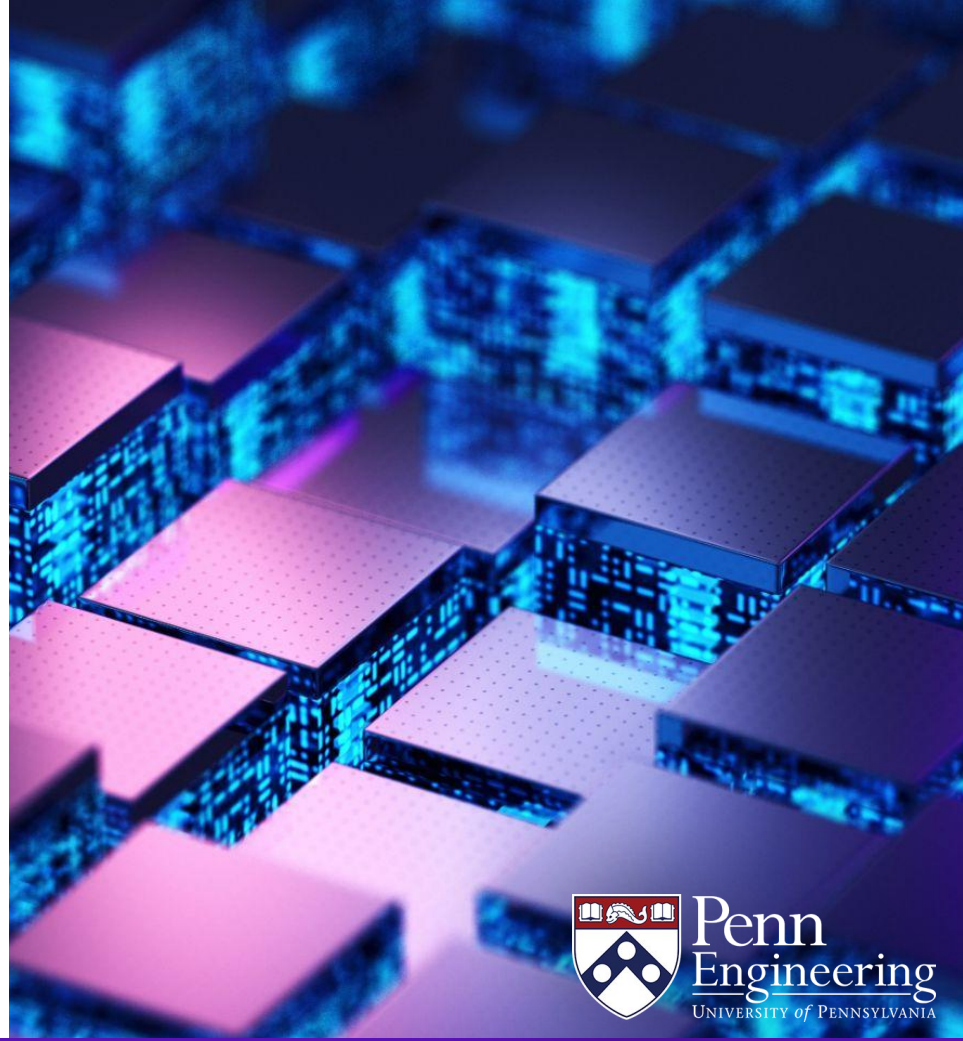
EAS 5830: BLOCKCHAINS

Censorship Resistance

Professor Brett Hemenway Falk



"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."

- “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”
- “there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services”
- “Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers.”

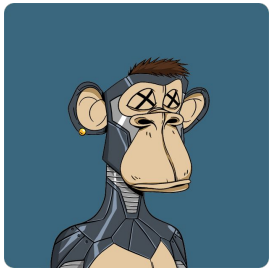
Censorship resistance

- Bitcoin was founded on the idea of censorship resistance
  - Not privacy
- If no one can censor your transactions no one can reverse mistaken or fraudulent transactions

Fat Fingers: a Bored Ape NFT Was Sold for $3K Instead of $300,000

Author: George Georgiev • Last Updated Dec 13, 2021 @ 15:15

A user fat-fingered Ape 3457 from the BAYC collection and sold it for $3K instead of $300K.



Money > Crypto

A Typo Sent $36 Million of Crypto Into the Ether

Developers of the Juno cryptocurrency meant to send $36 million in tokens to a community-controlled wallet. Human error sent it to an inaccessible address.

Daniel Van Boom

May 5, 2022 8:56 p.m. PT

3 min read

No ‘forgot password’ option

- “I accidentally threw away $60M worth of Bitcoin” (Now
  - “I had two hard drives in a desk drawer. One was empty and the other contained my bitcoin private keys,” Howells recalled. “I meant to throw away the empty drive — and I accidentally threw away the one with the bitcoin information.”

LOUISE MATSAKIS SECURITY MAY 20, 2018 7:00 AM

How WIRED Lost $100,000 in Bitcoin

We mined roughly 13 bitcoins and then ripped up our private key. We were stupid—but not alone.

MAI SCHOTZ

Irish drug dealer loses £46m bitcoin codes he hid in fishing rod case

Clifton Collins fears fishing gear was taken to dump by his landlord after he was jailed


ANNALS OF MONEY DECEMBER 13, 2021 ISSUE
HALF A BILLION IN BITCOIN, LOST IN THE DUMP
For years, a Welshman who threw away the key to his cybercurrency stash has been fighting to excavate the local landfill.
By D. T. Max
December 6, 2021

Cryptocurrencies + Add to myFT

‘Fat finger’ $24m charge exposes fragility in crypto market

Erroneous fee is refunded, in proof to DeFi proponents of shared community values

MARKETS

Tether's $5 Billion Error Exposes Crypto Market's Fragility

Sudden flood of digital coins spooked market and drove down price of bitcoin by about 12%

By Paul Vigna

July 16, 2019 8:28 am ET

Share

Resize

News › Business

Crypto.com Accidentally Sent $400M in Ethereum to Wrong Address, CEO Calls Concerns 'FUD'

Crypto.com's $400 million mishap leaves its token down 50% and raises doubts over the exchange's transparency following FTX's collapse.

By Ben Munster

Nov 13, 2022

3 min read

Censorship resistance

- There is a fundamental tradeoff between censorship resistance and fraud protection
- You can build in fraud protection using smart contracts
  - Daily transfer limits
  - Multiple signoffs for large value transactions
  - Recovery partners