- No commingling of BTC
- Both transactions are separately recorded on blockchain

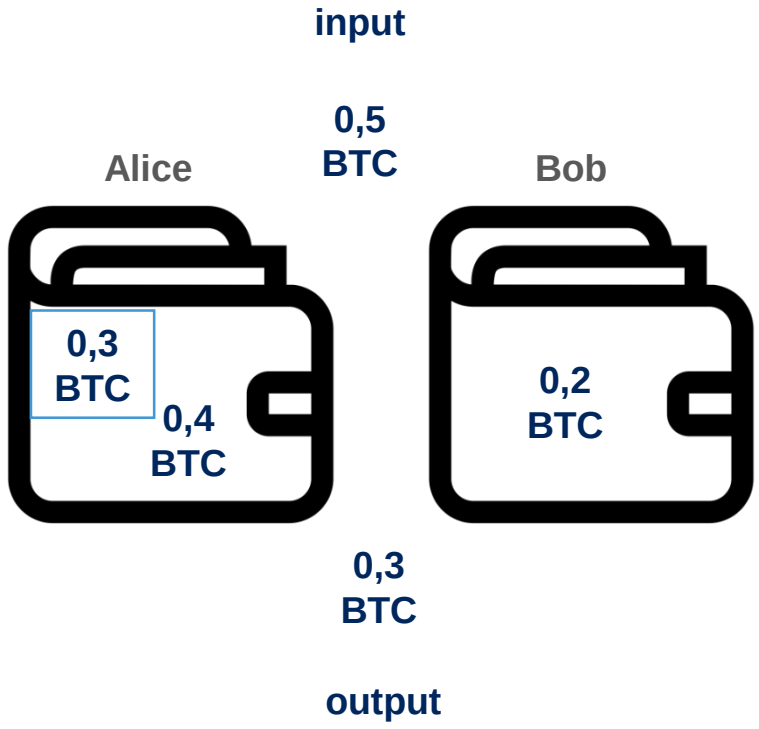
How transactions on (bitcoin) blockchain work

Bitcoin transaction inputs and outputs



“Balance”: 0,9 BTC **“Balance”: 0 BTC**

- Alice agrees to transfer 0,2 BTC to Bob
- 0,5 BTC is (randomly) selected to be spent



“Balance”: 0,7 BTC **“Balance”: 0,2 BTC**

- Alice’s wallet unlocks 0,5 BTC output and uses the whole amount as an input
- 0,3 BTC is new output for Alice
- All transactions are recorded and available on blockchain

Bitcoin Address

15Fzk4v84j9gG4gxXQUcF5fCRJsnwSNykJ

Mycelium

BLOCKCYPHER

BTC | Address, transaction or block

Output

4/6 confirmations

48362d5e6426ab49051286514bf1d8a88dad1e2123182cfc86c542578f90454c

1 Input Consumed

0.00166673 BTC from
14pdPTCJAhVeTgt6ZHJWBUwSLB752RktPc (output)

2 Outputs Created

0.00122989 BTC to
17rhYWFYnMf6m62biNggrV9hrkvLmURXsv (unspent)

0.00032288 BTC to
15Fzk4v84j9gG4gxXQUcF5fCRJsnwSNykJ (unspent)

Value Transacted : 0.00155277 BTC

Coinbase

6+ confirmations

Output

628fdba6f06e6f7691879b596b8009dc26d7638a053ca8d30d0ad4fe771429c8

1 Input Consumed

0.00111388 BTC (output)

2 Outputs Created

0.0008102 BTC to
15Fzk4v84j9gG4gxXQUcF5fCRJsnwSNykJ (spent)

0.00020489 BTC

Value Transacted : 0.00101509 BTC

Bitcoin Address

15Fzk4v84j9gG4gxXQUcF5fCRJsnwSNykJ

Bitcoin Address

1Pj4UeQnvrt6CGD7iCC2mBkeQvYnDqH3gu

- Received: 0,00019273
- Change: 0,0005277
- Fees: 0,00008977
- Total: 0,0008102

Types of contractual arrangements with exchanges

coinbase

Omnibus account

"although we maintain separate ledger accounting entries for customer and Coinbase Group accounts, **no member of the Coinbase Group shall have any obligation to segregate by blockchain address** Digital Currencies owner by you from Digital Currencies owned by other customers or by any member of the Coinbase Group"*

GEMINI

Unique blockchain addresses

"Our records will at all times provide for the separate identification of your Assets. You agree that and understand that nothing herein prevents us from using our Cold Storage System to custody our own property and/or property of third parties; provided, that, at minimum, **separate Blockchain Addresses are utilized** to segregate your Assets from such other property"**

* Coinbase User Agreement (updated in March 2019)
** Gemini Custody Agreement (last modified in November 2018)

“I definitely hope centralized exchanges go burn in hell as much as possible”

Vitalik Buterin

Insolvency of crypto-custodian: MtGox

- Once the largest bitcoin exchange by trading volume
- In February 2014 it filed for insolvency protection
- On 22 June 2018, the District Court of Tokyo issued an order commencing civil rehabilitation proceedings against MtGox (deadline for rehabilitation plan 28 October 2019)

Judgment of Tokyo District Court from August 2015

1. Bitcoin cannot be object of ownership/co-ownership, since it is not a tangible thing

2. The person who manages the private key of a bitcoin address does not have the exclusive control of the remaining bitcoin balance on this address (the involvement of a person other than the parties is required in order to carry out the transaction)

Insolvency of crypto-custodian: BitGrail

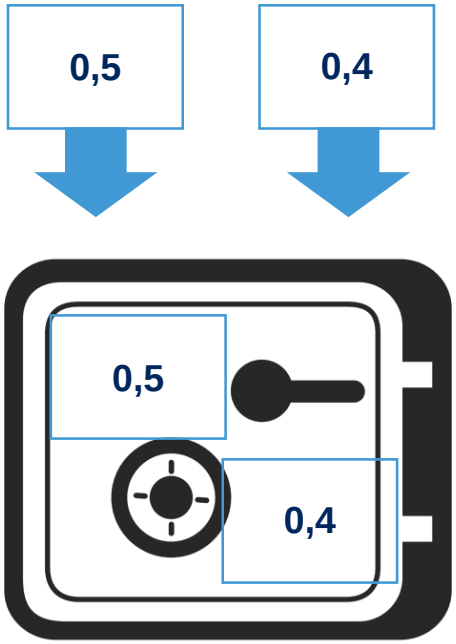
- Italian crypto-exchange platform
- In February 2018 it released a statement, announcing the loss of 17 million Nanos worth approx. USD 170 million

Court of Florence, Decision No. 17/2019 from 21 January 2019

1. Cryptocurrencies may be considered property ("negotiable digitized value")
2. Cryptocurrencies are fungible (interchangeable) and the custodian can dispose of and use them
3. "Once the users' cryptocurrencies were directed toward BitGrail's main address, the currencies […] no longer bore the distinctive elements associated with ownership by a single user, thereby giving rise to a relationship of irregular deposit" (Art. 1782 ICC)
4. Irregular deposit entails an obligation to return items of the same type, quantity and quality, rather than an individualized item

5. In case of irregular deposit, the deposited items become property of the custodian

Insolvency of crypto-custodian: position of Dutch law



Dutch Supreme Court 12 January 1968,
ECLI:NL:PHR:1968:AC2286, NJ 1968/274
Mulder c.s./Teixeira de Mattos

- Investors deposited numbered paper bearer shares in a so-called open deposit with the bank Teixeira de Mattos
- The bank was declared insolvent and failed to register specific shares to individual investors and the bank's own shares
- The bank was deemed to hold the shares for itself and was presumed the possessor and therefore the owner of those shares, subject to counterproof
- Investors were unable to provide the required (counter)proof and therefore could not assert their ownership rights

Insolvency of crypto-custodian: three approaches

1. **Japan** – no ownership rights over bitcoin (no longer the case)

2. **Italy** – loss of ownership in case of irregular deposit (1. interchangeable good, 2. custodian can dispose freely, 3. return of the same quality, quantity, etc.)

3. **The Netherlands** – (potentially) no loss of ownership in case of 'unspent' bitcoin (and change from 'spent' bitcoin) and loss of ownership in case of 'spent' bitcoin

Conclusions

1. Crypto-custodian insolvency risk is real and investors rarely receive anything from defunct crypto-exchanges

2. Rights of crypto-investors depend on applicable property law and operation of a crypto-exchange

3. In principle, segregation by operation of blockchain. What is more important is the practice of re-use:

- Crypto-investors must know of re-use
- Reuse may be forbidden for consumers (?)
- Segregated blockchain addresses are safer, but more expensive to operate
- If crypto-custodian violates contractual/statutory prohibition → investors' claim with priority on custodian's estate (?)

Universiteit Leiden
The Netherlands

Thank you!

Ilya Kokorin

Department of Financial Law
Leiden University
M +31 6 33 82 73 05
E i.kokorin@law.leidenuniv.nl