DeFi, NFTs, and crypto in business

Raghavendra Rau, University of Cambridge

Ownership, trust, and society

What does ownership mean?

Of a physical asset:

- Might makes right?
- Social norms and structure
- Rule of law

The rule of law is governed by databases

But who maintains the databases?

- Central authority (government)

- Intermediaries (exchanges, depositary institutions)

But trust is fragile.

- Expropriation by governments
- Banks are not very good at maintaining databases

Alternative idea: Trust (a lot of) complete strangers

The essence of crypto

Completing transactions between two people without a centralized record-keeper.

- Sending money
- Writing a legal contract
- Creating a market

But with a whole bunch of strangers economically interested in keeping all the records safe.

Consensus protocols

But suppose a bunch of anonymous strangers verify your transactions. How do they do it? Majority rule?

- Sybil attacks

Make it economically interesting for each stranger to act truthfully vs. fraudulently

- Proof of work

Crypto is trustless – so you can trust it.

What is crypto?

Crypto is a general phrase that applies to a lot of different things:

- Cryptocurrencies (deals with money)
- Tokens (sort of deals with money)
- Decentralized Finance (deals with automatic contracts)
- Blockchains (deals with databases)
- Web3 (a decentralized evolution of Web1 and Web2)

Crypto and finance

Finance is bizarre.

Crypto is equally bizarre: In the past 15 years, crypto has built a whole financial system from scratch. Crypto has reinvented or rediscovered things that finance has been doing for centuries.

- It has found new and better ways to do things.
- It has found worse ways, heading down dead ends abandoned by traditional finance decades ago.
- It has reinvented solutions to problems just like traditional finance, but with new names and explanations.

What is a cryptocurrency?

A store of value?

- Value in finance comes from two things: Cash flow and risk

- Crypto allows you to transfer ownership of a number from one computer to another

- Why did cryptocurrencies explode in number?
- Are cryptocurrencies uncorrelated with other asset classes?
- Is it like a meme stock?

What is a cryptocurrency?

A distributed computer that can execute smart contracts?

Enter Vitalik Buterin and the Ethereum Virtual Machine

Allows the possibility of adding if-then statements to the mechanism of sending payments from one person to another

- Needs an oracle to connect to the real world
- Or acts like a self-contained vending machine

A distributed computer

No keyboard, no mouse, no monitor

Distributed apps (dApps)
Programs that run on the web but keep the data in a blockchain

Broadcast the instructions to thousands of nodes on the network, and they each execute the instructions and reach consensus on the results of the instructions. The program needs to run thousands of times on thousands of computers.

How does the distributed computer reach consensus?

Proof of stake

- You can “validate” a transaction by buying the network currency and deposit into a special smart contract and there are limits on withdrawals – a stake.
- Validators compile all the transactions into blocks
- At a fixed interval, one validator is randomly chosen to propose a block and another set is chosen to review and vote.
- If the validator acts dishonestly or is lazy, it loses its stake.

How do you earn money?

Proof of work (Bitcoin)	Proof of stake (Ether)
Buy lots of computers	Deposit ether to buy a stake
Solve meaningless mathematical riddles	Validate a transaction
Earn bitcoin	Earn (gas) fees based on your stake

Reinventing interest

Why do you earn interest when you deposit money in a bank?

Why do you earn interest when you lend ether to a validator?

Fungible Tokens

Why do you need a token?

Platforms and network effects

Creating a new token in Ethereum is easy
- ERC-20: The Ethereum white paper has a four-line code snippet “for implementing a token system”.

Reinventin

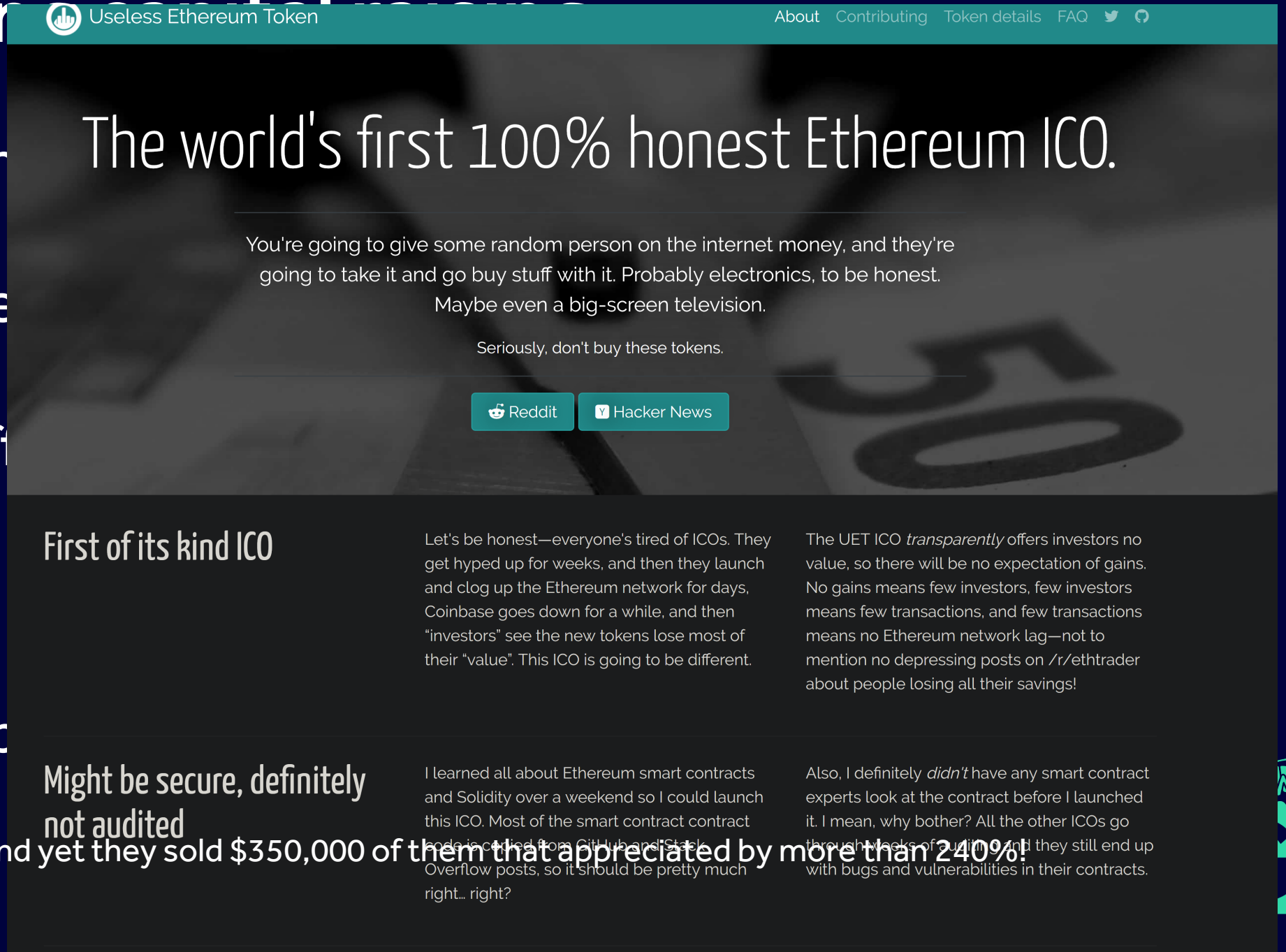
How does a r

How did Ethe

Initial coin off

DAO

But this has p



And yet they sold $350,000 of them that appreciated by more than 240%!

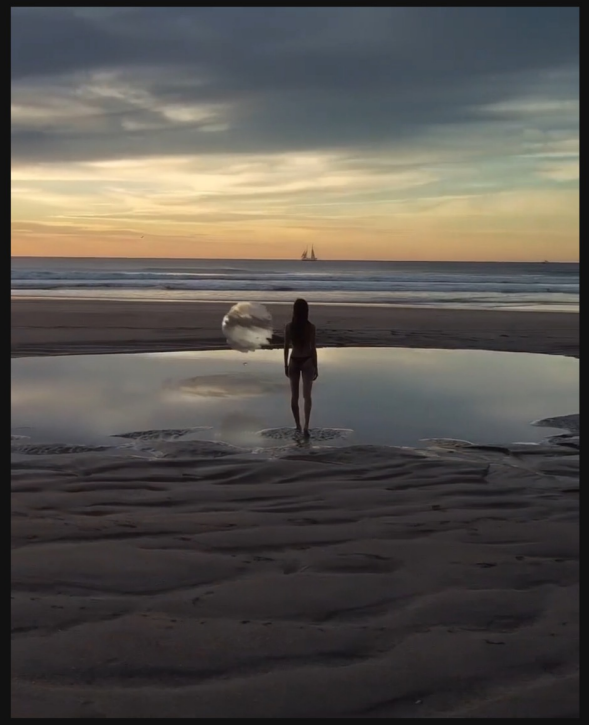
Non-Fungible Tokens

But tokens can be unique as well. How?

Answer: Ethereum protocol ERC-721: Add a token id to the contract so that [contract, tokenid] is unique.

Non-Fungible Tokens

THE VERGE TECH REVIEWS SCIENCE CREATORS ENTERTAINMENT VIDEO



Danilo

OBJKT#274808

info listings history

D[ ]STANCE

L'Eau de Distance [LDD]
Digital perfume exploring Virtual Scents.

CNET Your guide to a better future

Culture

Someone just bought a cryptocurrency cat for $172,000

Was it an accident? Money laundering? No one knows. But someone just bought a CryptoKitties digital cat for $172,000.

Mark Serrels

Sept. 4, 2018 8:26 p.m. PT

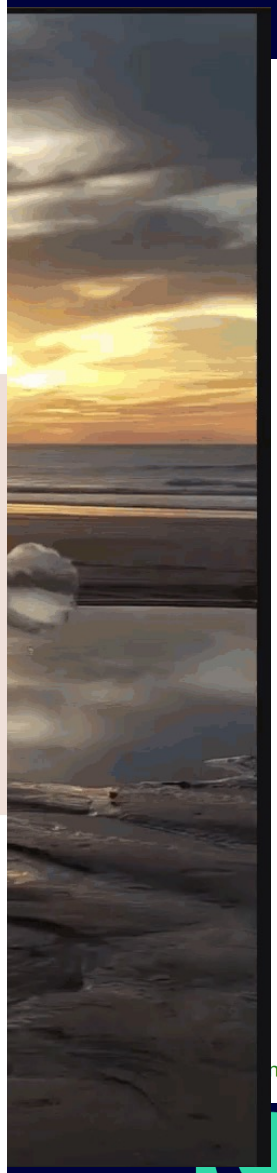
CryptoKitties

Meet CryptoKitty #896775. Her name is Dragon.

She has chestnut coloured eyes, her base colour is "cottoncandy". According to her bio she "bit Rebecca Black once" and finds spying on neighbours "exhilarating".

She is a digital cat and Tuesday someone bought her for the equivalent of $172,000.

Yep, that's $172,000 in US dollars, or 600ETH (Ethereum) to be precise. Welcome to 2018.



Reinventing borrowing

How do you borrow money against a secured asset (like a house) in the traditional finance world?

What about the crypto world?

Martingale fractionalization

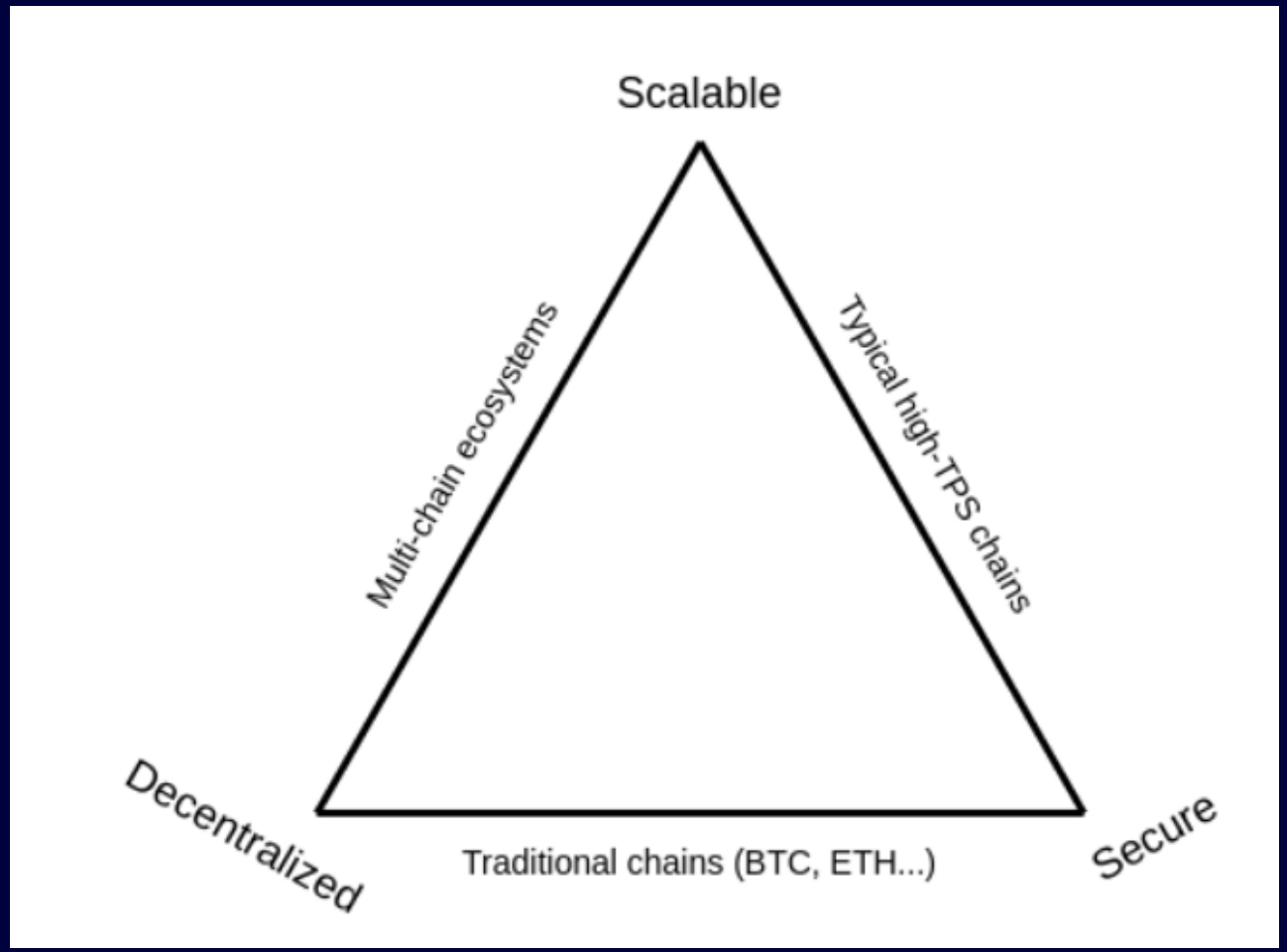
Making blockchains useful in business

The blockchain trilemma

- Security
- Scalability
- Decentralization

Regulators

Permissioned blockchains



https://vitalik.ca/general/2021/04/07/sharding.html

Moving from the crypto world to the real world

Moving from one blockchain to another: Crypto bridges

Moving from a blockchain to the real world

The crypto financial system

Crypto is:

- A set of tokens, which are worth fluctuating amounts of money.
- A set of ways to create new tokens and distribute them and try to make them worth money.
- A way of recording your holding of assets
- A way to write contracts and computer programs (computer programs that are contracts, and contracts that are computer programs).

Source: Matt Lewin, Bloomberg Businessweek, Oct 31, 2022

How does it compare to the real financial system?

It is an elegant self-contained system with permissionless innovation.

- Opinion 1: It is a streamlined, modernized, innovative evolution of the traditional system.
- Opinion 2: It is a chaotic devolution of the traditional financial system that never learnt important historic lessons about fraud, leverage, risk, and regulation.

Centralized intermediation vs disinterm

Who is respo

What happe

How about t

The New York Times

Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes

Bitcoin owners are getting rich because the cryptocurrency has soared. But what happens when you can't tap that wealth because you forgot the password to your digital wallet?

Source: https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html

Stefan Thomas, a German-born programmer living in San Francisco, has two guesses left to figure out a password that is worth, as of this week, about $220 million.

The password will let him unlock a small hard drive, known as an IronKey, which contains the private keys to a digital wallet that holds 7,002 Bitcoin. While the price of Bitcoin dropped sharply on Monday, it is still up more than 50 percent from just a month ago, when it passed its previous all-time high of around $20,000.

The problem is that Mr. Thomas years ago lost the paper where he wrote down the password for his IronKey, which gives users 10 guesses before it seizes up and encrypts its contents forever. He has since tried eight of his most commonly used password formulations — to no avail.

How can mainstream investors invest in crypto?

Bitcoin futures

Bitcoin future ETFs

Buying crypto through an exchange

- Can you actually get the crypto yourself?

- Quis custodiet ipsos custodes?

Who guards the guardians?

Several exchanges have been hack

- Mt. Gox (2011-2014) - 850k Bitc
- Bitfloor (2012) - 24k Bitcoin
- Bittfinex (2016) - 120k Bitcoin
- Coincheck (2018) - 523 million N the time)
- Binance (2019) - 7k Bitcoin

FINANCIAL TIMES

US arrests two and seizes $3.6bn in cryptocurrency from Bitfinex hack

Prosecutors charge New York-based couple with conspiring to launder billions stolen in 2016 breach

Hong Kong-based Bitfinex was hacked in 2016 © Dado Ruvic/Reuters

Stefania Palma in Washington and **Hannah Murphy** in San Francisco YESTERDAY 8 February 2022

The US Department of Justice has arrested two people and confiscated more than $3.6bn worth of cryptocurrency that it said was stolen during the high-profile 2016 hack of the Bitfinex exchange, executing the government agency's largest financial seizure.

New York-based Ilya Lichtenstein, 34, and his wife, Heather Morgan, 31, were arrested on Tuesday and accused of conspiring to launder proceeds of 119,754 bitcoin valued at $4.5bn, prosecutors said in a statement. The cryptocurrency was allegedly taken when Hong Kong-based Bitfinex was breached.

Crypto exchanges vs. stock exchanges

Security exchanges for finance: Margin calls, clearing houses, brokers etc

Crypto exchanges for crypto: Provide leverage

- How do they set leverage limits?
- What is the level of collateral necessary?

Stablecoins

A stablecoin is a crypto token that's supposed to always be worth $1.

How do they do this?

- Collateralized stablecoins
  - Tether
- Algorithmic stablecoins
  - Leverage: You put in $100 and get back a thing that's worth $100, with that value guaranteed by a larger amount of a volatile cryptocurrency. The stablecoin is like debt – a senior claim on the bank's assets
  - Problem: Death spirals

How do crypto exchanges work?

Regular stock market: Market makers and Central limit order books

This does not work in smart contracts – gas fees are too high – even for incomplete and withdrawn transactions

How do crypto exchanges work?

DEX and Automated Market Makers

A market maker deposits equal amounts of Ether and a dollar equivalent stablecoin.

1 Ether = US$1,200
Deposit 1000 Ether and $1.2 million USDC.
Constant product market maker: Keep the product of 1000 and 1.2 million constant = 1.2 billion

DEX and Automated Market Makers

Suppose someone wants to buy 100 Ether. That leaves 900 Ether in the fund.

To keep the product the same, I have to increase the number of USDC in the pool. How much more?
1.2 billion/900 = 1.333 million USDC.

So to buy 100 Ether will cost 1.333m USDC – 1.2m USDC = 133,333 USDC which means that the exchange rate is

1 Eth = 1,333.33 USDC

Earning transaction fees: Anyone can provide liquidity into an AMM pool and earn tokens for providing liquidity.

Lending your crypto

Secured against cryp

Unsecured lending fo

Tokenomics:

- Stake Ether to become a validator (say in L
- Get receipt for staked ether
- This receipt is valuable
- Borrow against this receipt to get another token
- Yield farming: OlympusDAO and the (3,3) Prisoner's Dilemma

Arbitrage in crypto

Real world arbitrage is tough to do

Good news: Decentralized finance is new enough that pricing anomalies exist, but efficient enough that everything happens visibly on a virtual computer running public code, so you can reliably exploit them.

How? Flash loans

Flash loans

Suppose Ether is trading at 2 different prices on two exchanges. What do you do?

1. Borrow $100 million from some decentralized lending protocol, such as Aave.
2. Use the $100 million to buy a token on Decentralized Exchange A
3. Sell the token on Decentralized Exchange B for $110 million
4. Return the $100 million to the lending protocol (plus a small fee)
5. Keep the leftover $10 million ...

... all in the same transaction that executes all at once.

This seems cool. What is the problem?

In crypto, a

Some
occas

Exam

Somebody
to put
up the

The Attack

Transaction Hash: 0xb5c8bd9430b6cc87a0e2fe110ece6bf527fa4f170a4bc8cd032f768fc5219838

Status: Success

Block: 9484688 3470101 Block Confirmations

Timestamp: 535 days 20 hrs ago (Feb-15-2020 01:38:57 AM +UTC)

From: 0x148426fdc4c8a51b96b4bed827907b5fa6491ad0 (bZx Exploiter 1)

hort position

Uniswap

reserve, causing large slippage.

- The attacker swapped the 112 wBTC borrowed from Compound to 6871 ETH on Uniswap, resulting in a profit

Transaction Action:

- Borrow 10,000 Ether From dYdX
- Supply 5,500 Ether To Compound
- Borrow 112 WBTC From Compound
- Swap 5,637.623762376237623786 WETH For 51.3455758 WBTC On Kyber
- Repay 10,000.00000000001 Ether To dYdX

98,250

Any other problems? Front-running

In traditional finance, when you place an order, your order goes to your broker, who routes it to different exchanges at different times through different pipes
Problem? Flash traders

In crypto, this is explicit

The great financial crisis

Why did Satoshi Nakamoto invent Bitcoin?

It was a new financial system with transparent and irreversible transactions, with no special power for governments or big banks.

But there were a lot of traditional finance people who were also interested:

- It was fun, it was wide open, it allowed for permissionless innovation, and everyone was getting rich.

The great crypto crisis

TerraUSD and Luna

Celsius bank?

Contagion among crypto assets

FTX/Alameda

What is the future of crypto?

Real assets

Digital assets

- Institutions
- Communities
- Trust

FOR THE LOVE OF LEARNING SINCE 1597