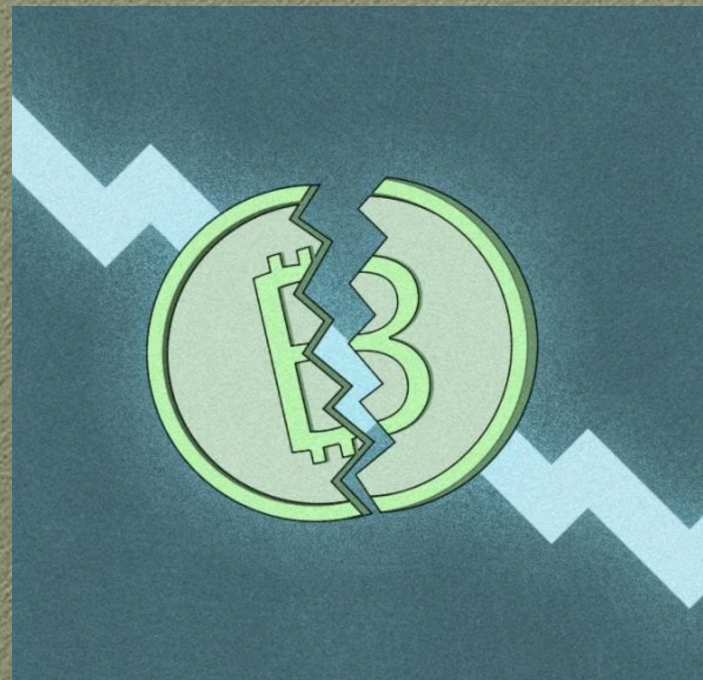# CRYPTOCURRENCY, BLOCKCHAIN, AND A NEW ECONOMIC WORLD

OLLI
LATE SUMMER 2021
LECTURE 5
BEBO WHITE - BEBO.WHITE@GMAIL.COM

County I.T. Supervisor Mined Bitcoin at the Office, Prosecutors Say

Christopher Naples is accused of hiding 46 devices used for mining cryptocurrency in Suffolk County offices, costing the county thousands of dollars in electricity.

By Jonah E. Bromwich

Sept. 8, 2021

A Long Island man was charged on Wednesday with using his position as an I.T. supervisor for Suffolk County to mine cryptocurrency from government offices, costing the county thousands of dollars in electricity.

Prosecutors said that Christopher Naples, 42, of Mattituck, L.I., had hidden 46 specialized devices used to mine Bitcoin and other cryptocurrencies in six rooms in the Suffolk County Center in Riverhead, including underneath floorboards and inside an unused electrical panel.

Sen. Elizabeth Warren calls crypto the 'new shadow bank'

The Massachusetts senator said that it's "worth considering" banning U.S. banks from holding the reserves to back private stablecoins.
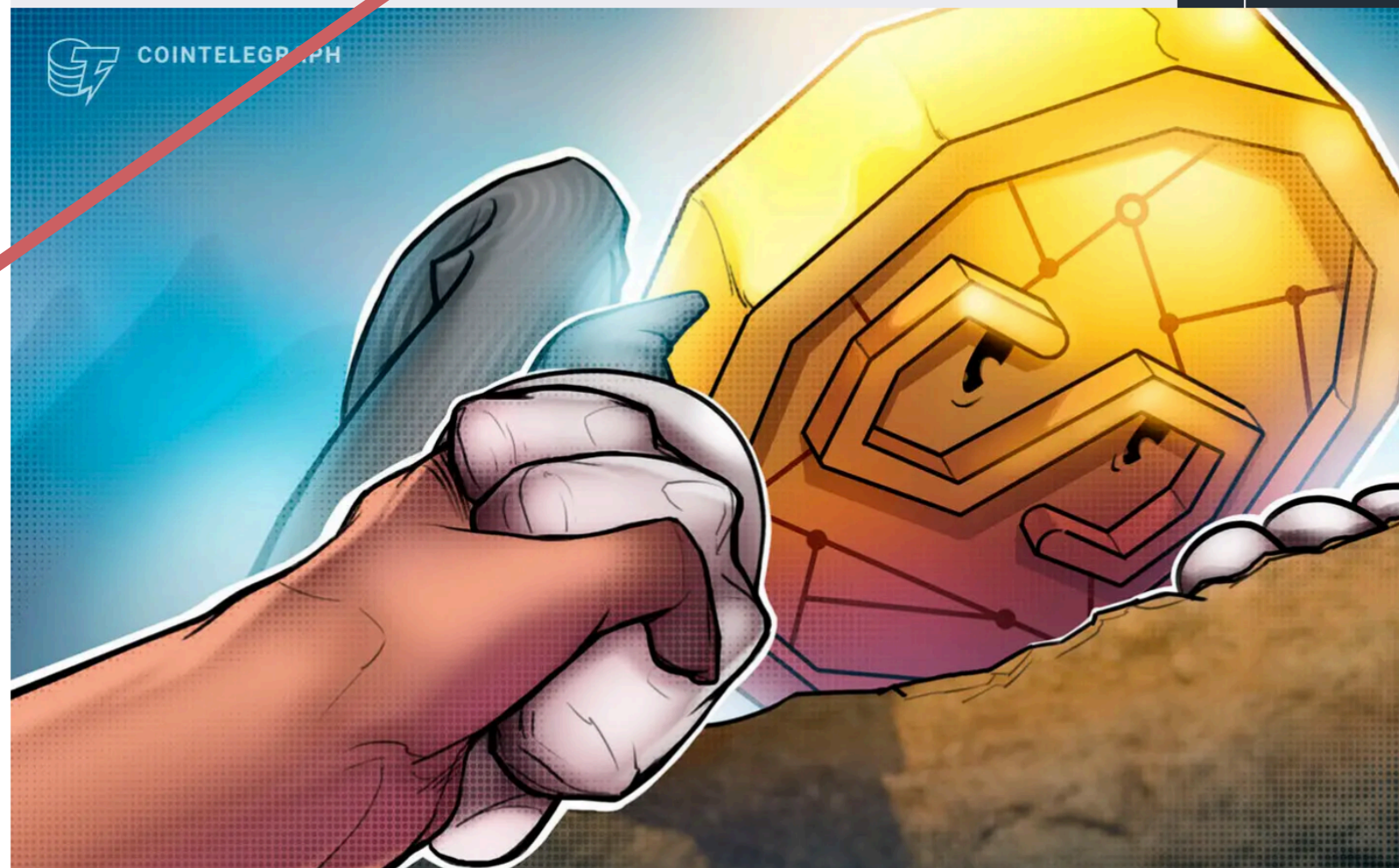
The cryptocurrency industry offers "many of the same services" as shadow banks but still lacks "consumer protections or financial stability that back up the traditional system"
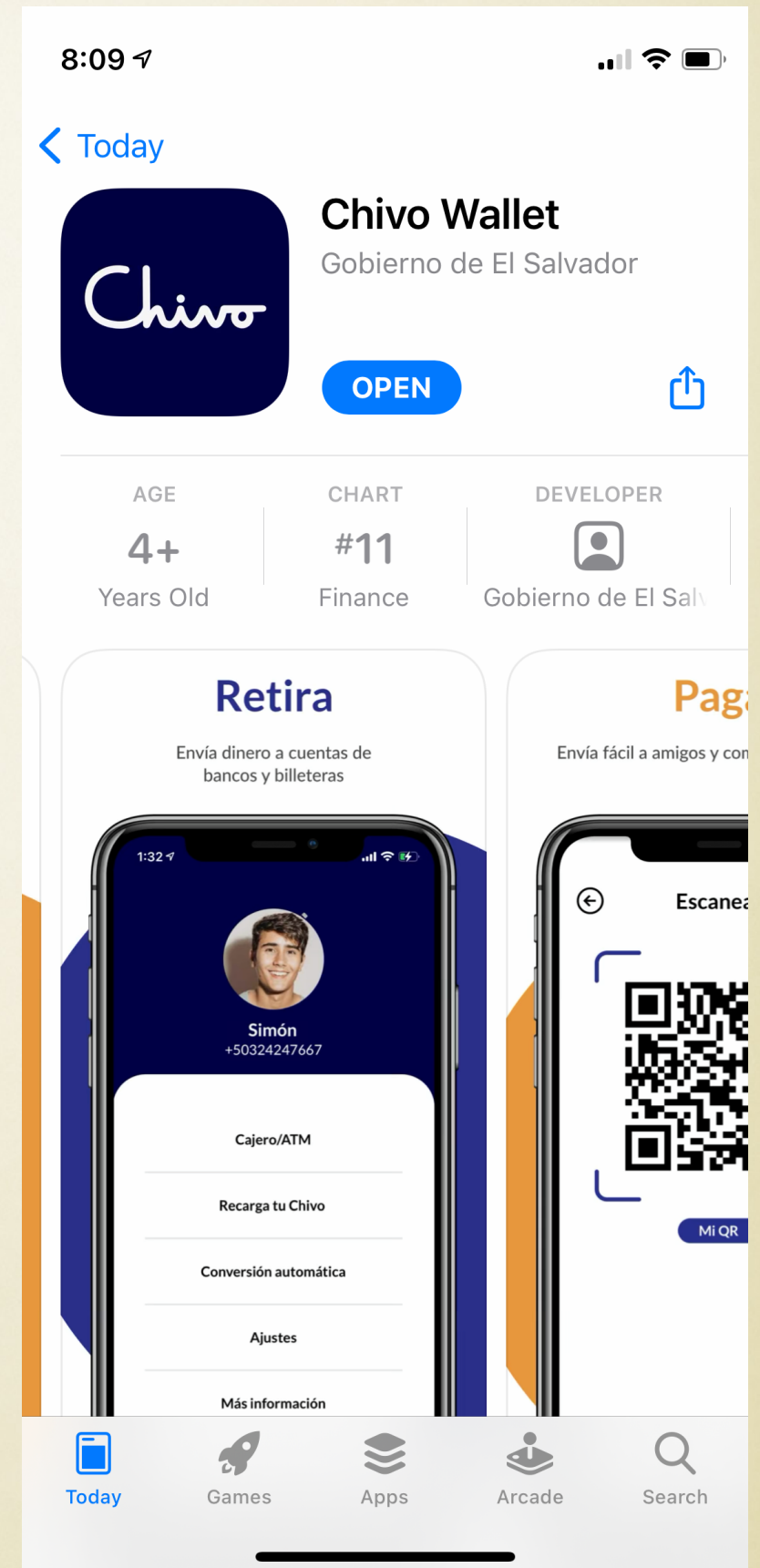
3

THOUSANDS OF PEOPLE PLAN TO BUY $30 OF BITCOIN TO CELEBRATE EL SALVADOR

People from all over the world are planning on buying $30 worth of bitcoin to celebrate El Salvador making it legal tender.

NIK HOFFMAN · 5 HOURS AGO
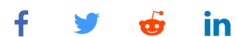
The world is about to change forever as today is the last day on planet Earth where bitcoin won't be legal tender somewhere. Because tomorrow, BTC officially becomes legal tender in El Salvador, marking a historic milestone in Bitcoin's journey to becoming the world reserve currency.

Chivo Wallet
Gobierno de El Salvador

OPEN

AGE	CHART	DEVELOPER
4+	#11	
Years Old	Finance	Gobierno de El Sal

Today · Games · Apps · Arcade · Search

QUESTIONS FROM LECTURE 4

How can a contract be executable? Is a contract not a <u>fixed</u> thing? Example?

DApps seems to be worse than Facebook - at least I know where Facebook is and who runs it.

DeFi - if no intermediaries, who resolves conflicts?

If it is true that BTC uses as much electricity as Greece - who pays for it? with what? (crypto?)

Who pays for the mining rigs?

How do I know the executable code has not been corrupted?

THE TEN MINUTE BTC TRANSACTION TIME APPEARS IMPLAUSIBLE/UNUSABLE

- <u>yes, it is</u>; transaction speed is an indicator of how long it takes to approve a transaction on the blockchain;

- for BTC the approval of one transaction is 10 minutes; overall for the entire network is 7 transactions/second

- who does it better?

  - Ripple - transaction approval 3-5 sec = 1,500 transactions/sec;

  - EOS (for DeFi) - 2,800 transactions/second

  - Ethereum - 10 transactions/second; Ethereum 2.0 - 10,000 transactions/second

- will this ever compete with Visa, Mastercard?

WHAT DOES BITCOIN HALVING MEAN AND HOW DOES IT RELATE TO THE MAXIMUM QUANTITY?

- after every 210,000 blocks mined (~ 4 years), the block reward to miners for processing transactions is cut in half

- the last was May 11, 2020

- this cuts in half the rate at which new BTC are put into circulation

- this continues until all BTC are put into circulation (21 million)

- halving is a <u>synthetic</u> form of inflation

- imagine if the amount of gold mined was cut in half every 4 years

  - gold's value is based on relative scarcity

  - gold halving would drive the demand/price up

Bitcoin: Price, USD

Bitcoin has formed a local peak within 1.5 years of both historical block reward halvings.

Cryptocurrencies   Exchanges   NFT   Portfolio   Watchlist   Calendars   Products   Learn   Log In   **Sign up**

🟠 Bitcoin Halving Countdown

Bitcoin block reward will decrease from 6.25 to 3.125 coins in approximately

866	**12**	**27**	**1**
Days	Hours	Minutes	Seconds

Tell your friends about this historic event! Share now:

Current block
699,522

Halving at Block **840,000**   Blocks left **140,478**

(on 9/7/2021 at 1 pm)

ON THE SUBJECT OF VOLATILITY, PLEASE SAY MORE ABOUT SCARCITY

- <u>scarcity</u> is the gap between the limited supply of various resources and the limitless want of people

- <u>non-scarce</u>

  - the <u>dollar</u> is non-scarce since it can be printed at will

- <u>relatively scarce</u> resources do not have an (apparently) fixed supply, so whenever the demand increases, supply will also eventually increase to meet demand

  - <u>gold</u> is only scarce relative to the amount of energy put into mining it

- <u>absolute scarce</u> resources have a finite, fixed supply, so whenever the demand increases, there is no additional supply response to meet it

  - <u>bitcoin</u> is absolutely scarce since no matter how much energy is put into mining it, the issuance rate and maximum supply remains the same

The Next Frontier: Space Miners Are the Universe's Future Tycoons

Asteroid mining is the new Wild West, and the resources hidden in asteroids, potentially worth trillions, are available to whomever can get there first.

THE IDEA OF PURELY DIGITAL ASSETS (BEYOND MONEY) IS NOT NEW
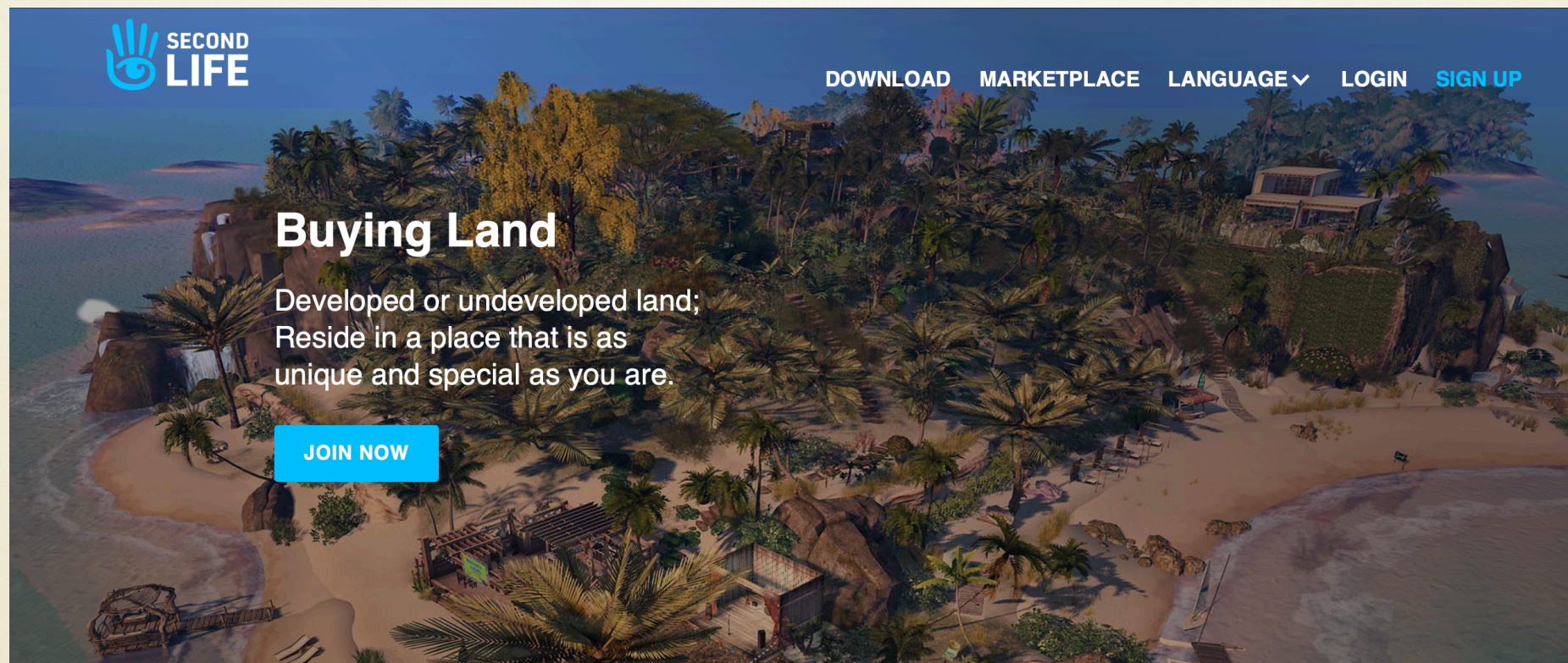
(when I say purely digital - not digitized from another medium - photos, music, books, etc.)

WHAT ABOUT DOMAIN NAMES?

- olli.sfsu.edu is just bits in databases

- domain names have collectively been given value via accepted protocols

- they have value because they are unique

- large amounts of money have been made/paid for domain names - registration might cost ~US$50

  - cars.com - US$872 million

  - hippo.com - US$3.3 million (last week)

  - NFTBay.com - US$30 thousand (last week)

REMEMBER TOKENS?

- crypto assets that are used on <u>decentralized applications</u>

- usually built on alternative blockchains from <u>altcoins</u>

- <u>Initial Token Offering</u> (ITOs) - similar in concept to ICOs

- tokens can have proven (or unproven) intrinsic utility, e.g., granting investors access to a platform through a subscription, with token holders unlocking the right to use exclusive services with a system, etc.

- tokens are essentially smart contracts that can be bought and sold

FUNGIBILITY IS A CORE IDEA OF CRYPTOCURRENCY

- For example,

  - bitcoin is *fungible*, (i.e., they can be traded or exchanged, one for another)

  - one bitcoin is always equal in value to another bitcoin

  - 1 satoshi will always be equal to .000000001 bitcoin and equal to another satoshi

  - if your wallet has 5 bitcoin, you can spend parts of it however you wish (just like fiat currency): 5, 4+1,3+2,2+2+1, etc.

- non-fungibility suggests uniqueness and non-interchangeable

  - e.g., a one carat diamond is not directly interchangeable with another one carat diamond since they may have unique features

NOW TRY TO WRAP YOUR HEAD AROUND NFTs

WTF IS AN NFT? (1/3)

- <u>non-fungible tokens</u> (NFTs) are making big news

- NFTs are smart contract data entries (tokens) on a blockchain that are <u>digitally signed</u> and declared a <u>unique</u> asset

- people "mint" NFTs creating a record of ownership that cannot be changed by anyone except the owner

- they are therefore <u>not interchangeable</u>, i.e., <u>non-fungible</u>

- the asset can be any type of digital file e.g., photographs, videos, audio file, software source files, etc.

- remember, these are digital files (bits) and not tangible items e.g., baseball cards (which are also non-fungible)

WTF IS AN NFT? (2/3)

- value of an NFT = <u>utility</u> + <u>ownership history</u> + <u>future value</u> + <u>liquidity premium</u>

- <u>utility</u> - how it can be used

- <u>ownership history</u> - who issued it and previous owners

- <u>future value</u> - scarcity and speculation

- <u>liquidity premium</u> - "on-chain vs. off-chain" - ease of selling

WTF IS AN NFT? (3/3)

- an NFT is a contract and can include whatever might be appropriate in a contract

- for example, the issuer of an NFT could demand a royalty when/if the asset is resold

NFTs are not DRM

- both deal with digital assets but

- DRM (digital rights management) restricts who can access various media

  - Amazon uses DRM to sell Kindle books and restrict who can read them

  - Spotify uses DRM to allow you to download music but not share it with non-subscribers

- an NFT is just a public record of a contract

"The Honus Wagner baseball card is $0.50 of physical goods (cardboard/ink) and $3M of virtual value (scarcity and demand); a rare Nike sneaker is $5 of physical goods (plastic/rubber) and $500 of virtual value; NFTs are going to take this phenomenon to Internet scale"

IT ALL STARTED WITH DIGITAL CATS
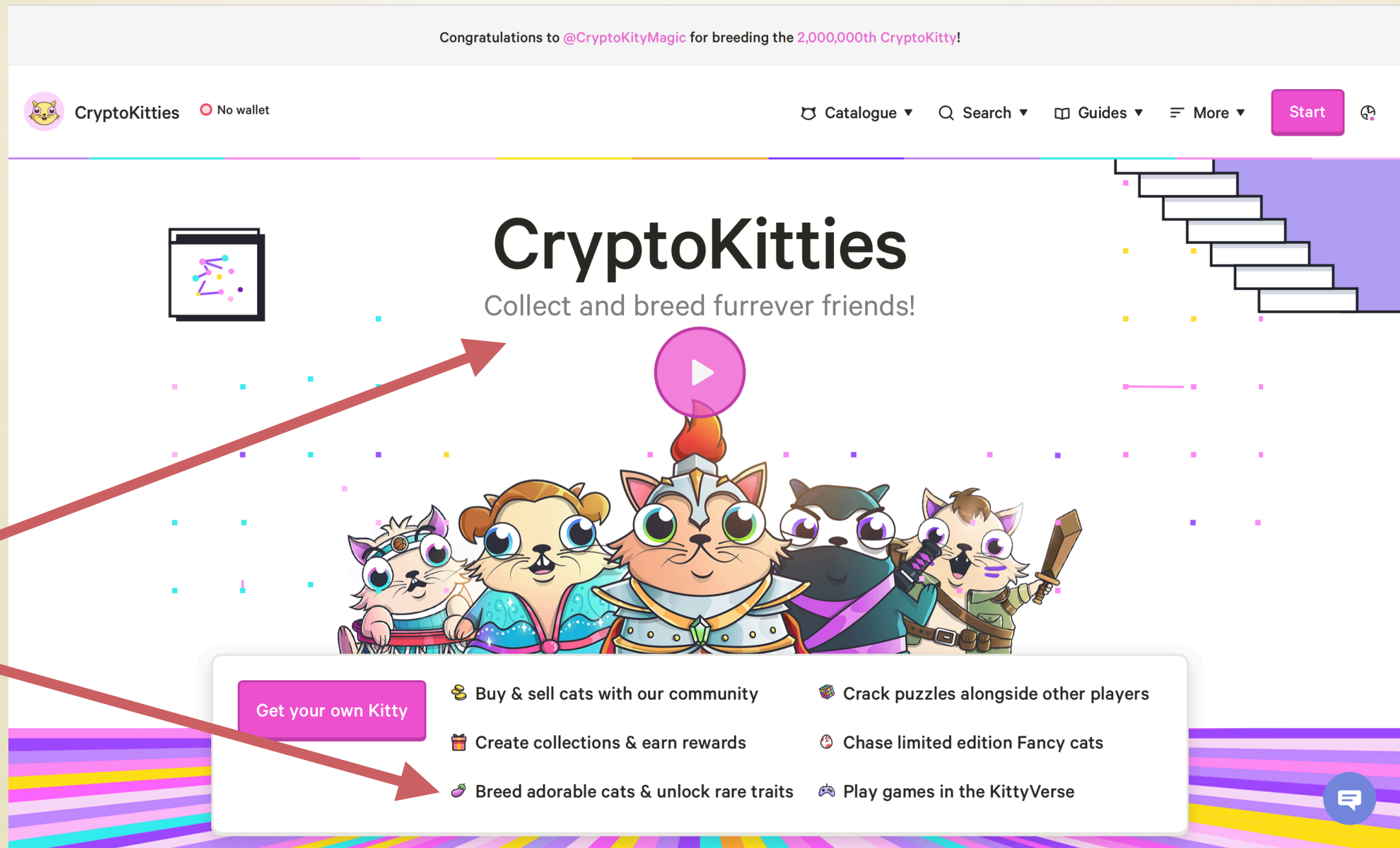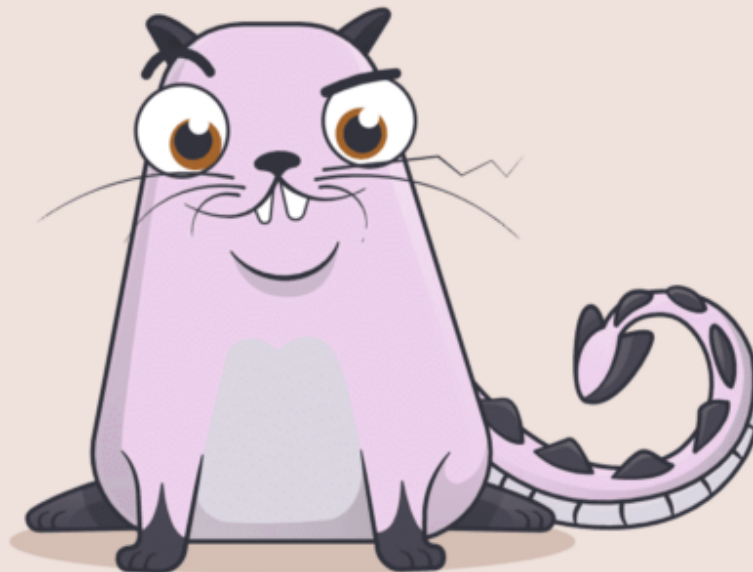
Dragon - 600 ETH ~= $390,000

Beeple's opus

Created over 5,000 days by the groundbreaking artist, this monumental collage was the first purely digital artwork (NFT) ever offered at Christie's

EVERYDAYS: THE FIRST 5000 DAYS sold online for $69,346,250

NEWS ▾ GOVERNMENT SECURITY FINANCE EVENTS ▾ RESOURCES ▾ PODCAST   LOG IN SUBSCRIBE

Bids soar to US$2.8 million for World Wide Web code NFT

By Staff Writer
Jun 29 2021
6:35AM

0 Comments

As auction nears end.

Bids for a non-fungible token of the original source code for the World Wide Web written by inventor Tim Berners-Lee have soared to US$2.8 million (A$3.7 million) from an opening price of US$1000 with two days to go until the Sotheby's auction ends.

Berners-Lee, a London-born computer scientist, invented the World Wide Web in 1989, revolutionizing the sharing and creation of information in what is seen as one of the

WHAT IS A POSITION ON A BLOCKCHAIN WORTH?

- a blockchain is a linked list (queue) of entries that indicate

  - a record of when an entry was added e.g., cryptocurrency mining

  - an immutable chronology of transactions

  - an immutable record of ownership

- entries are available for all to see
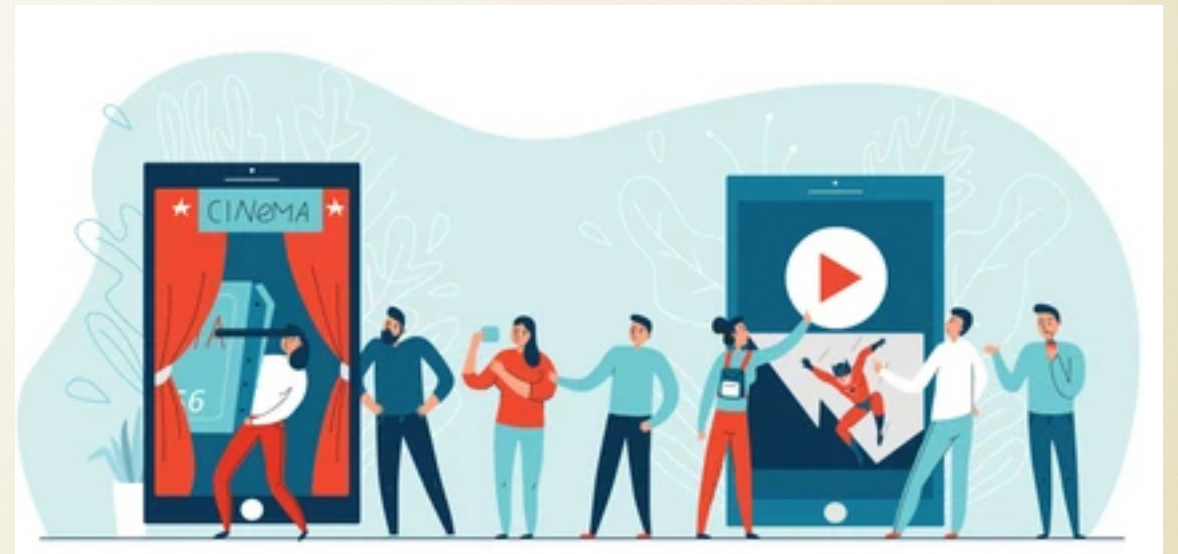
What would you pay to be first in line? Why?
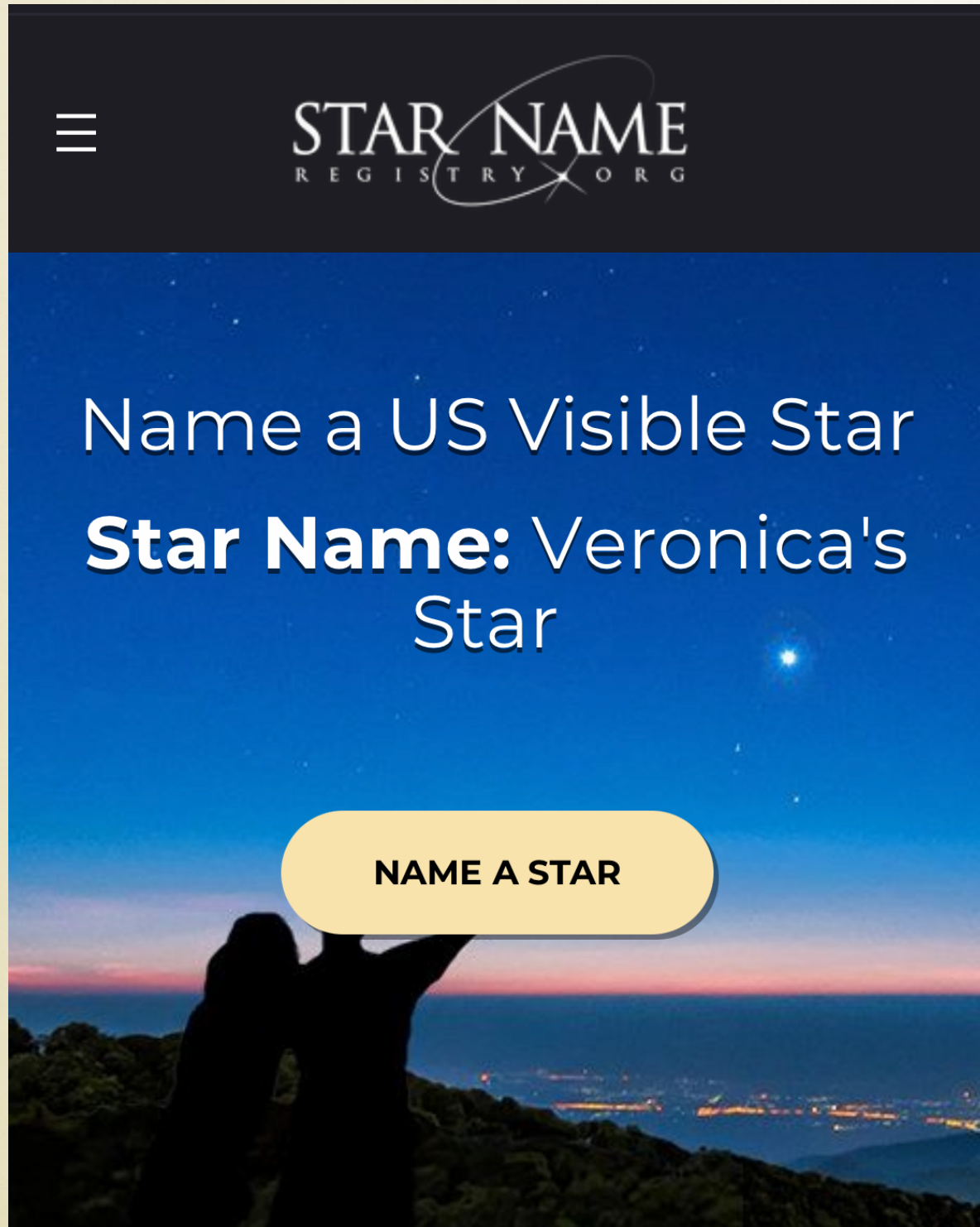
WHAT IS THE BUYER OF AN NFT ACTUALLY GETTING? (1/3)

- bragging rights to a cryptographic asset that is linked to an object - not the object itself

- a position on a blockchain connected to that object; a sale is completed when a position on a blockchain of the seller is transferred to the buyer's account

- the buyer has the right to sell, trade, donate that position as they wish

REMEMBER THESE?

STAR NAME
REGISTRY.ORG

Name a US Visible Star

Star Name: Veronica's Star

NAME A STAR

LUNARLAND.COM
Earth's Oldest, Most Recognized Celestial Real Estate Agency

NAVIGATION MENU

Moon Land Available
Since Inception Millions of Acres Sold

ACRES OF LAND ON THE MOON FOR SALE

IAOHPE Authorized

Every deed is recorded and registered in the International Association Of Human Planetary Exploration (IAOHPE).

As Seen on TV

Lunar Land has been featured on BBC, Conan, NBC, CNN, Fox News & more

WHAT IS THE BUYER OF AN NFT ACTUALLY GETTING? (2/3)

- an NFT does not mean ownership of the linked object, for example in the case of the Beeple art

  - all the buyer owns is blockchain position

  - the art is still available online in non-identifiable copies

  - the artist has not granted the buyer any <u>copyright</u> license e.g., proceeds from postcards, posters, etc.

  - the buyer doesn't have any <u>property</u> rights e.g., the buyer of the WWW NFT cannot claim ownership of the Web (it's open source anyway)

WHAT IS THE BUYER OF AN NFT ACTUALLY GETTING? (3/3)

MARCH 3, 2021 8:00AM ET

Kings of Leon Will Be the First Band to Release an Album as an NFT

The band's revolutionary tokens will unlock special perks like limited-edition vinyl and front row seats to future concerts

By **SAMANTHA HISSONG** ⊕

Multiple purchasers

Music still available via usual channels but NFT owners get special privileges

All handled in a smart contract

Search by creator or collectible

All   Art   Celebrities   Gaming   Sport   Music   Crypto

72 Editions Minted   18 for Sale

Hello

STARTING FROM

$**420**

Klarens x Lionel Richie

3 Editions Minted   1 for Sale

Three Madonnas (Yellow)

$**250,000**

Boy George

5 Editions Minted   3 for Sale

Three Madonnas (Green)

STARTING FROM

$**18,880**

Boy George

Steph Curry jumps into NFTs with $180,000 purchase of Bored Ape digital artwork
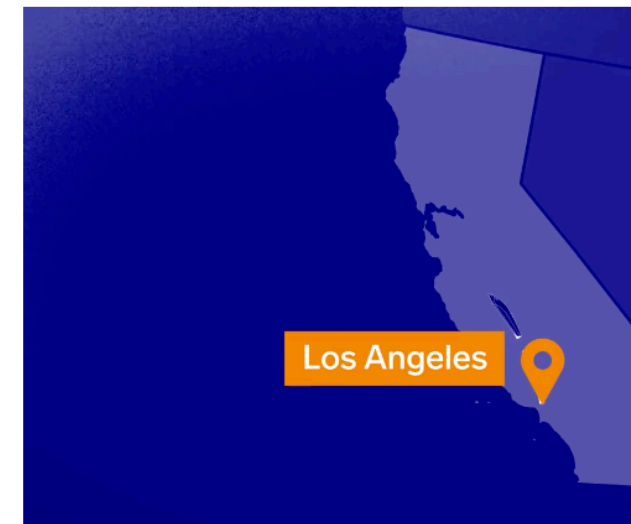
Isabelle Lee

Aug. 30, 2021, 09:19 AM

SHARE

NBA superstar Stephen Curry (left). Stephen Curry's Bored Ape Watch Club NFT (right).

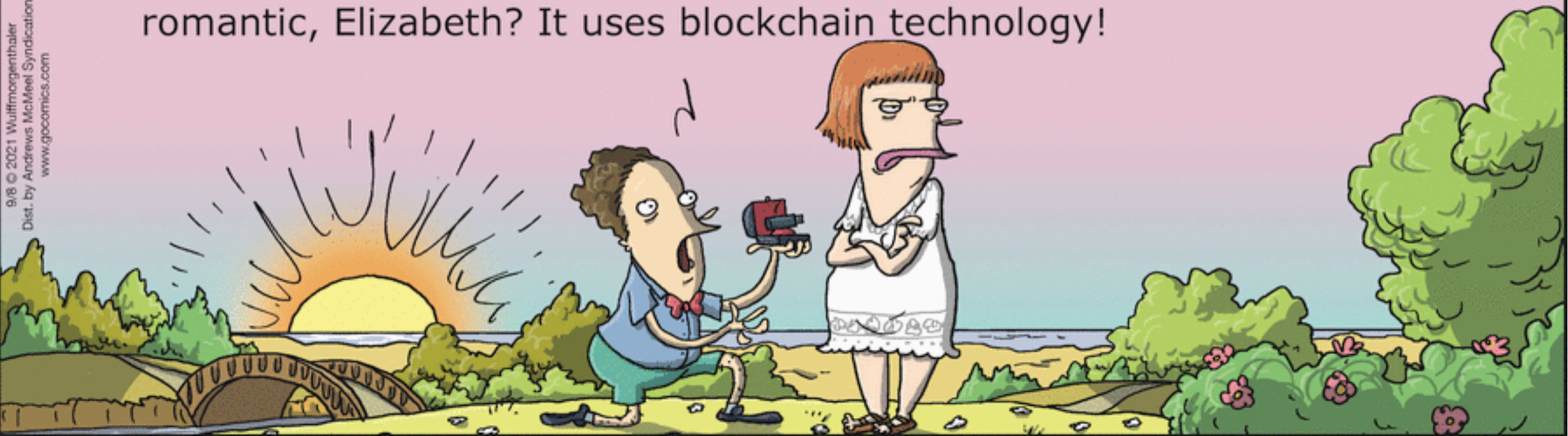Bill O'Leary/The Washington Post via Getty Images and Bored Ape Watch Club NFT.

- **Stephen Curry has bought a $180,000 ethereum-based NFT from the Bored Yacht Club collection**

THANKS TO MARY

WE HAVE COME FULL CIRCLE

Ether Rock - Pet Rocks On The Blockchain

Launched in 2017, EtherRock was one of the first crypto collectible NFT-type projects on the Ethereum blockchain, having launched shortly after CryptoPunks. Only 100 rocks can ever be available, and each new virgin rock gets more and more expensive. This game is built entirely on the Ethereum blockchain, with a *decentralized* smart contract (deployed here (https://etherscan.io/address/0x41f28833be34e6ede3c58d1f597bef429861c4e2)) used to manage everything including the buying and selling of rocks, their prices and owners (though this website is still necessary so you can see pretty pictures of the rocks).

These virtual rocks serve NO PURPOSE beyond being able to be brought and sold, and giving you a strong sense of pride in being an owner of 1 of the only 100 rocks in the game :)

How to play: you must be connected to the Ethereum mainnet to view info on rocks, and some Ether (the currency of Ethereum) to buy a rock. The easiest way to connect to the Ethereum mainnet is to use the MetaMask plugin for Chrome (https://chrome.google.com/webstore/detail/metamask/nkbihfbeogaeaoehlefnkodbefgpgknn?hl=en) -- go ahead and install it (takes 1 minute), then refresh this page. To get Ether you will need to buy some from an exchange like Coinbase.

Own a rock? Go to the rock management console allowing you to sell, hold or transfer your rock.

etherrockcom@gmail.com | Discord (https://discord.gg/cuzYmchbQx) | Twitter (https://twitter.com/etherrockcom) | Latest rock prices (https://twitter.com/etherrockprice) | **NFT Sprites** (https://nftsprites.com) (An NFT project launched in March 2021 by the same developer)

Latest Virgin Rock [Never Before Sold]

All 100 rocks have been sold. You can purchase non-virgin rocks below, if they have been listed for sale by their owners. Beware of any other projects claiming to sell rock NFT's, which may either be scams and/or using buggy exploited contracts (e.g. "we like the rocks" or weliketherocks.com). Read more on projects to avoid.

All Active (USED) Rocks

Once you connect to the Ethereum mainnet, information on all the rocks Ethereum users have brought would be shown below. Any rocks that users have listed for sale could also be brought here.

Rock ID 0 NO INFO	Rock ID 1 NO INFO	Rock ID 2 NO INFO	Rock ID 3 NO INFO	Rock ID 4 NO INFO
???	???	???	???	???
Rock ID 5 NO INFO	Rock ID 6 NO INFO	Rock ID 7 NO INFO	Rock ID 8 NO INFO	Rock ID 9 NO INFO
???	???	???	???	???

MARKETS   BUSINESS   INVESTING   TECH   POLITICS   CNBC TV   WATCHLIST   PRO 🔒

CRYPTO DECODED

CRYPTO DECODED

Somebody just paid $1.3 million for a picture of a rock

PUBLISHED MON, AUG 23 2021·6:17 PM EDT | UPDATED MON, AUG 23 2021·9:37 PM EDT
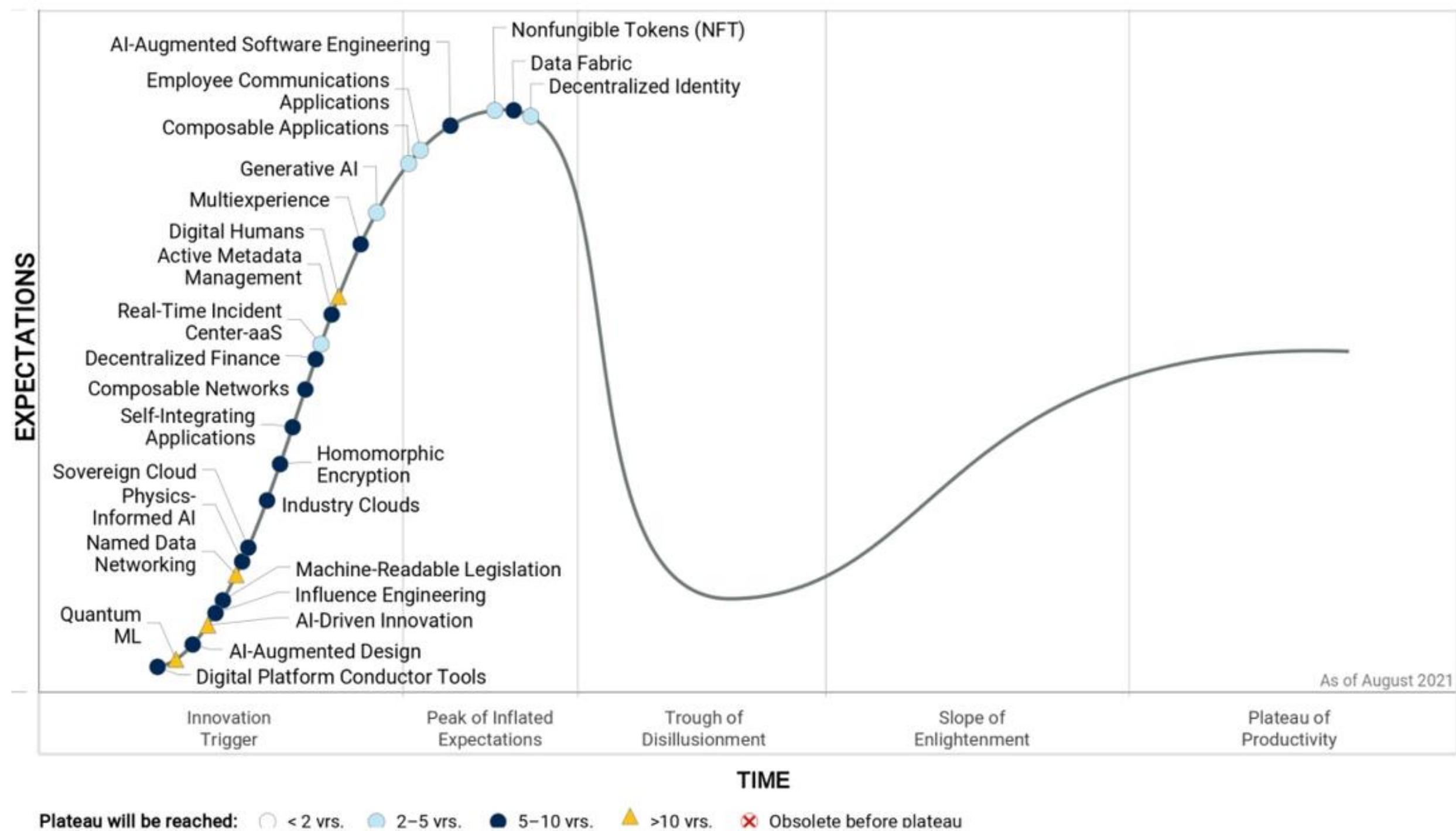
MacKenzie Sigalos
@KENZIESIGALOS

SHARE

KEY POINTS

- Clipart of a rock just sold for 400 ether, or about $1.3 million, late Monday afternoon.

- The transaction marks the latest sale of EtherRock, a brand of crypto collectible that's been around since 2017 — making it one of the oldest non-fungible tokens (NFTs) on the block.

36

Hype Cycle for Emerging Technologies, 2021

Source: Gartner (August 2021)

747576

Investing ▾   Stocks ▾   Funds ▾   **Crypto** ▾   Real Estate ▾   Retirement ▾   Personal

Are NFTs the Right Investment for You?

NFTs are truly a new thing. Blockchain and cryptocurrencies have been around for nearly a decade, but NFTs haven't been around that long. But like all things connected with cryptocurrency investments, NFTs are on a tear. *Some are even selling for millions of dollars.*

Does that make them an investment, or more particularly, the right investment for you?

At this point in the game, it seems as if **NFTs are speculations and not true investments**. The bubble in cryptocurrencies seems to have extended to all things connected to them, including NFTs.

If you do speculate in NFTs, make sure you're doing it with as little money as possible. **Not only are these assets totally unpredictable, but they have not stood the test of time**. Nor do they provide any type of cash flow, like interest or dividends.

Think of them as something you buy only with money you can afford to lose.

Volatility of cryptocurrency vs. volatility of NFTs

This could not have been foreseen by Satoshi

SAINTS, SINNERS AND SCHEMERS

MT. GOX

- "Magic: The Gathering Online Exchange" launched in 2010 for game trading cards; became a bitcoin exchange a year later

- 2013-early 2014 handled 70% of all BTC transactions worldwide

- 2014 - announced that ~850,000 BTC missing and likely stolen; 200,000 were later found

- blame was placed on hacking and embezzlement

- CEO arrested in August 2015

- May 2016, creditors claimed they lost US$ 2.4 trillion

_____

The Willy Report: proof of massive fraudulent trading activity at Mt. Gox, and how it has affected the price of Bitcoin

Posted on May 25, 2014

Somewhere in December 2013, a number of traders including myself began noticing suspicious bot behavior on Mt. Gox. Basically, a random number between 10 and 20 bitcoin would be bought every 5-10 minutes, non-stop, for at least a month on end until the end of January. The bot was dubbed "Willy" at some point, which is the name I'll continue to use here. Since Willy was buying in such a recognizable pattern, I figured it would be easy to find in the Mt. Gox trading logs that were leaked about two months ago (there's a torrent of the data here). However, the logs only went as far as November 2013; luckily, I was able to detect the buying pattern in the last few days of November. Below is a compiled log of its trades on the last two days of November (from the file "2013-11_mtgox_japan.csv"):

```
29-11-2013 0:38 - UID: 817985 Type: buy Currency: USD BTC: 10.02069695 Fiat: 11011.54
29-11-2013 0:47 - UID: 817985 Type: buy Currency: USD BTC: 16.80501168 Fiat: 18256.07
29-11-2013 0:56 - UID: 817985 Type: buy Currency: USD BTC: 13.46333525 Fiat: 15078.58
29-11-2013 1:01 - UID: 817985 Type: buy Currency: USD BTC: 14.60390798 Fiat: 16324.46
29-11-2013 1:10 - UID: 817985 Type: buy Currency: USD BTC: 18.89383201 Fiat: 21909.61
29-11-2013 1:15 - UID: 817985 Type: buy Currency: USD BTC: 12.63500728 Fiat: 14339.39
29-11-2013 1:21 - UID: 817985 Type: buy Currency: USD BTC: 15.36861265 Fiat: 17395.3
29-11-2013 1:30 - UID: 817985 Type: buy Currency: USD BTC: 13.69985504 Fiat: 15469.14
29-11-2013 1:40 - UID: 817985 Type: buy Currency: USD BTC: 16.24860284 Fiat: 18411.35
29-11-2013 1:46 - UID: 817985 Type: buy Currency: USD BTC: 13.08811052 Fiat: 14901.38
29-11-2013 1:53 - UID: 817985 Type: buy Currency: USD BTC: 15.95674773 Fiat: 18116.97
29-11-2013 2:01 - UID: 817985 Type: buy Currency: USD BTC: 13.37224115 Fiat: 15224.97
29-11-2013 2:10 - UID: 817985 Type: buy Currency: USD BTC: 19.88618992 Fiat: 22699.37
29-11-2013 2:16 - UID: 817985 Type: buy Currency: USD BTC: 14.53897264 Fiat: 17228.68
29-11-2013 2:24 - UID: 817985 Type: buy Currency: USD BTC: 13.06074749 Fiat: 15496.65
29-11-2013 2:31 - UID: 817985 Type: buy Currency: USD BTC: 17.2701824 Fiat: 20845.52
29-11-2013 2:40 - UID: 817985 Type: buy Currency: USD BTC: 12.01285719 Fiat: 14394.19
```

Gox Rising Limited

Gox Rising Limited ("Gox Rising" or the "Company"), a BVI company, was established in January 2019 to help drive the ongoing Mt. Gox Civil Rehabilitation process to a positive conclusion.

The Company is exploring options to create value for those hurt by the Mt. Gox bankruptcy in 2014, including potentially launching a new future crypto exchange with the voluntary participations of participating Mt Gox Creditors. Gox Rising will also consider acquiring claims of Mt Gox Creditors with a need or desire for liquidity.

If you are Mt. Gox Creditor or know someone that might be looking for liquidity, click here *for more information.*

SILK ROAD (1/3)

- online black/darknet market place

- launched in 2011

- known for anonymous transactions using bitcoin

- shut down after Ross Ulbricht ("Dread Pirate Roberts" was arrested in San Francisco

- Ulbricht was ultimately sentenced to life in prison without possibility of parole

SILK ROAD (3/3)

- "honor amongst criminals"

  - Ulbricht only allowed "victimless crimes" - no child porn, WMDs, stolen credit card numbers, etc.

  - after investigation, FBI and DHS agents reported that Silk Road was surprisingly reliable in both delivery and quality…

FOR A SHORT TIME THE US GOVERNMENT WAS ONE OF THE LARGEST OWNERS OF BITCOIN!

- approximately 315,000 bitcoin was seized from Silk Road and Ulbricht (> US$16 billion at today's rates!)

- auctioned off by the US Government

- one of the investigating Secret Service agents was arrested and imprisoned for stealing bitcoin from Silk Road

1A7QdSuQ6x86eYKM57EyyD9AZipTJpUXum   ➡   US Marshal Auction coins ⧉   0.0001 BTC

0.0001 BTC

421a10d9480778aa66b1cdbc4d10beec46565bcf8c17d3853964d80300d63337   2014-07-01 20:43:53

1NhPPVto17umjztua1wpmg3ma4K2eL2S6w   ➡   US Marshal Auction coins ⧉   0.001 BTC
1AUx6GYKUrQpZraBaaWh4AfkHRcaXiSWUV

0.001 BTC

9e95c3c3c96f57527cdc649550bf8e92892f7651f718d846033798aee333b0c3   2014-07-01 19:13:03

US Marshal Auction coins ⧉   ➡   1A6mFe9CMLXC4w4PDdbfihVrm33wTjnABD   2.28533471 BTC
1a8LDh3qtCdMF... (Tim Draper Auction ⧉)   29,656.51306529 BTC

-29,658.7984 BTC

9d060863f363cfed4da708fa95ff3b469d3bffa7fe9c7442e40ed2ecf49ba03e   2014-06-26 23:13:04

1EWZaeyKcM9wFN9qxmuhc2Zqmoq81yvnvV   ➡   US Marshal Auction coins ⧉   0.0001 BTC

0.0001 BTC

MONEY LAUNDERING

- problem: how do you take large quantities of dirty money and make it usable/spendable?

- you can't just walk into a bank and deposit it into your account - otherwise *Breaking Bad* and *Ozark* would have no plot line

- criminals have always been able to find a way so cryptocurrency is just another method

- anonymity, non-traceability, lack of regulations and easy transfer does make it attractive and straightforward

DEA

April 02, 2018
Contact: Erica C. Curry
Phone Number: (602) 664-5600

FOR IMMEDIATE RELEASE

Drug Enforcement Administration

Phoenix
Douglas W. Coleman, Special Agent in Charge
@DEAPhoenixDiv

DEA Phoenix Bitcoin Target Found Guilty Of Money Laundering

PHOENIX - The DEA announces the conviction of Thomas Mario Costanzo, a.k.a. Morpheus Titania, of Mesa, Arizona, by a federal jury on March 28, 2018, on five counts of money laundering in Phoenix. This long term investigation resulted in one of the first convictions of a money launderer in Arizona who utilized bitcoin in his criminal activities.

"The DEA is committed to identifying and targeting those criminals like Costanzo who utilize sophisticated methods such as bitcoin and the dark web to conceal their drug trafficking and money laundering enterprises," said Doug Coleman, the DEA Special Agent in Charge of Arizona. "The DEA and our law enforcement partners will never relent in its pursuit of justice against those who continue to destroy our communities with their illicit activities."

DEA United States Drug Enforcement Administration

Who We Are ∨   What We Do ∨   Resources ∨   Search 🔍

Home / Press Releases / 2018 / 07 / 09 / "Bitcoin Maven" sentenced to federal prison in virtual currency money laundering case

July 09, 2018
Contact: SA Kyle Mori
Phone Number: (213) 621-6700

FOR IMMEDIATE RELEASE

Drug Enforcement Administration

Los Angeles
David Downing, Special Agent in Charge
@dealosangeles

"Bitcoin Maven" sentenced to federal prison in virtual currency money laundering case

LOS ANGELES - The so-called "Bitcoin Maven," who admitted to operating an unlicensed bitcoin-for-cash exchange business and laundering bitcoin that was represented to be proceeds of narcotics activity, was sentenced today to 12 months and one day in federal prison, three years of supervised release, and a fine of $20,000.

Theresa Lynn Tetley, 50, of Southern California, a former stockbroker and real estate investor, was sentenced by United States District Judge Manuel L. Real for conducting an illegal business and engaging in unlawful monetary transactions involving bitcoins. Tetley was also ordered to forfeit 40 bitcoin, $292,264.00 in cash, and 25 assorted gold bars that were the proceeds of her illegal activity.

Tetley pleaded guilty to one count of operating an unlicensed money transmitting business and one count of money laundering.

How bitcoin is fueling America's opioid crisis

- Drug dealers are using bitcoin to finance the deadly wave of fentanyl flooding into the country from overseas.
- We follow the money from Main Street to the dark web and show how the cryptocraze allows drugs to get delivered right to your doorstep.

Ylan Mui | Karen James Sloan

Published 8:01 AM ET Fri, 13 April 2018 | Updated 10:16 AM ET Sun, 15 April 2018

CNBC

Bitcoin is Criminal Money Says the Media While Deutsche Bank Gets Raided for Laundering

RICK D. | NOVEMBER 29, 2018 | 5:00 PM

Deutsche Bank has been raided today on the suspicion of money laundering. The German institution was stormed by 170 officials and, weirdly enough, no Bitcoin was found on the scene.

Deutsche Bank Believed to Have Handled $354 Million in "Dirty Money" in 2016

The way the mainstream media talks about Bitcoin in relation to financial crimes, anyone would think money laundering is a completely new phenomenon, only enabled by the revolutionary fintech innovation. Of course, this is not the case and the point has been beautifully highlighted by today's news that Deutsche Bank AG has been raided based on allegations of concealing ill-gotten funds.

Organized crime is laundering money through Fortnite's in-game currency

Criminals are using stolen credit cards to buy Fortnite V-bucks, then selling the in-game currency for bitcoin at a discount on the dark web as a way to launder money.

From **The Independent**:

> Discounted V-bucks are being sold in bulk on the dark web – a hidden section of the internet only accessible using specialist software – as well as in smaller quantities on the open web by advertising them on social media platforms like Instagram and Twitter.

WeeklyPenny **24 Gadgets That May Go Out Of Stock Soon**

MONEY LAUNDERING IS A TWO-WAY STREET (1/2)

- suppose you are Ross Ulbricht or a cartel boss or a ransomware perpetrator or a coin exchange embezzler…

- how do you convert 1000s of bitcoin into fiat currency?

- you certainly don't buy a fleet of Teslas or a lot of bling (or do you?) or stand in front of an ATM for hours (or maybe you do?)

Bitcoin ATMs

A guide to cleaning cash

1. Walk up to a machine with a wad of cash.

2. Enter the amount of Bitcoin you want to buy.

3. Enter a burner phone number for a verification code to create an account.

4. Scan a QR code or have one printed for new accounts.

5. Plug in your cash and blindly accept whatever fees they charge.

6. Shred your receipt and sleep soundly knowing your clean, shiny Bitcoin has made it to its criminal destination.

Illustrations by Louisa Gagliardi

THE ROLE OF CRYPTOCURRENCY IN ORGANIZED CRIME MONEY LAUNDERING IS UNKNOWN

Laundering Drug Money: Why Mafia Can't Hide Behind Bitcoin

2593 Total views   191 Total shares

"there is no indication that El Chapo ever used cryptocurrency since it would be difficult to pay expenses - salaries, bribes, travel, safe houses, etc."

Criminal entities received ~US$ 5 billion in money in 2020 and those illicit entities distributed ~US5$ billion to other entities, representing <1% of overall cryptocurrency movements (Chainalysis)

CRYPTOCURRENCY "LAUNDRIES"/DARK EXCHANGES HAVE BECOME A COTTAGE INDUSTRY

Are these just for criminals?
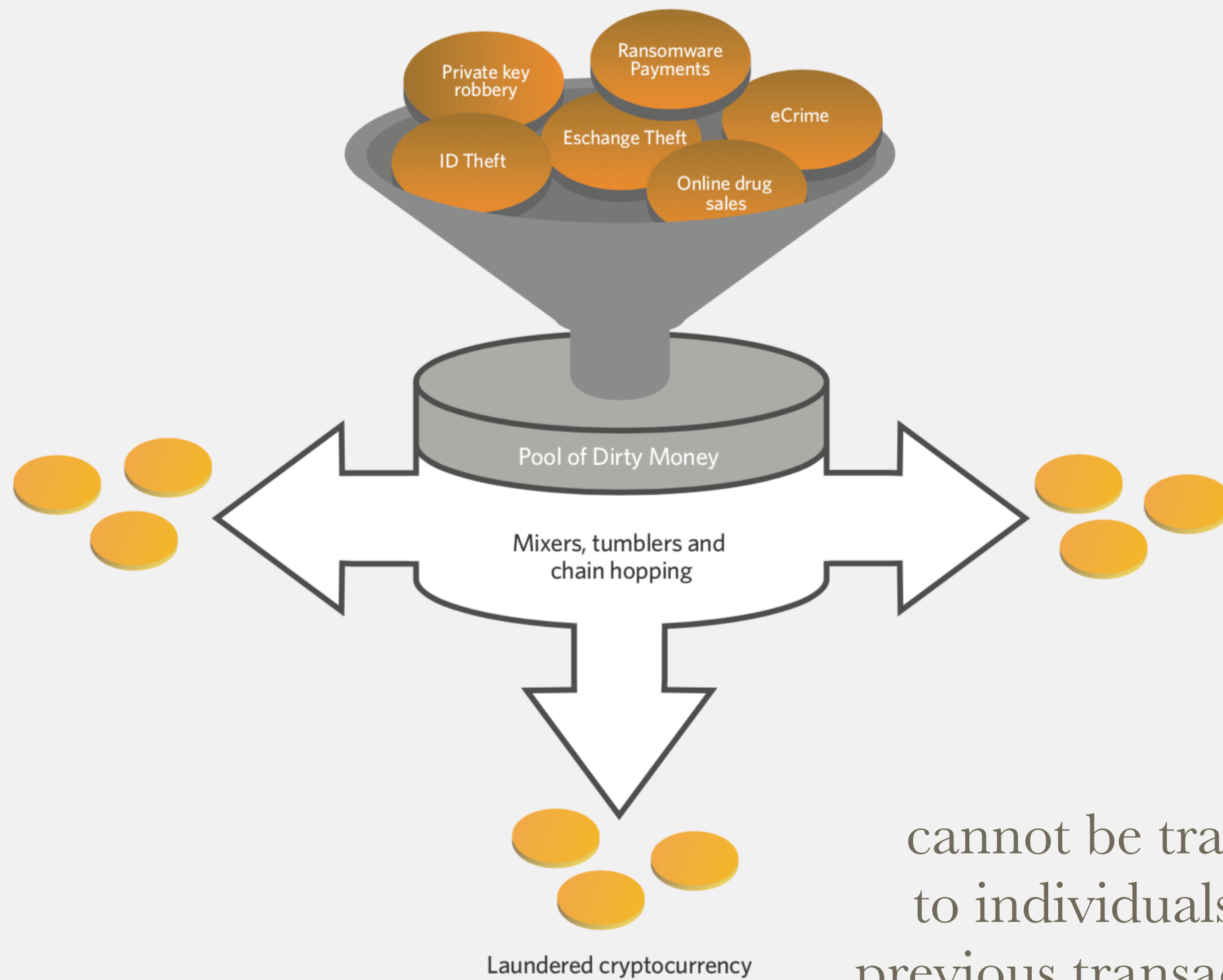
cannot be traced to individuals or previous transactions

MONEY LAUNDERING IS A TWO-WAY STREET (2/2)

- by using a coin exchange <u>you</u> could be a part of cryptocurrency laundering

- it is estimated that between 2011 and 2019 the main exchanges assisted in the distribution of 60-80% of bitcoin exchanges from known criminal actors (Elliptic)

- some exchanges have enhanced their Anti-Money Laundering (AML) and Know Your Customer (KYC) procedures and the share has dropped to 45%; other exchanges remain unregulated

- has anyone ever visited a business with money laundering connections?

RITZ

Old Poodle Dog
65 POST ST. ★ SAN FRANCISCO

FRENCH RESTAURANT

Over a Hundred Years of Service

In '49 a French couple opened the Poodle Dog Restaurant at Clay and Dupont Streets. In '68 it was moved to Bush and Grant Avenue where it became the "Old Poodle Dog." In the '90's my father, Calixte Lalanne, became one of the owners 'til it was destroyed by the earthquake and fire of 1906. In 1908 Lalanne and his associates opened the world famous Bergez Franks Old Poodle Dog at 415 Bush Street, and it remained there 'til prohibition closed its door. The name of Lalanne has been associated with San Francisco and its French restaurants for years.

LOUIS J. LALANNE, *Managing Owner*

1849 - 1868	1868 - 1906	1906 - 1908	1908
CLAY & DUPONT	BUSH & GRANT	EDDY & VAN NESS	415 - 427 BUSH

Telephone: 781-1919

COUNTERFEITING (1/2)

- counterfeiting fiat currency has been a problem <u>since the beginning</u>

    - <u>classic counterfeiting</u>

    - can be a form of state-sponsored terrorism, e.g., North Korea, Iran

    - has anyone ever suggested eliminating fiat currency as a way to combat counterfeiting?

- why don't we hear of cryptocurrency counterfeiting?

COUNTERFEITING (2/2)

- counterfeiting cryptocurrency is impossible - there is no physical medium

- counterfeiting cryptocurrency requires spending a single unit more than one time

- cryptocurrency/blockchain actively addresses the double spending problem

RANSOMWARE HAS BECOME THE POSTER CHILD FOR CRYPTOCURRENCY CRIME

Colonial Pipeline paid 75 Bitcoin, or roughly $5 million, to hackers.

The shutdown of the Colonial Pipeline triggered a cascading crisis that led to a jump in gas prices and panic buying at gas pumps. Erik S Lesser/EPA, via Shutterstock

By Nicole Perlroth

May 13, 2021

Colonial Pipeline paid its extortionists roughly 75 Bitcoin, or nearly $5 million, to recover its stolen data, according to five people briefed on the transaction.

The New York Times

Biden's Agenda › | Politics Updates   Taxing the Rich $4 Trillion Economic Plan   Liz Cheney

Majority of Colonial Pipeline Ransom Recovered, Justice Dept. Says

Last Updated June 15, 2021, 8:43 a.m. ET

"Earlier today, the Department of Justice has found and recaptured the majority of the ransom Colonial paid to the DarkSide network," the deputy attorney general said Monday. Vice President Kamala Harris, in Guatemala, discussed efforts to curb migration.

WHAT EXACTLY IS RANSOMWARE?

- ransomware is malicious software (malware) used in a cyberattack

- it is usually installed on the victim's computer system via social engineering e.g., phishing, spoofing, infected downloads, etc.

- it encrypts the victim's data with an encryption key known only to the attacker or downloads sensitive data

- unless the victim pays a designated ransom within a certain period of time, the data will be destroyed or sensitive data will be made public
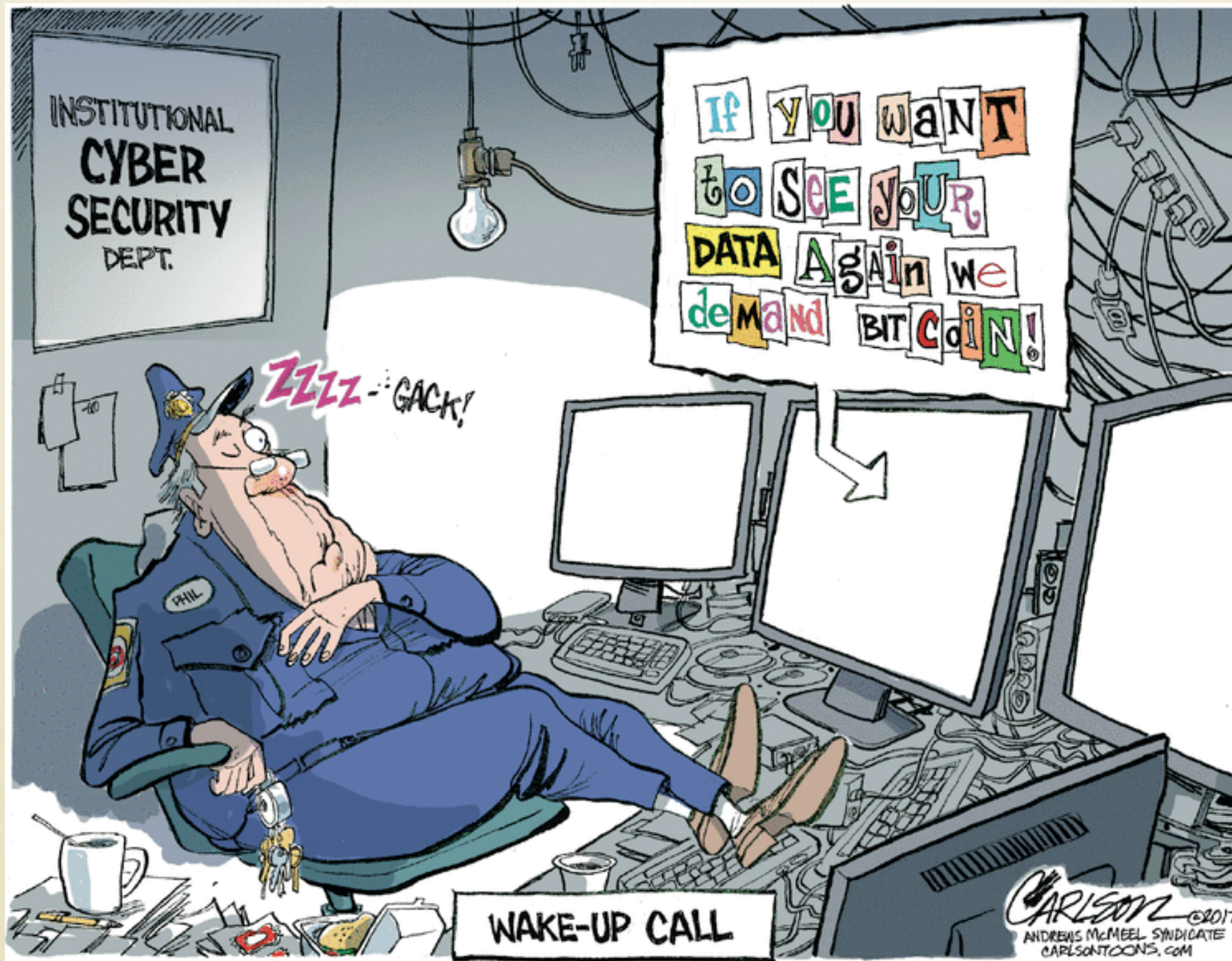
RANSOMWARE ATTACKS ARE ON THE RISE

- major U.S. cities have been victims crippling critical services e.g., Atlanta, Baltimore

- the San Francisco Bay Area has been hit

  - the SFMTA, Asian Art Museum

  - UCSF, Jewish Community Center

  - the Santa Clara Valley Transportation Authority

  - probably others we don't know about and ransom payments we were not told about

WHAT DOES CRYPTOCURRENCY HAVE TO DO WITH RANSOMWARE?

- cryptocurrency/BTC is one of the most popular ways for attackers to demand ransom

- why?

  - all payments can be made digitally and online - remember the attackers are usually tech-savvy

  - cryptocurrency is (supposedly) anonymous and non-traceable

  - attacker can readily verify that payment has been made

  - cryptocurrency can be easily converted to fiat currency e.g., $$

- there is certainly no required reason to use cryptocurrency

From [_____]com ☆

Reply   Forward   Archive   Junk   Delete   More ⌄

Subject **Your account has been hacked! You need to unlock.**   8/27/19, 12:45 PM

To [_____]com ☆

Hello!

I am a representative of the ChaosCC hacker group.
In the period from 03/06/2019 to 25/08/2019 we got access to your account [_____].com by hacking one of the [_____]com mail servers.

You already changed the password?
Sumptuously! But my program fixes this every time. And every time I know your new password!

Using access to your account, it turned out to be easy to infect the OS of your device.

At the moment, all your contacts are known to us. We also have access to your messengers and to your correspondence.
All this information is already stored with us.

We are also aware of your intimate adventures on the Internet.
We know that you adore adult sites and we know about your sexual addictions.
You have a very interesting and special taste (you understand what I mean).

While browsing these sites, your device's camera automatically turns on.
Video-record you and what you watch is being save.
After that, the video clip is automatically saved on our server.

At the moment, several analogy video records have been collected.
From the moment you read this letter, after 60 hours,
all your contacts on this email box and in your instant messengers will receive these clips and files with your correspondence.

If you do not want this, transfer 700$ to our Bitcoin cryptocurrency wallet: 1KE1EqyKLPzLWQ3BhRz2g1MHh5nws2TRk
I guarantee that we will then destroy all your secrets!

As soon as the money is in our account – your data will be immediately destroyed!
If no money arrives, files with video and correspondence will be sent to all your contacts.
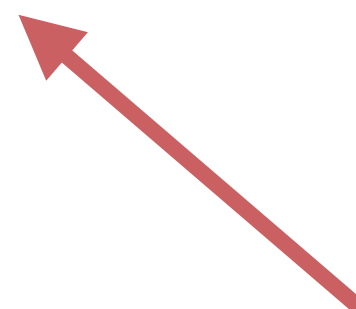
You decide... Pay or live in hell out of shame...

We believe that this whole story will teach you how to use gadgets properly!
Everyone loves adult sites, you're just out of luck.
For the future – just cover a sticker your device's camera when you visit adult sites!

Take care of yourself!

REMEMBER

- that only the sender (attacker) and receiver (victim) public keys are required to make payment

- public keys are public but not traceable to individuals

- details of the payment/transaction are securely recorded on the blockchain to establish "proof of payment"

- all of the above are anonymous and supported by strong and robust encryption techniques
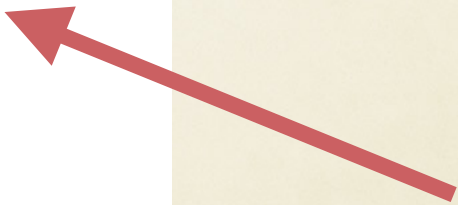
SO, HOW WAS THIS POSSIBLE?

The New York Times

Biden's Agenda › | Politics Updates   Taxing the Rich $4 Trillion Economic Plan   Liz Cheney

Majority of Colonial Pipeline Ransom Recovered, Justice Dept. Says

Last Updated June 15, 2021, 8:43 a.m. ET

"Earlier today, the Department of Justice has found and recaptured the majority of the ransom Colonial paid to the DarkSide network," the deputy attorney general said Monday. Vice President Kamala Harris, in Guatemala, discussed efforts to curb migration.

Where was the security?

SATOSHI'S CORE FRAMEWORK IS ROBUST AND SECURE

- it's the <u>on-ramps</u> and <u>off-ramps</u> to that framework that are vulnerable

- remember it's not the system's fault if you lose your keys (and your cryptocurrency); it's the system's robustness that offers no solution

- vulnerabilities can lie in software wallets, coin exchanges (many well-known examples), payment systems, etc.

- these are independent software services and applications that can interact with the core framework

Gemini: Buy
Bitcoin Instantly
GET ✕
Bitcoin Wallet & Exchange

MetaMask -
Blockchain Wallet
GET
Browse Web3 Sites & Use Cr...

BlockFi
GET
Earn, Borrow, Grow Wealth.

Voyager - Buy Bitcoin
& Crypto
Buy or Sell BTC & 50+ Altcoins

Trust: Crypto &
Bitcoin Wallet
GET
Buy Bitcoin and Cryptocurre...

Fold: Bitcoin
Cashback Rewards
GET
Earn BTC on everyday purch...

Kraken Pro
GET
Advanced Crypto Trading

Celsius - Secure
Crypto Wallet
GET
Earn & Borrow Cryptocurrency

BlueWallet - Bitcoin wallet
GET
Bitcoin & Lightning

BEST
CRYPTO
EXCHANGE

Feb 03

Necessary to have
but
how do you establish trust?

THE DOJ STRATEGY

- start with the attacker's public key(s) - necessary for payment

- identify transactions with those key(s) in the blockchain (including victim's payment) - publicly accessible information

- using the key(s), track how the attacker was moving funds around and identify the <u>on-ramps</u> and <u>off-ramps</u> they used e.g., coin exchanges, wallets, etc.

- work with software vendors or exploit identified vulnerabilities in the tools, sites, etc.

WHICH LEADS TO THE DEBATE

- do cryptocurrency users have a false sense of anonymity and/or security?

- is the connection between cryptocurrency and criminal activity perceived by many not that strong?

- can the on-ramps and off-ramps be held accountable? are software standards required?

- is this the beginning of government oversight, regulation and possible enforcement? (how did you check the virtual currency box on your 2020 federal taxes?)

- what would Satoshi and the cypherpunks think?
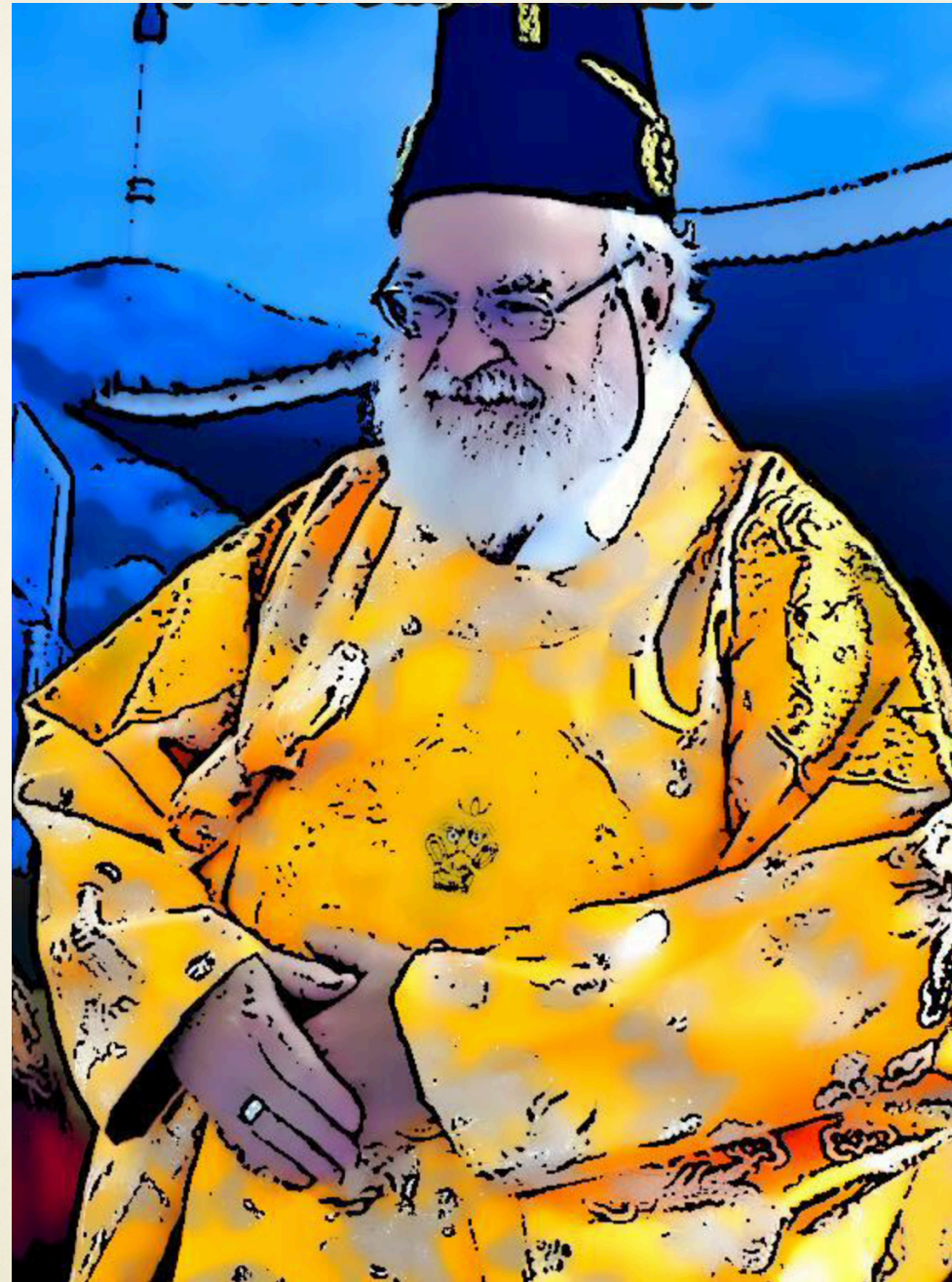
What would you pay for this NFT art?

Questions? Comments?
bebo.white@gmail.com