Are Cryptocurrencies Useful?

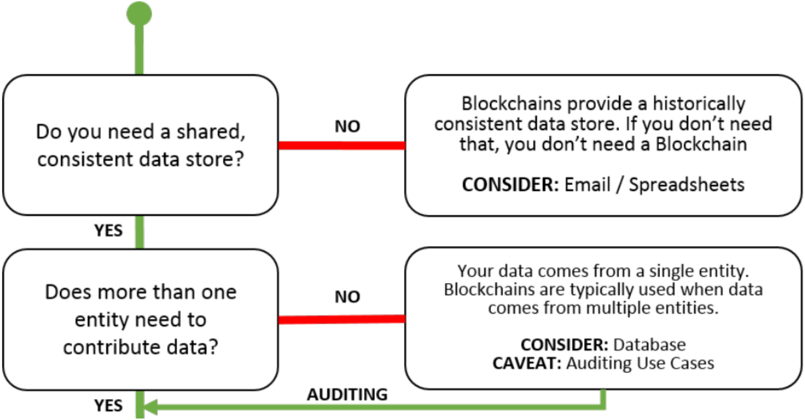
Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Associate Professor
Department of Electrical Engineering
Indian Institute of Technology Bombay

February 5, 2024

Do you need a blockchain?

US DHS Blockchain Flowchart (1/3)



Do you need a shared, consistent data store?

Blockchains provide a historically consistent data store. If you don't need that, you don't need a Blockchain

CONSIDER: Email / Spreadsheets

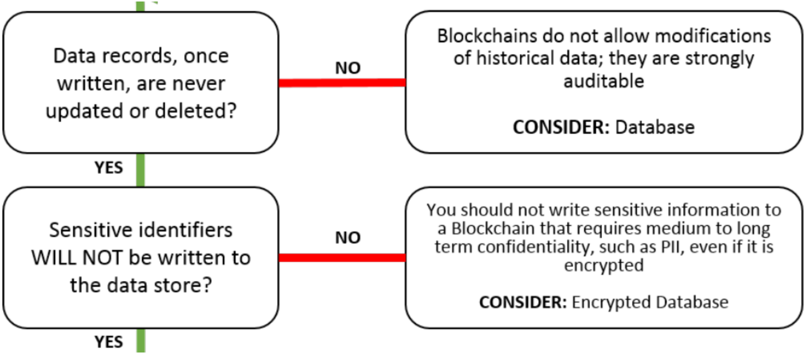
Does more than one entity need to contribute data?

Your data comes from a single entity. Blockchains are typically used when data comes from multiple entities.

CONSIDER: Database
CAVEAT: Auditing Use Cases

Source: NIST Blockchain Technology Overview
`https://doi.org/10.6028/NIST.IR.8202`

US DHS Blockchain Flowchart (2/3)



Data records, once written, are never updated or deleted?

NO

Blockchains do not allow modifications of historical data; they are strongly auditable

CONSIDER: Database

YES

Sensitive identifiers WILL NOT be written to the data store?

NO

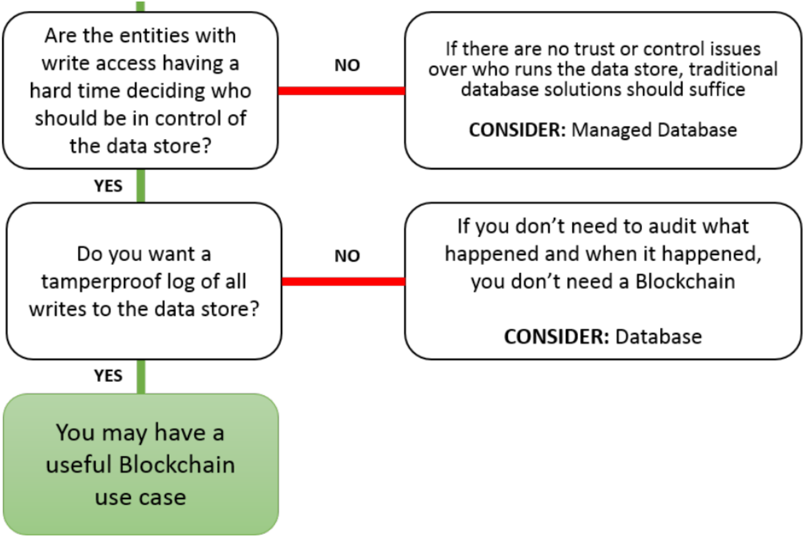
You should not write sensitive information to a Blockchain that requires medium to long term confidentiality, such as PII, even if it is encrypted

CONSIDER: Encrypted Database

YES

Source: NIST Blockchain Technology Overview
`https://doi.org/10.6028/NIST.IR.8202`

US DHS Blockchain Flowchart (2/3)



Are the entities with write access having a hard time deciding who should be in control of the data store?

NO

If there are no trust or control issues over who runs the data store, traditional database solutions should suffice

CONSIDER: Managed Database

YES

Do you want a tamperproof log of all writes to the data store?

NO

If you don't need to audit what happened and when it happened, you don't need a Blockchain

CONSIDER: Database

YES

You may have a useful Blockchain use case

Source: NIST Blockchain Technology Overview
`https://doi.org/10.6028/NIST.IR.8202`

Other Barriers for General Usage

- Users have to handle private keys
  - Loss of private keys cannot be reversed
  - Reversing key loss using secret sharing and social recovery possible, but not widespread as of now
- Privacy
  - Transaction amounts are public
  - Identities are pseudonymous and can be linked to real-world entities
- Scaling
  - Every blockchain node has to store a copy of all the transactions
- Every transaction on a cryptocurrency blockchain has a fee
- Permissioned blockchains (without a currency) have only reputational costs for history rewrites
- The oracle problem

Nefarious Uses of Cryptocurrencies

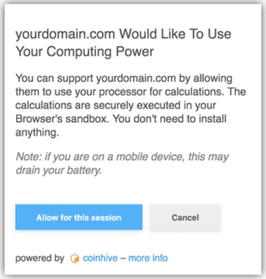
Donations

ادعم
المقاومة
ادعم المقاومة

- In Feb 2019, Hamas solicited bitcoin donations via social media
- By late March 2019, $5000 worth of bitcoin was received
- Traceability of public blockchains discourages such donations

Cryptojacking

- Hackers use a target's browser to mine Monero
- Coinhive is a cryptocurrency mining service written in JavaScript
  - Hacker embeds the code on website
  - When a user visits the website, her computer starts mining
  - Coinhive gets 30% and hacker gets 70%
- Some websites ask users to allow mining instead of showing ads

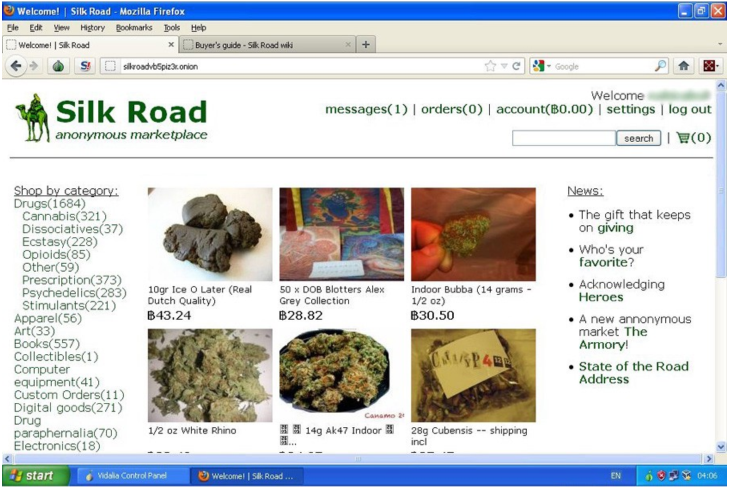


yourdomain.com Would Like To Use Your Computing Power

You can support yourdomain.com by allowing them to use your processor for calculations. The calculations are securely executed in your Browser's sandbox. You don't need to install anything.

Note: if you are on a mobile device, this may drain your battery.

Silk Road


Welcome! | Silk Road - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Welcome! | Silk Road
Buyer's guide - Silk Road wiki
silkroadvb5piz3r.onion
Google
start
Vidalia Control Panel
Welcome! | Silk Road ...
EN
04:06

Silk Road
anonymous marketplace

Welcome [redacted]
messages(1) | orders(0) | account(฿0.00) | settings | log out
search | 🛒(0)

Shop by category:
Drugs(1684)
- Cannabis(321)
- Dissociatives(37)
- Ecstasy(228)
- Opioids(85)
- Other(59)
- Prescription(373)
- Psychedelics(283)
- Stimulants(221)

Apparel(56)
Art(33)
Books(557)
Collectibles(1)
Computer equipment(41)
Custom Orders(11)
Digital goods(271)
Drug paraphernalia(70)
Electronics(18)

10gr Ice O Later (Real Dutch Quality)
฿43.24

50 x DOB Blotters Alex Grey Collection
฿28.82

Indoor Bubba (14 grams - 1/2 oz)
฿30.50

1/2 oz White Rhino

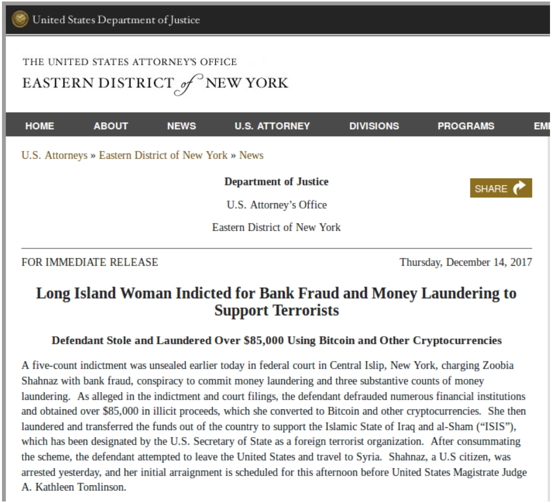
▩ ▩ 14g Ak47 Indoor ▩ ▩...

28g Cubensis -- shipping incl

News:
- The gift that keeps on giving
- Who's your favorite?
- Acknowledging Heroes
- A new annonymous market The Armory!
- State of the Road Address

- A darknet market for selling illegal drugs
  - Launched in Feb 2011
  - All transactions done using Bitcoin
  - Shut down in Oct 2013 after arrest of founder Ross Ulbricht

Money Laundering



United States Department of Justice
THE UNITED STATES ATTORNEY'S OFFICE
EASTERN DISTRICT of NEW YORK
HOME
ABOUT
NEWS
U.S. ATTORNEY
DIVISIONS
PROGRAMS
EM
U.S. Attorneys » Eastern District of New York » News
SHARE

Department of Justice

U.S. Attorney's Office

Eastern District of New York

FOR IMMEDIATE RELEASE — Thursday, December 14, 2017

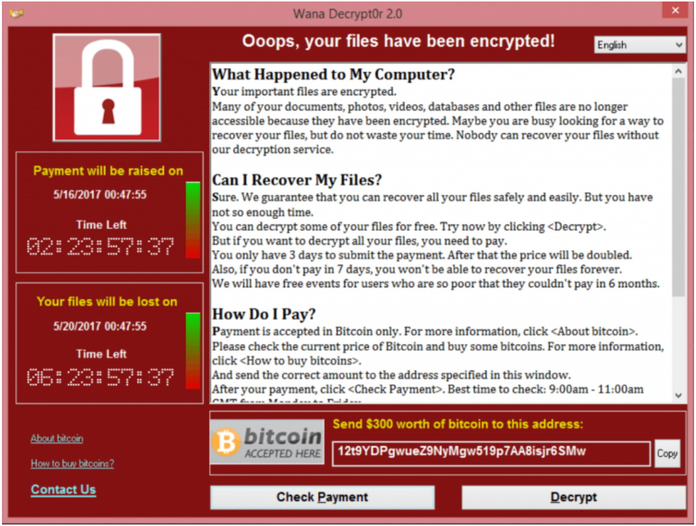
Long Island Woman Indicted for Bank Fraud and Money Laundering to Support Terrorists

Defendant Stole and Laundered Over $85,000 Using Bitcoin and Other Cryptocurrencies

A five-count indictment was unsealed earlier today in federal court in Central Islip, New York, charging Zoobia Shahnaz with bank fraud, conspiracy to commit money laundering and three substantive counts of money laundering. As alleged in the indictment and court filings, the defendant defrauded numerous financial institutions and obtained over $85,000 in illicit proceeds, which she converted to Bitcoin and other cryptocurrencies. She then laundered and transferred the funds out of the country to support the Islamic State of Iraq and al-Sham ("ISIS"), which has been designated by the U.S. Secretary of State as a foreign terrorist organization. After consummating the scheme, the defendant attempted to leave the United States and travel to Syria. Shahnaz, a U.S citizen, was arrested yesterday, and her initial arraignment is scheduled for this afternoon before United States Magistrate Judge A. Kathleen Tomlinson.

Compromised credit cards used to buy cryptocurrency which was converted to fiat and wire transferred to ISIS

Ransomware



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

- Computer worm that encrypts data on a victim’s computer and demands a ransom in Bitcoin

More Crypto Scams

Insolvent Exchanges

- Miners or validators own all newly created cryptocurrencies
- Exchanges buy from miners and resell to users
- General users don't want to handle private keys
- Exchanges also provide custodial wallets and offer trading between different cryptocurrencies
- An exchange is insolvent if its liabilities to its users exceeds its cryptocurrency reserves
- Insolvency may be due to hacks or exchange operator fraud
- Examples
  - Mt Gox lost 850k BTC in 2014 `https://en.wikipedia.org/wiki/Mt._Gox`
  - FTX 2022 `https://en.wikipedia.org/wiki/FTX`

Forking the Blockchain

- All account balances are public on cryptocurrencies without privacy features (Bitcoin, Ethereum)
- Several new blockchains have been launched which fork existing blockchains
- Users of the original cryptocurrency will have the same amount of new coins
- In some cases, the fork developers abandon development

Pump-and-Dump Schemes

- Small groups of investors coordinate to increase the price of a coin (the pump)
  - Buying up large amounts of the coin on exchanges
  - Social media posts
- Other users also buy the coin increasing its price further
- The original investors sell all their coins at the same time (the dump)
- The price of the coin crashes leaving retail users with losses

ICO Scams

- ICO = Initial Coin Offering
- Ethereum made it very easy to launch a new cryptocurrency
    - ERC-20 Token Standard
- Developers raise funds for a new project using a new token
- They publish a roadmap for the project
- Users buy the token with the hope that its price will rise
- Developers abandon project or slowly bleed the treasury

Silver Linings

Inflation Hedge

- Some national currencies suffer from hyper-inflation
  - In Argentina, YoY inflation was more than 100% in March 2023
  - Venezuela's currency plunged 100,000% fom 2014 to 2022
  - Source: Techopedia article
- Citizens in these countries use cryptocurrencies to preserve wealth
- Stablecoins are used even for everyday transactions

Other Promising Applications

- Decentralized Finance (DeFi)
    - High volumes but limited to crypto assets
    - Oracle problem a barrier to trading real-world assets (RWAs)
- Non-fungible Tokens
    - Went mainstream in 2020-21 but have since fizzled
    - Niche use cases like supporting creators still feasible
- Farcaster
    - A Twitter-like sufficiently decentralized social media protocol
    - Stores IDs on-chain and posts offchain
    - Not tested at planet-scale
- Games
    - Ownership of in-game items possible
    - No mainstream success yet
- In summary, promising but not yet proven

References

- NIST Blockchain Technology Overview https://doi.org/10.6028/NIST.IR.8202
- Cryptojacking https://www.interpol.int/en/Crimes/Cybercrime/Cryptojacking
- Article on Coinhive https://krebsonsecurity.com/2018/03/who-and-what-is-coinhive/
- AuthedMiner https://blog.sucuri.net/2017/10/cryptominers-on-hacked-sites-part-2.html
- Silk Road https://en.wikipedia.org/wiki/Silk_Road_(marketplace)
- Money laundering https://home.treasury.gov/news/press-releases/sm687
- WannaCry https://en.wikipedia.org/wiki/WannaCry_ransomware_attack