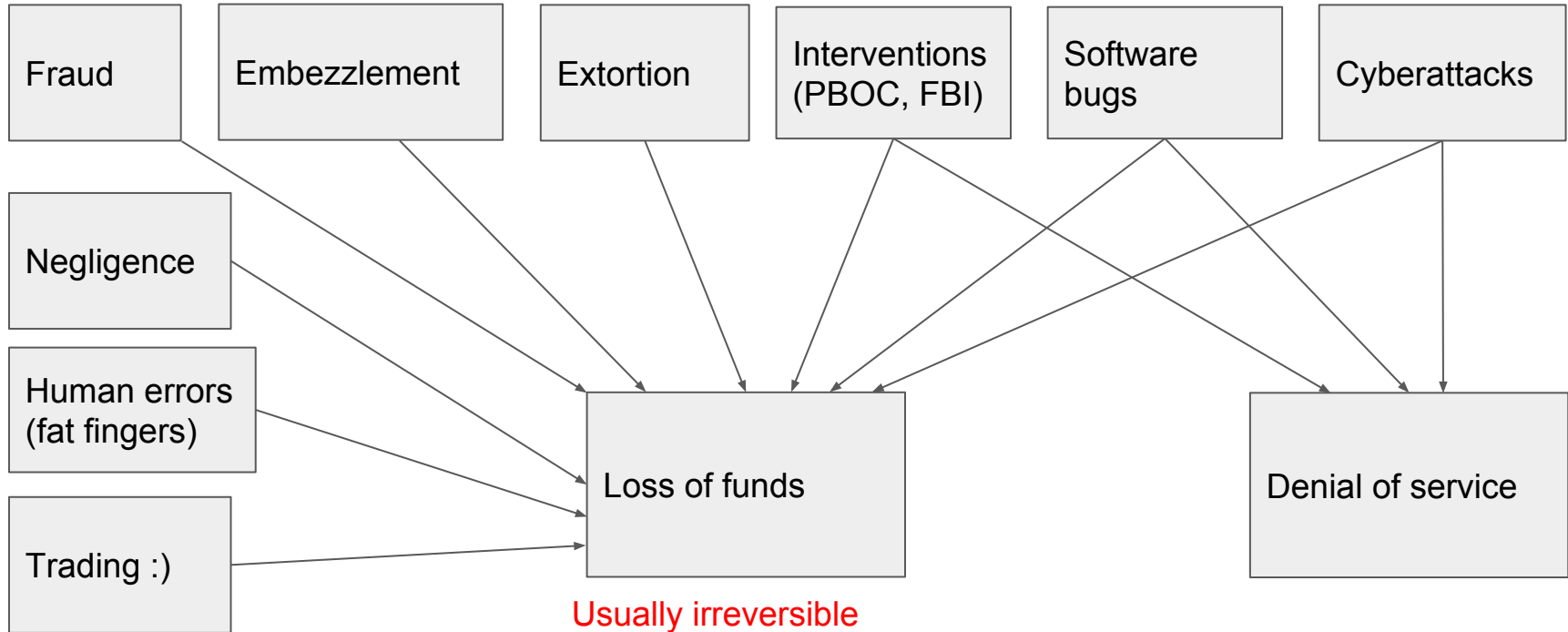


When things go wrong in cryptocurrencies world

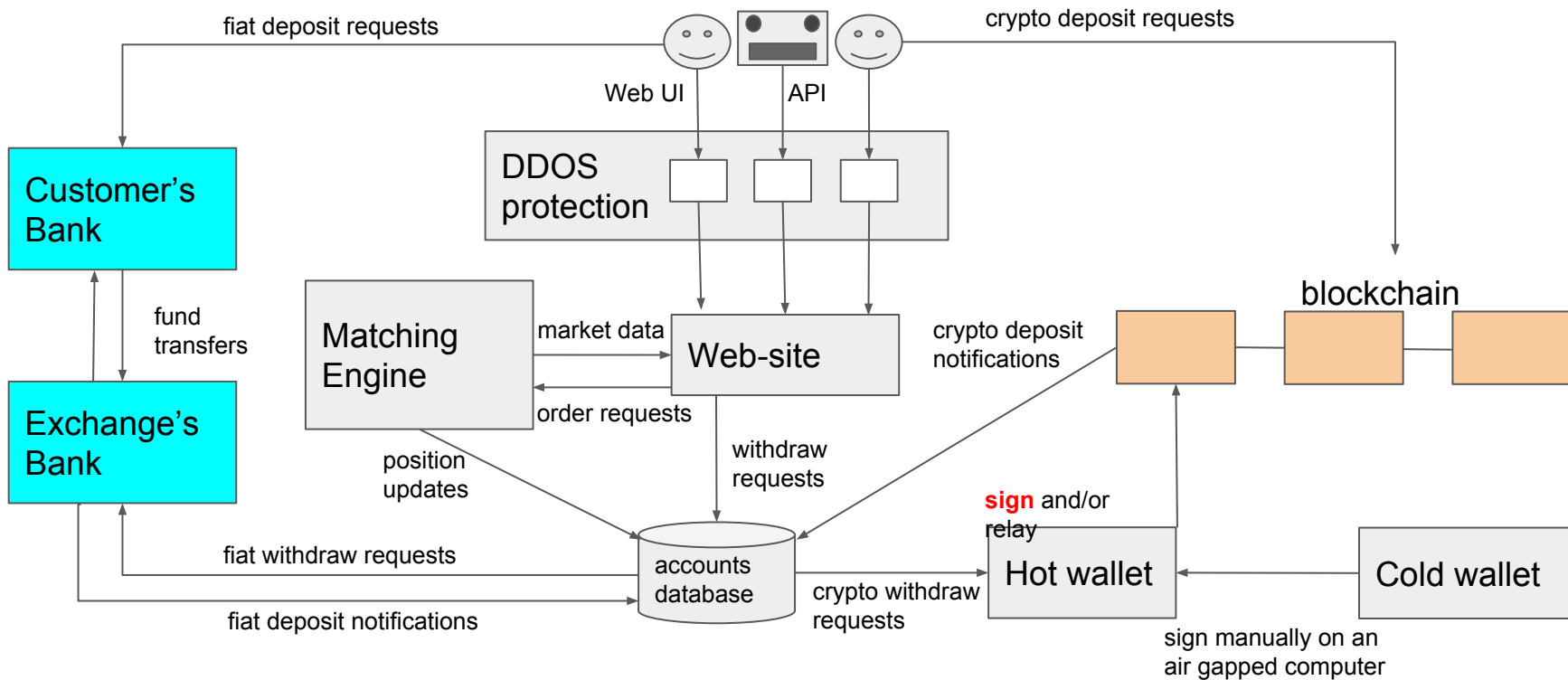
Alexey Akhunov, May 2017

What could possibly go wrong?

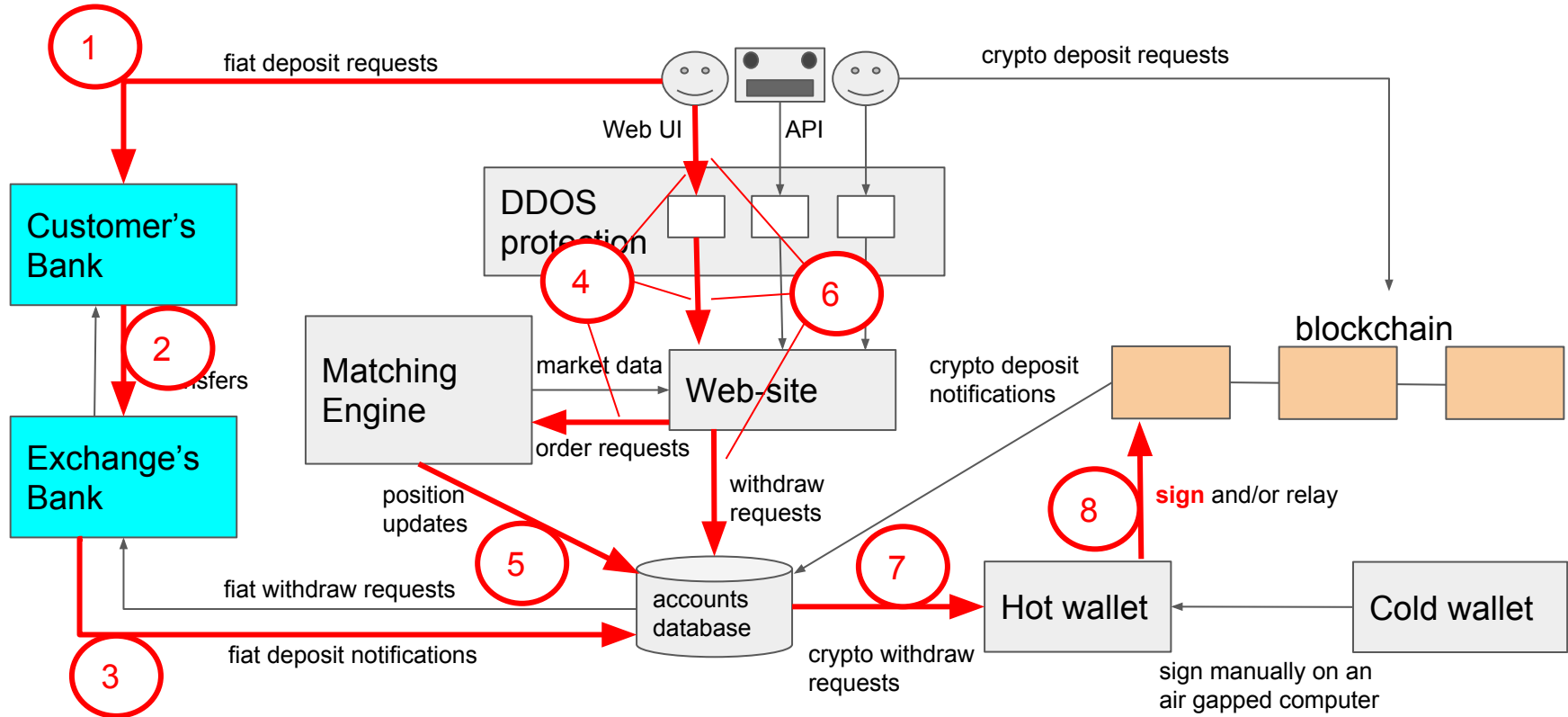


Usually irreversible
"Sorry For Your Loss"

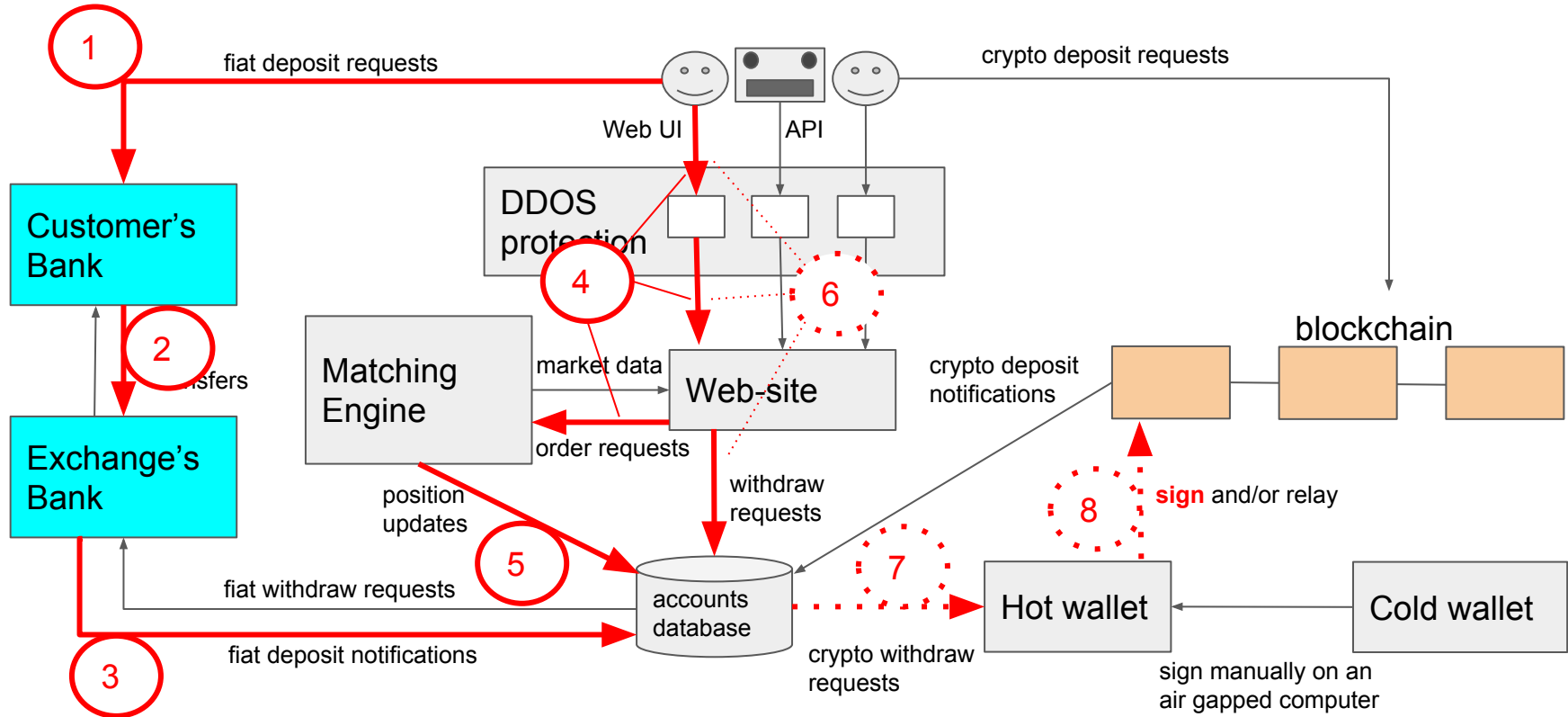
Typical cryptocurrency exchange



Example flow: user sells EUR, buys BTC



Problem 1: many users don't do 6-8

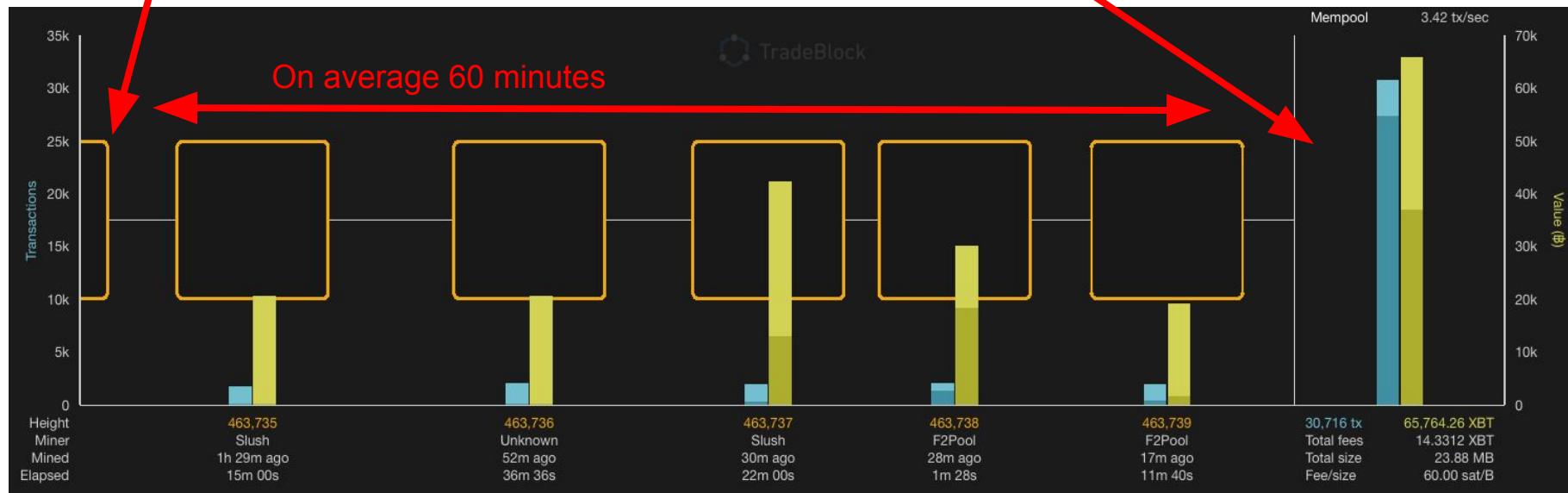


Why users leave their crypto on exchanges?

1. They want to be able to trade fast

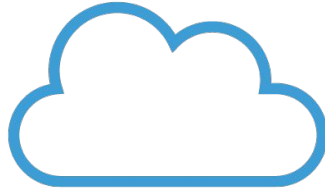
deposit gets here

Account database updated here
(6 confirmations for BTC)



Why users leave their crypto on exchanges?

2. They don't know how to store it securely



???



Why users leave their crypto on exchanges?

3. They trust that exchange can keep it better than themselves



Mt.Gox - Feb 2014 (~850'000 bitcoins went missing)

The bankruptcy case is still ongoing

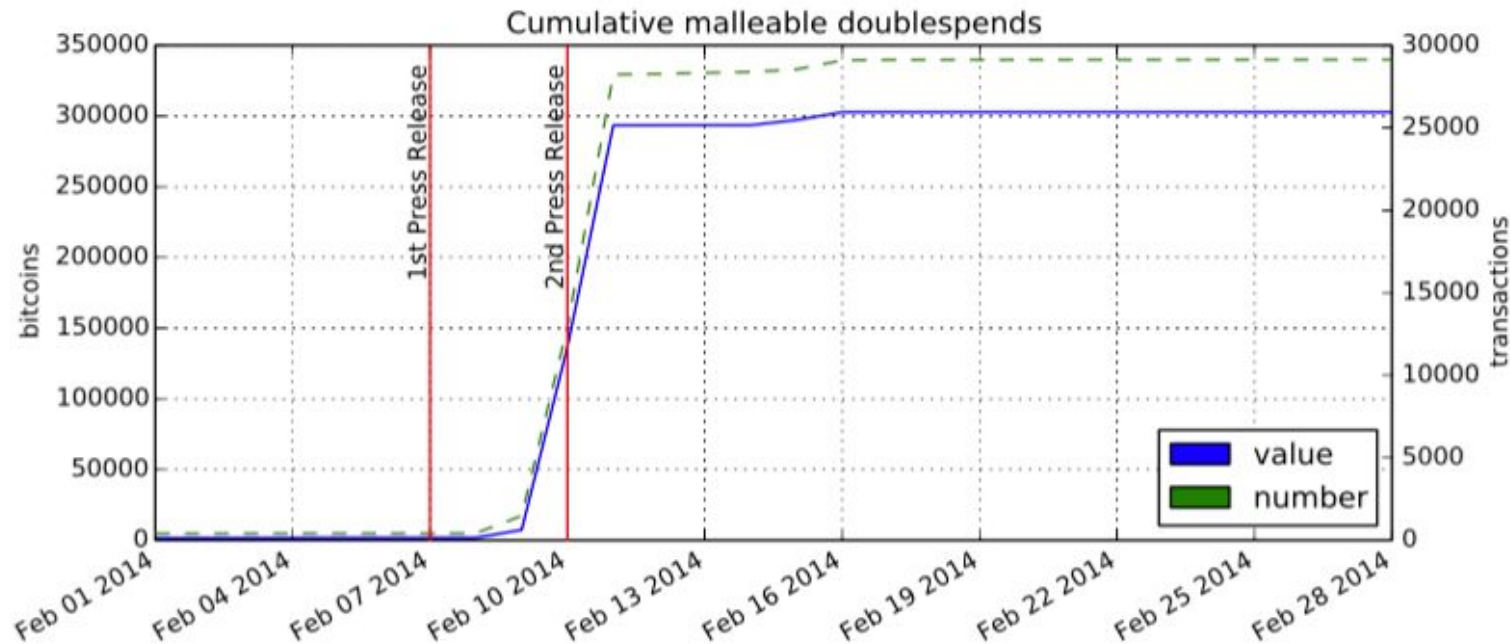
The real cause of fund loss has never been revealed



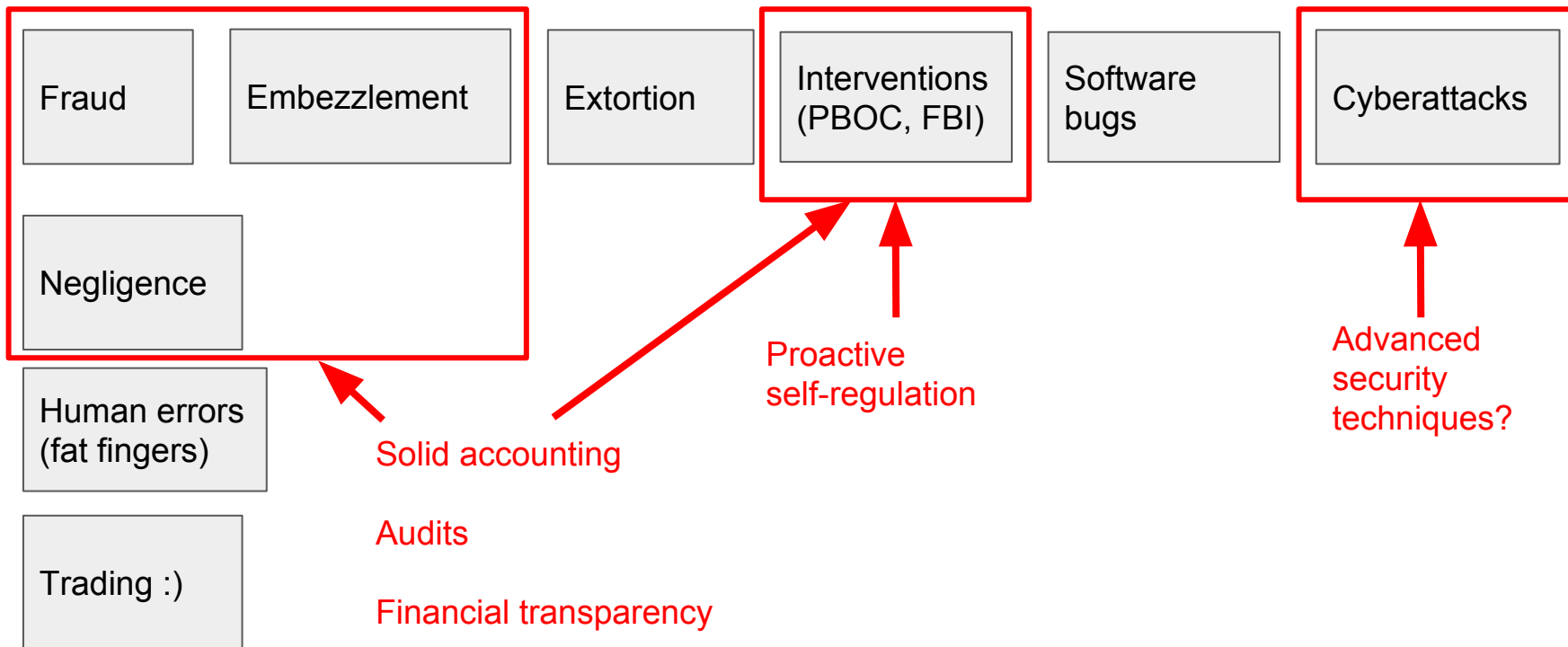
Suggested causes: transaction malleability, loss of keys, hackers, web server or database exploit, seizure by US government, embezzlement

Transaction Malleability? Nah...

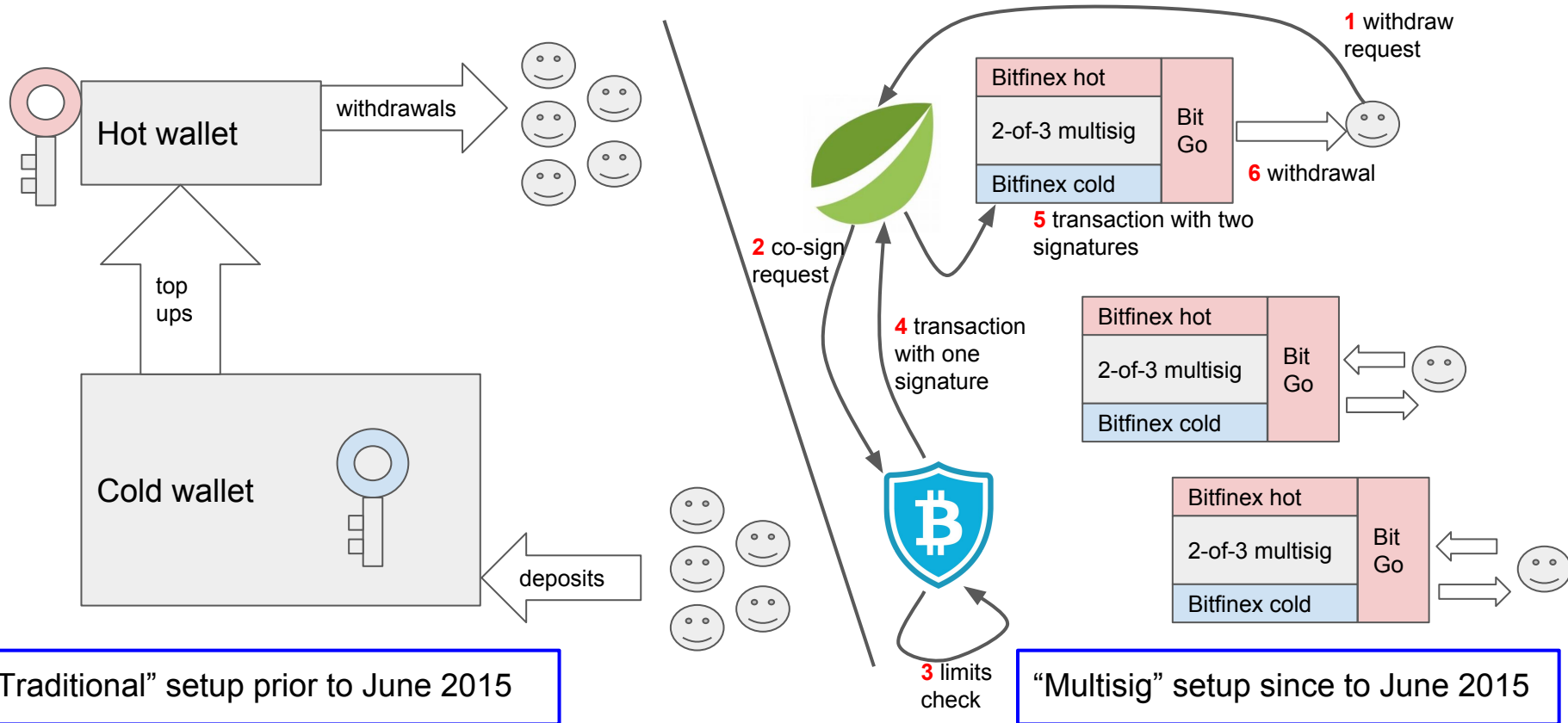
Transaction malleability could not be the cause (see “Bitcoin Transaction Malleability and MtGox” by Christian Decker and Roger Wattenhofer)



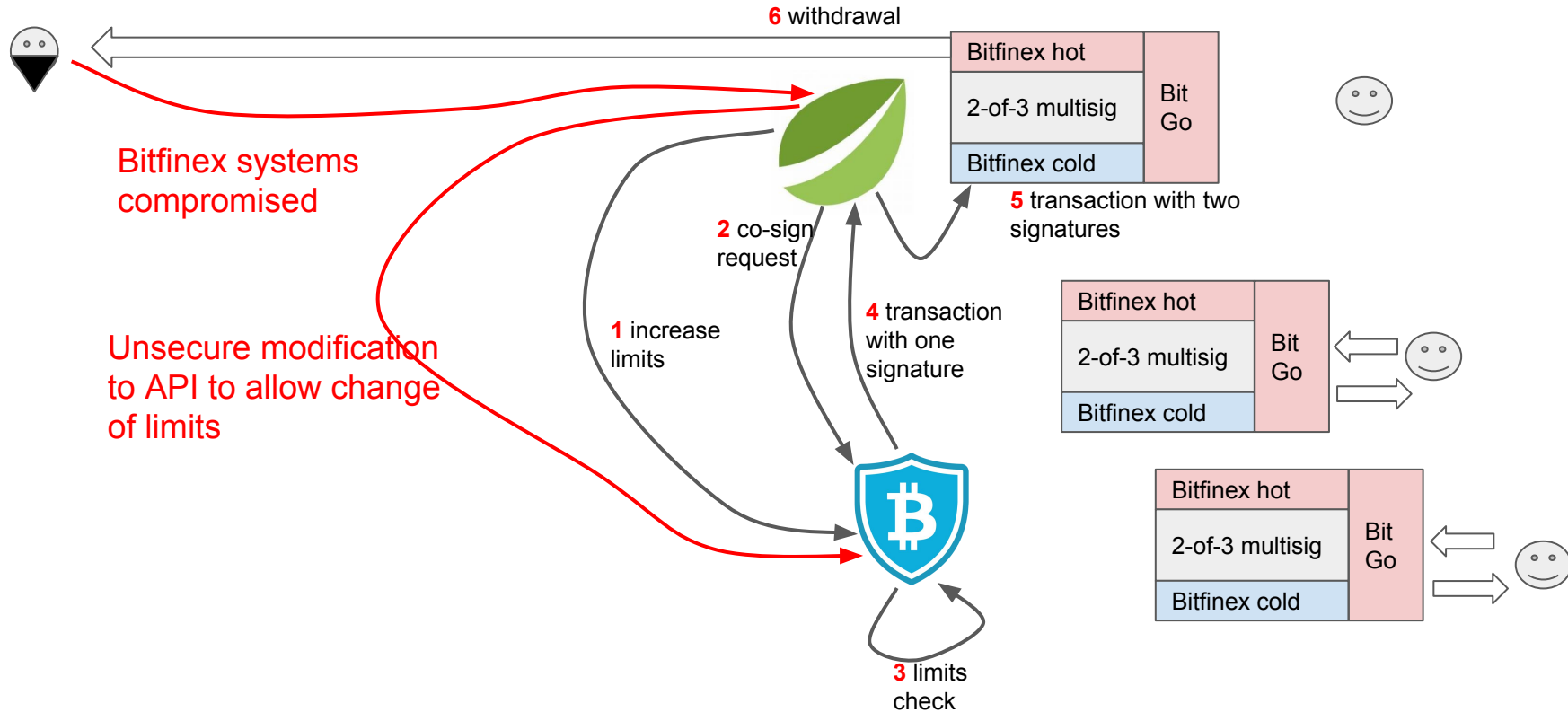
Lessons learnt?



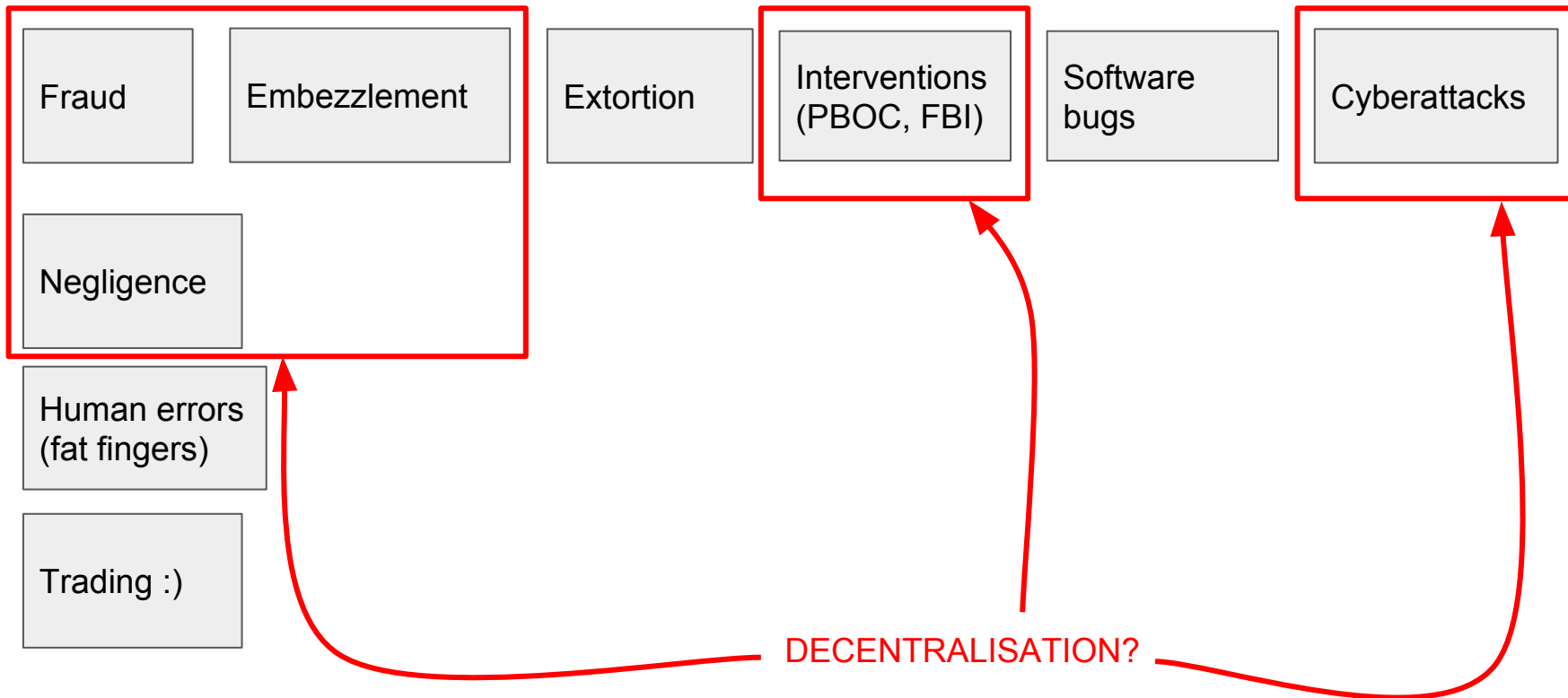
Bitfinex - August 2016 (~120'000 bitcoins stolen)



Bitfinex - August 2016 (~120'000 bitcoins stolen)

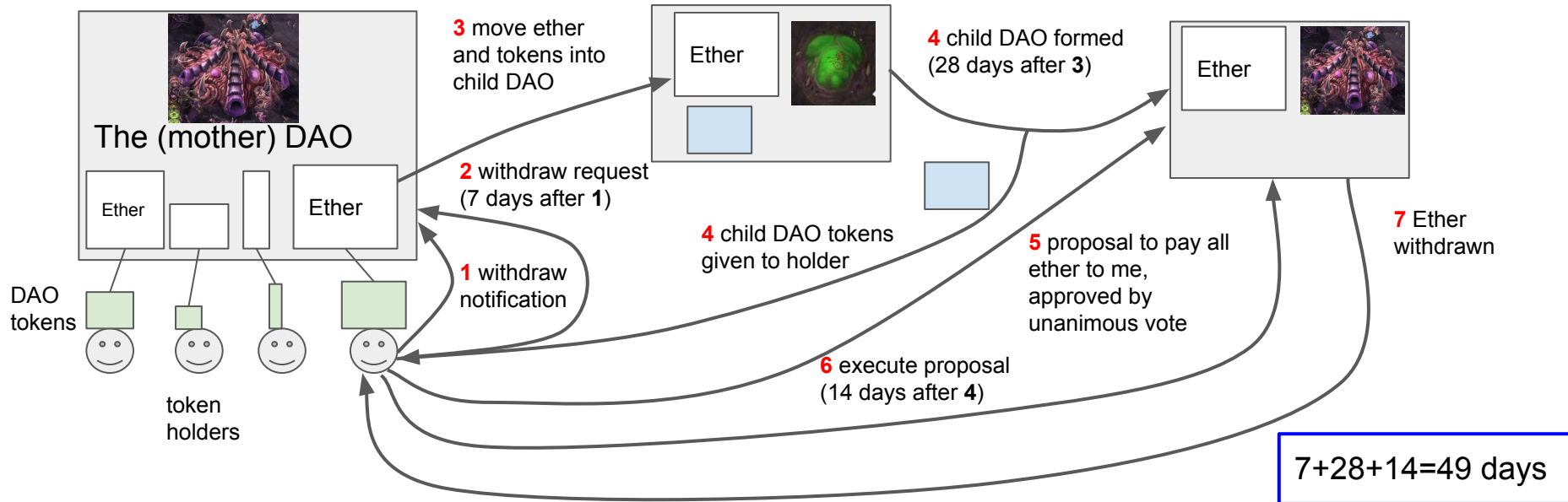


Lessons learnt?



DAO - June 2016 (~3.6m Ether lost to contract exploit)

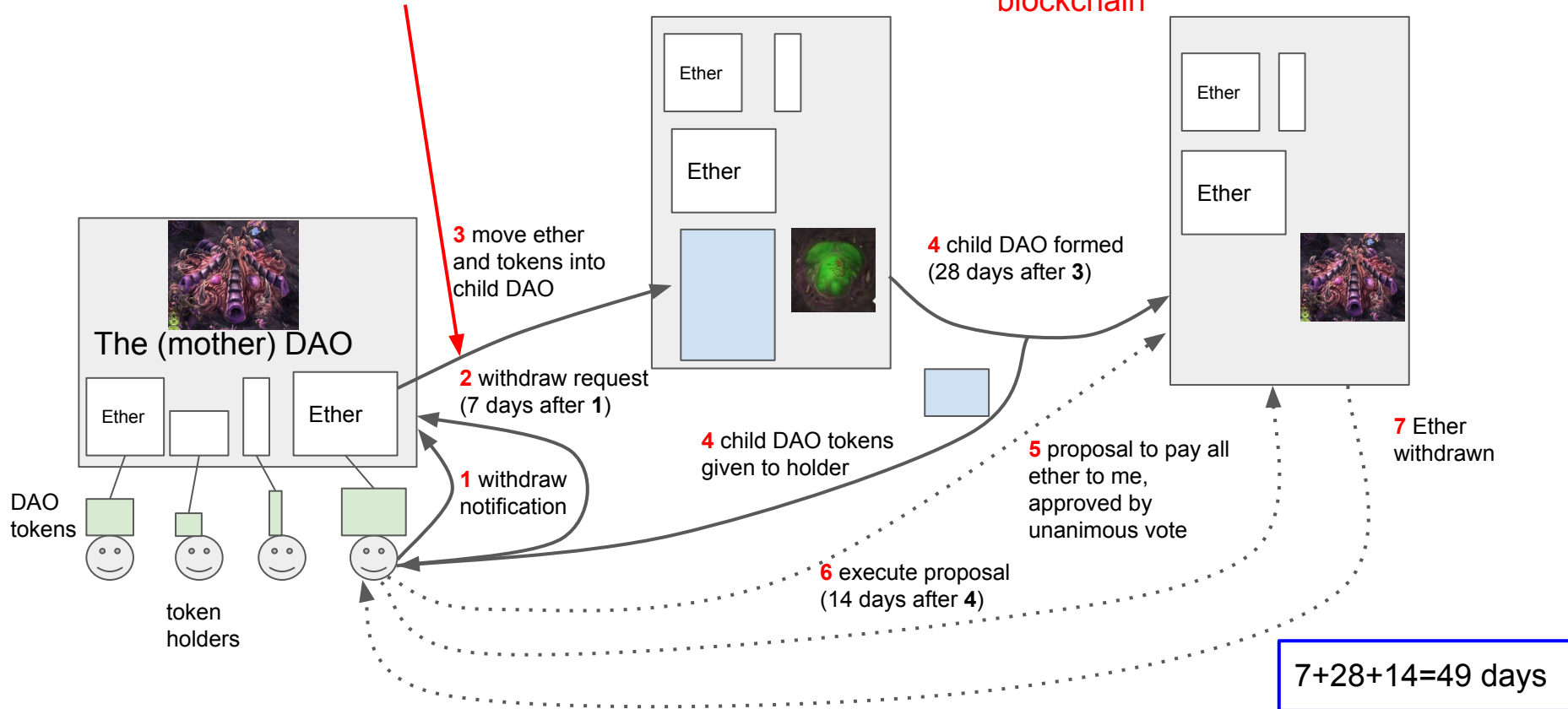
DAO is not an exchange, it is Decentralised Autonomous Organisation



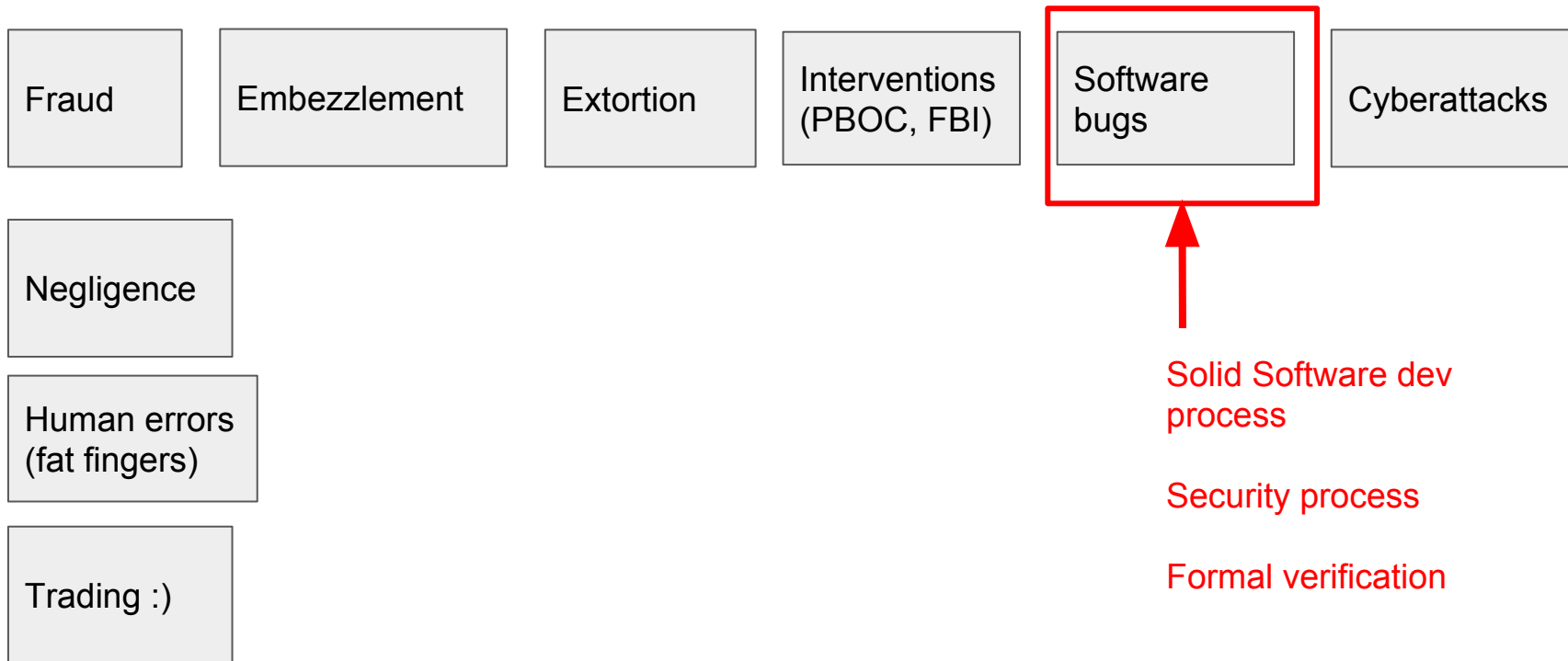


Someone discovered a way to move
someone else's Ether into their childDAO
without moving their tokens

Due to DAO recover hard fork of
Ethereum, some steps happened
only on Ethereum Classic
blockchain



Lessons learnt?



What is next?

Likely future problems:

- Incentive incompatibility?
- Game theoretical attacks? (also existed in the DAO)

Interesting security trends

- Hardware wallets for personal security
- Vaults (suggested for bitcoin, implemented in Dash)