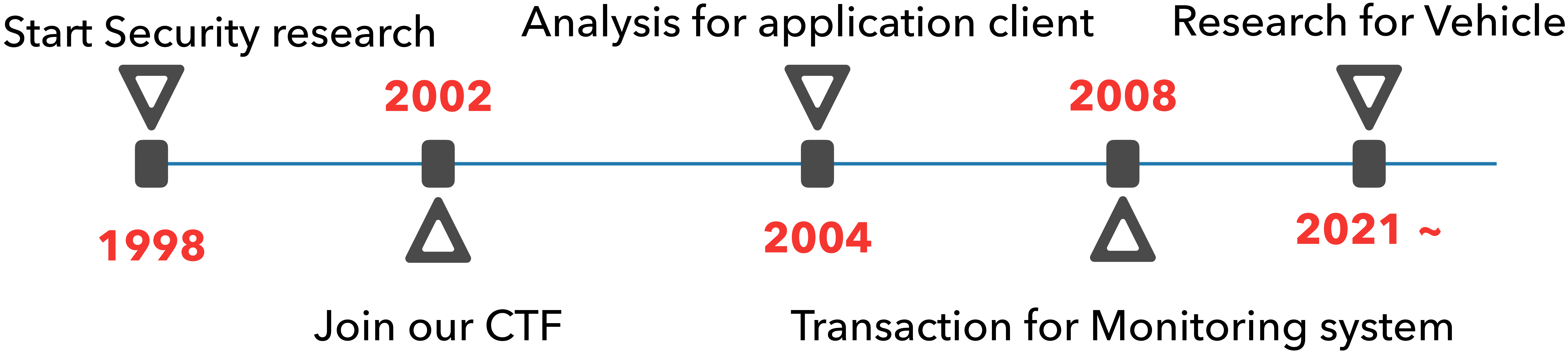
Cryptocurrency exchange events and accidents

Report and responding to exchange incidents

I'm crattack

crattack@gmail.com



1998 Start Security research

2002 Join our CTF

2004 Analysis for application client

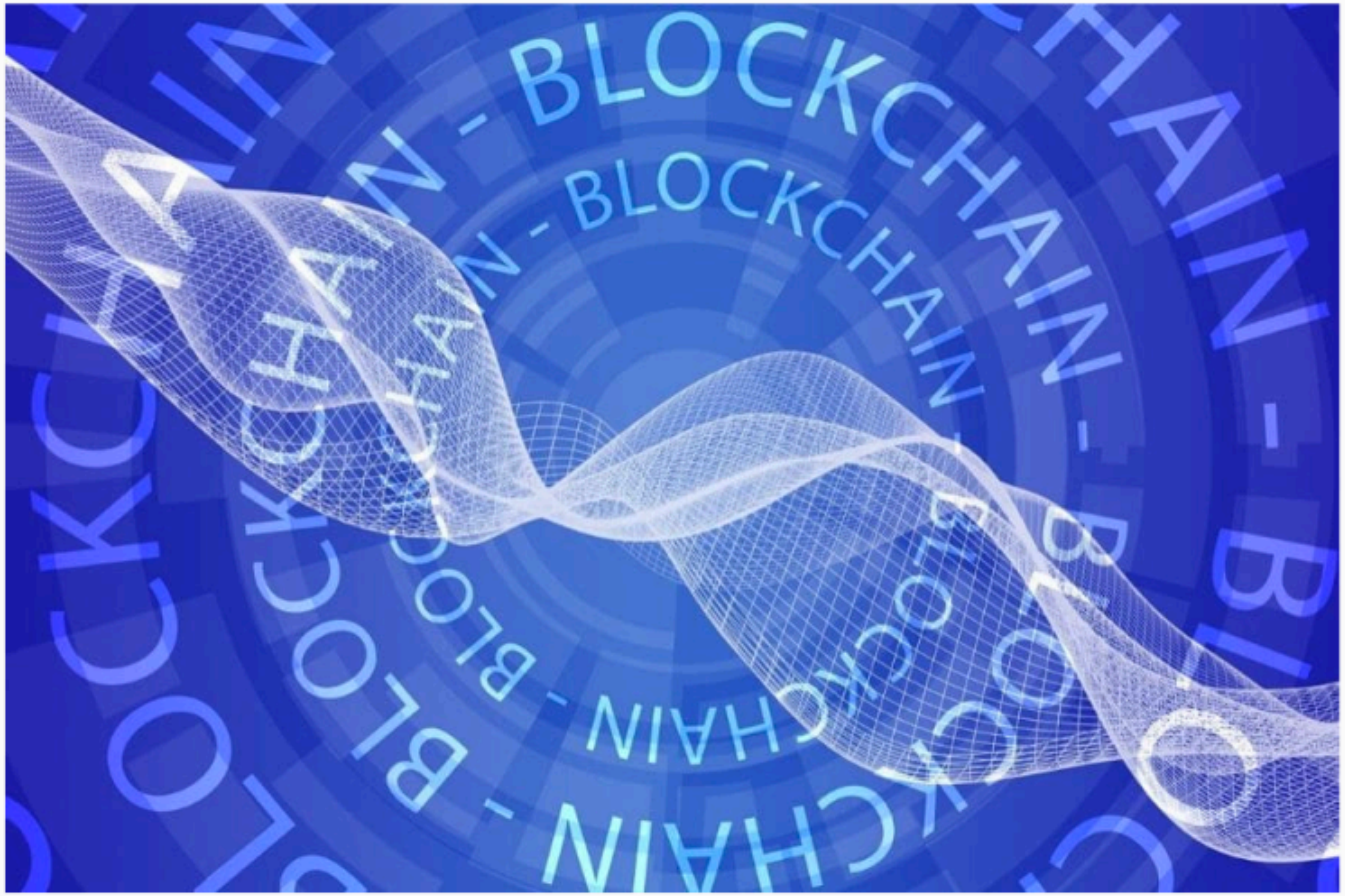
2008 Transaction for Monitoring system

2021 ~ Research for Vehicle

Table of Contents

- Criminal Cases on the cryptocurrency exchange
- Investigation of fraud techniques on the cryptocurrency exchange
- Transaction Analysis Methods
- How to respond to fraud on virtual exchanges

crattack@gmail.com

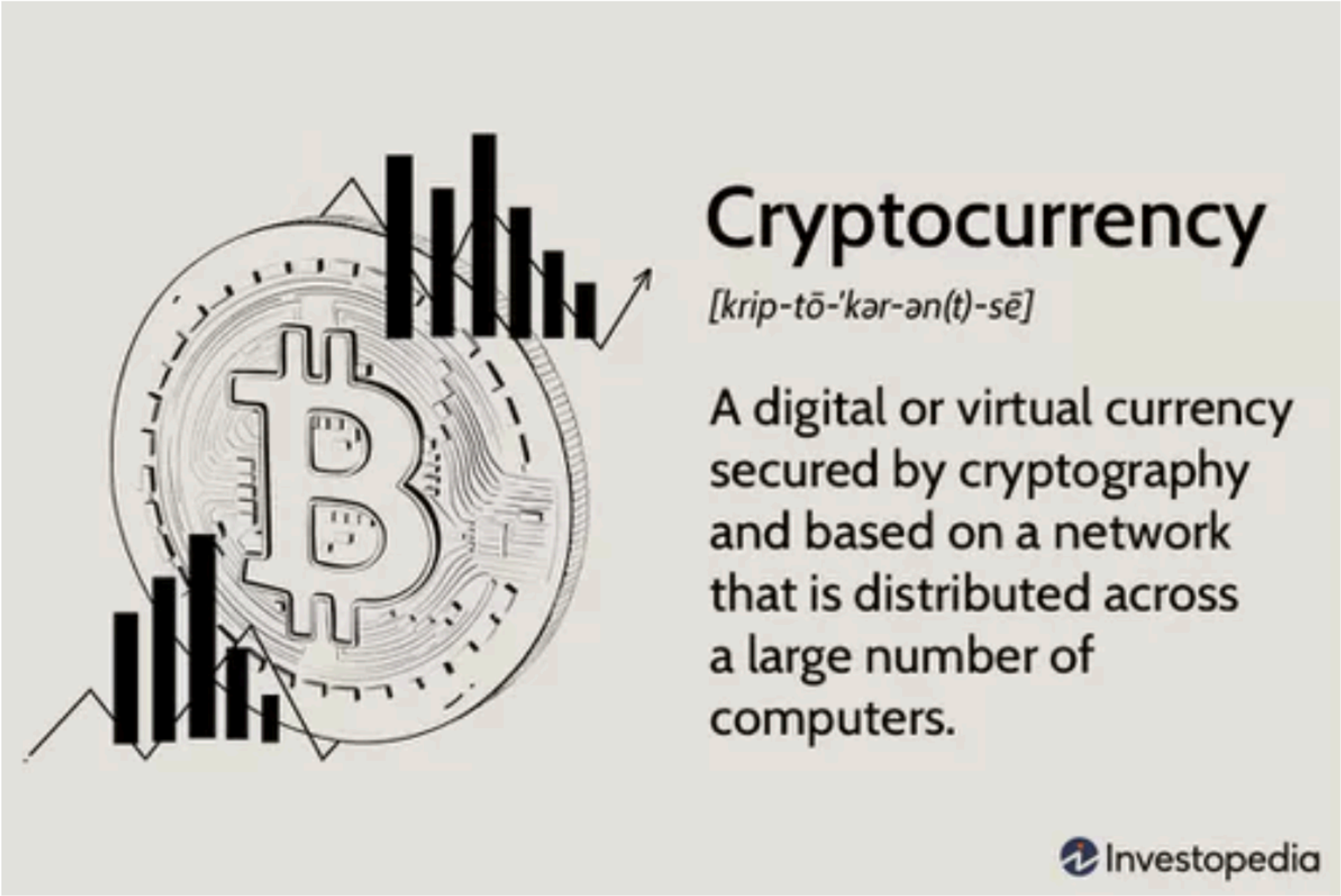


https://www.dailycoinews.com/dailycoinews/article/read.do?articleNo=6607&lang=kr

Cryptocurrency Elements!?!

- **Cryptocurrency = Crypto + Currency**
- **Distributed Ledger**
- Blockchain
- Node
- Coin
- Wallet
- Sevice Model

- Security Elements



Cryptocurrency

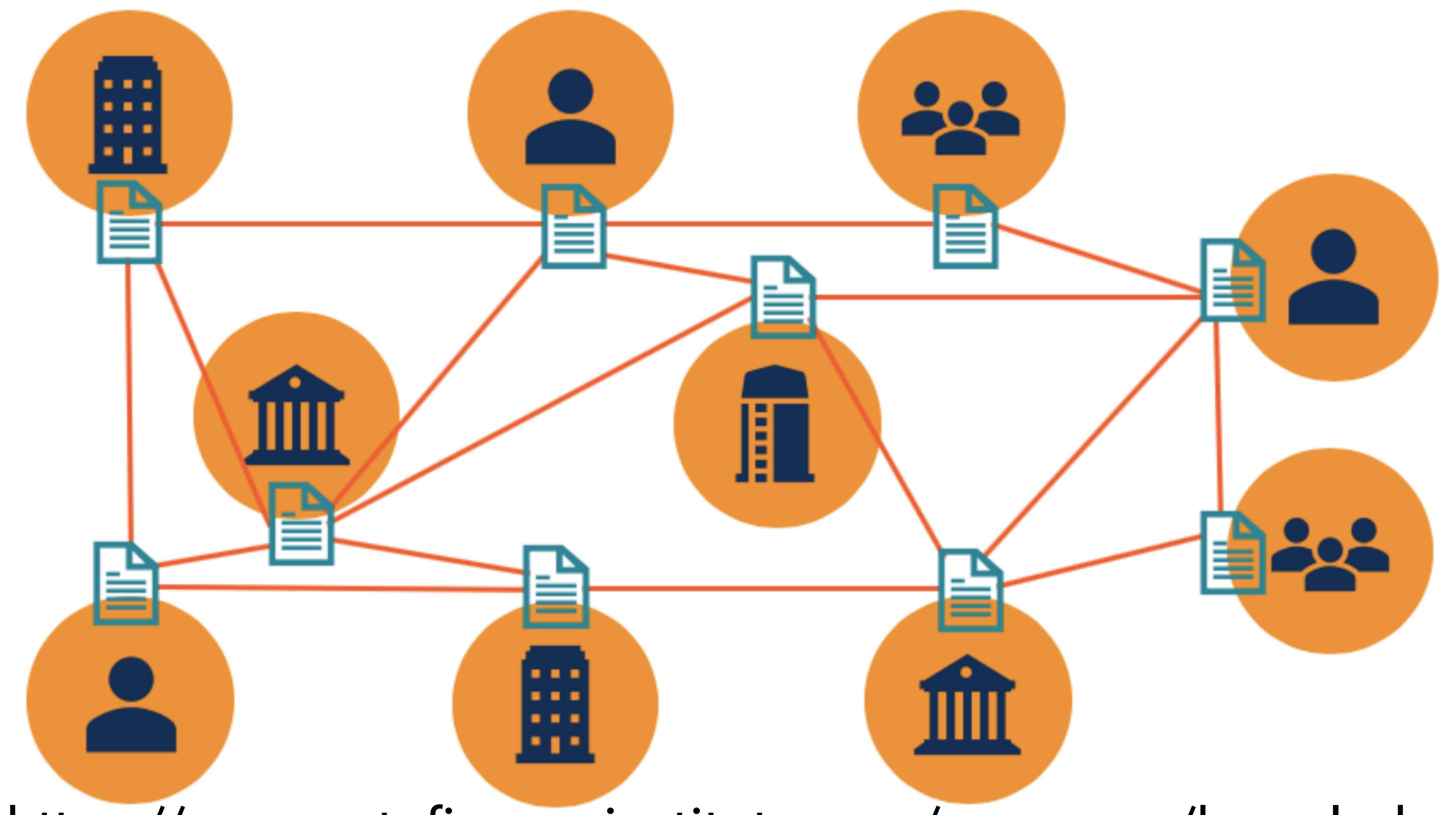
[krip-tō-'kər-ən(t)-sē]

A digital or virtual currency secured by cryptography and based on a network that is distributed across a large number of computers.

Investopedia

Investopedia / Tara Anand

Distributed Ledger Technology



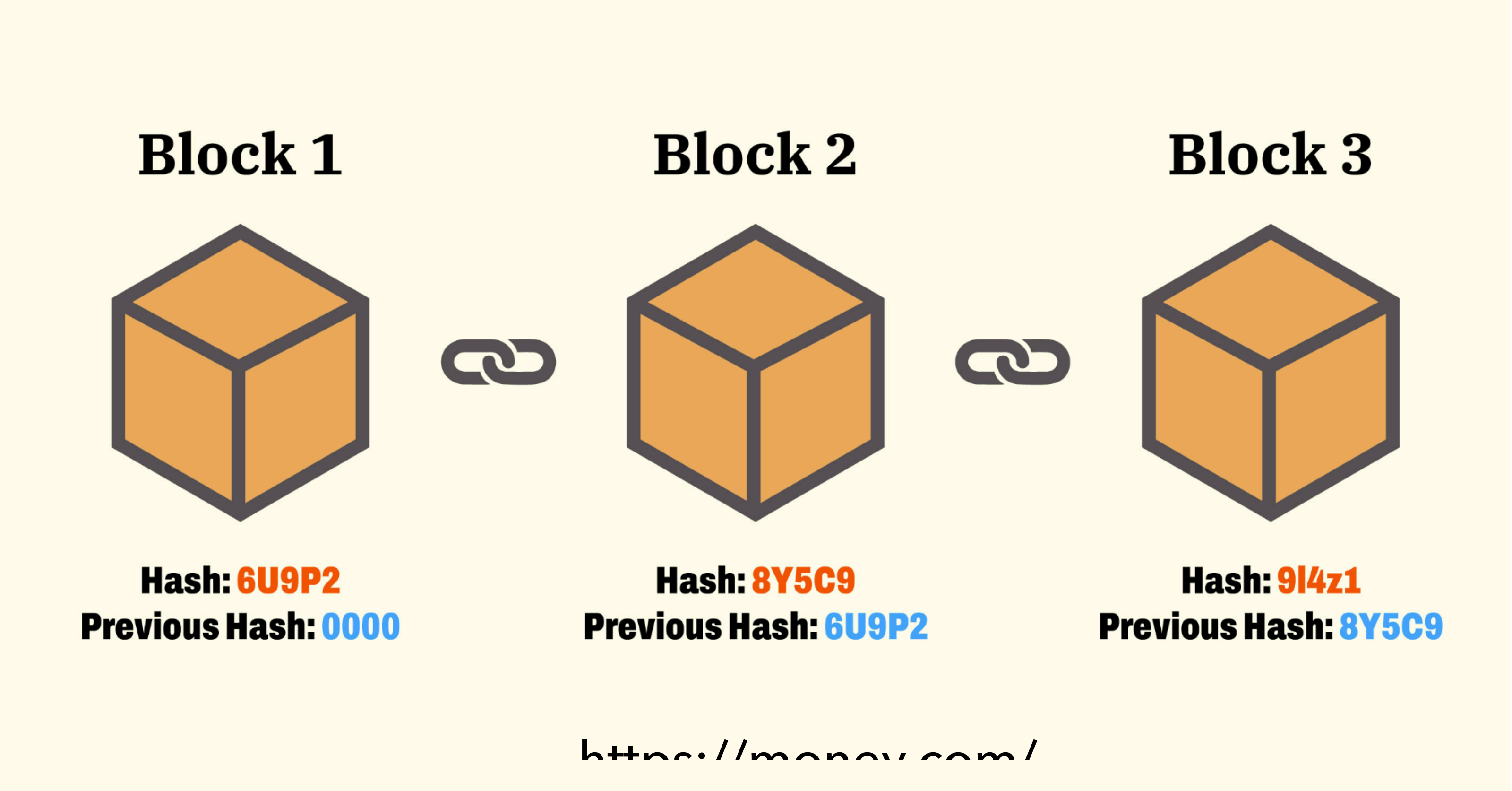
https://corporatefinanceinstitute.com/resources/knowledge/other/

https://money.com/what-is-blockchain/

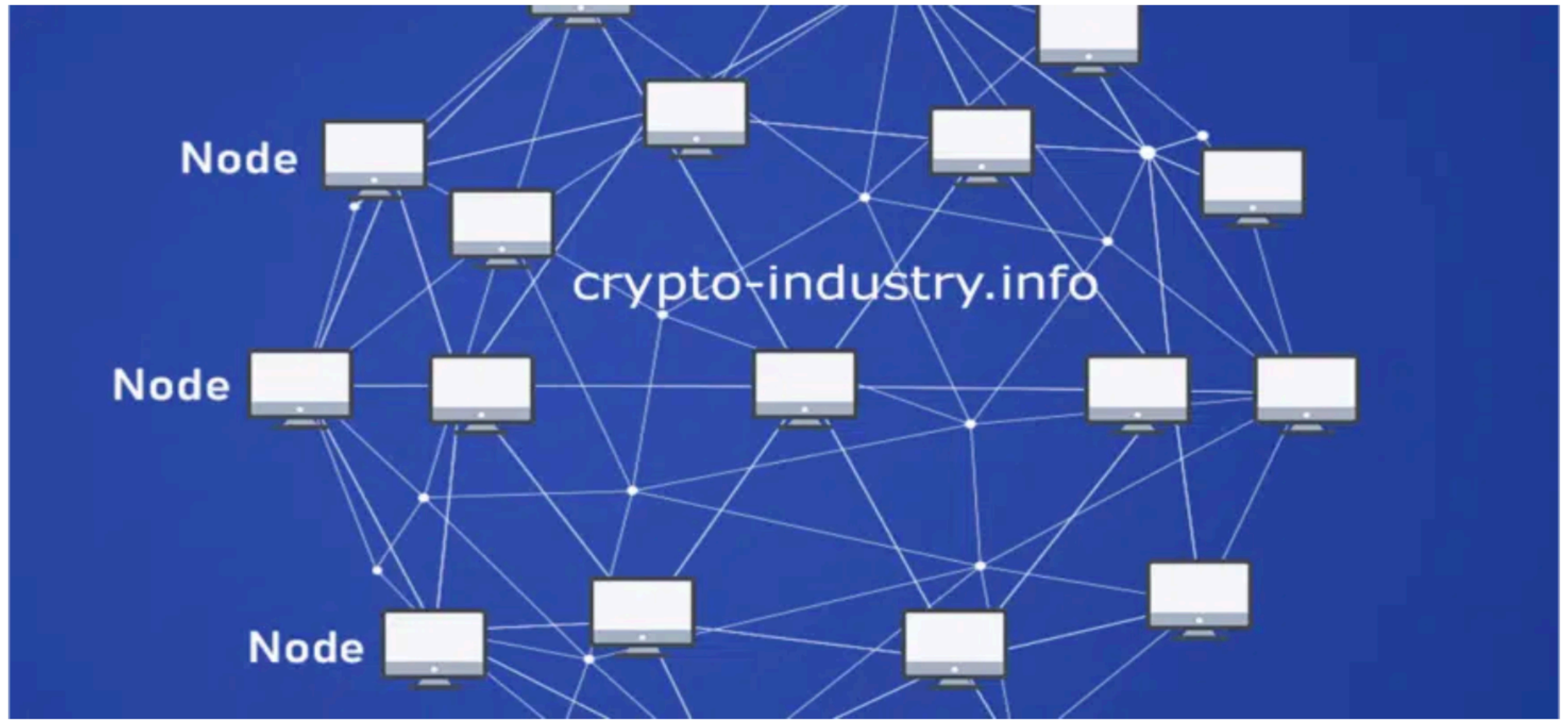
Cryptocurrency Elements!?!

- Cryptocurrency = Crypto + Currency
- Distributed Ledger
- **Blockchain**
- **Node**
- Coin
- Wallet
- Sevice Model

- Security Elements



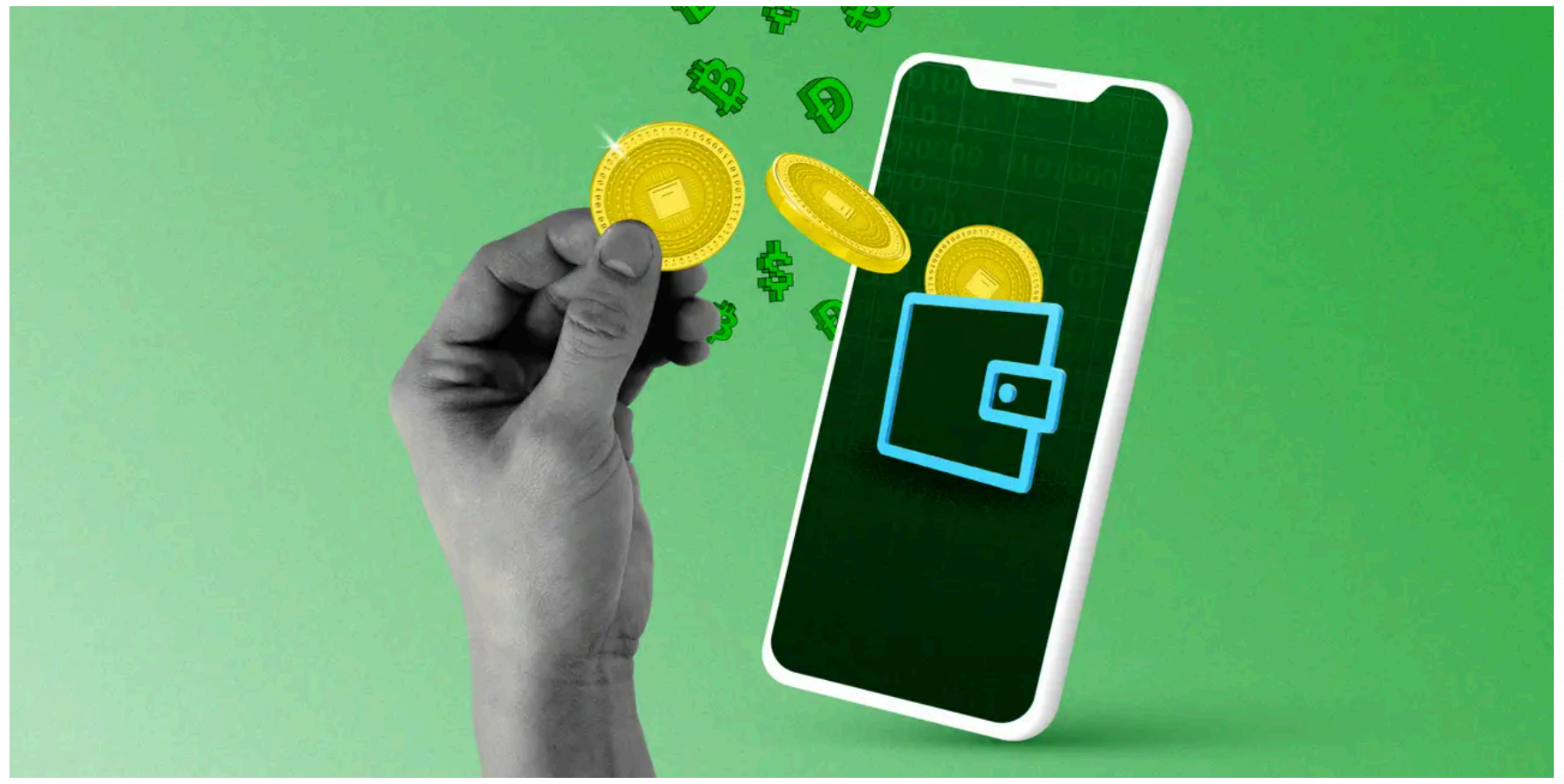
https://money.com/



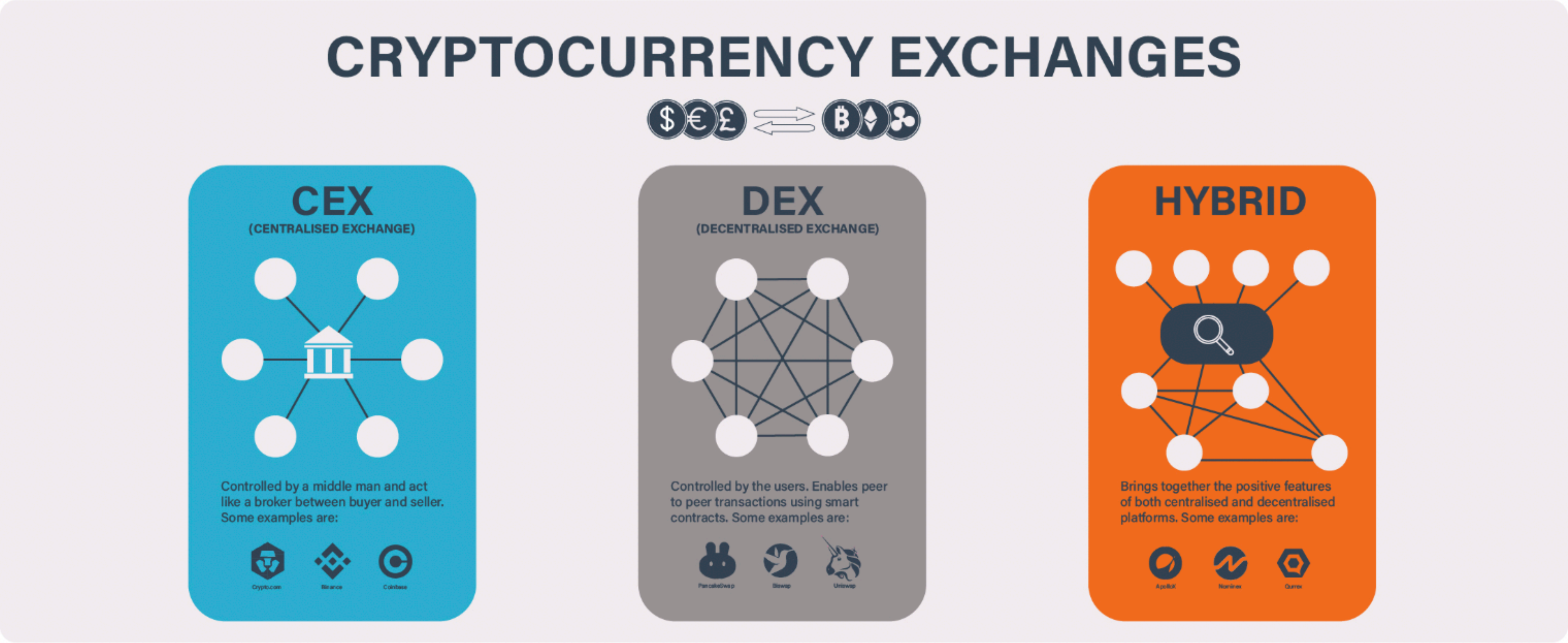
Cryptocurrency Elements!?!

- Cryptocurrency = Crypto + Currency
- Distributed Ledger
- Blockchain
- Node
- **Coin**
- **Wallet**
- **Sevice Model**

- Security Elements



Each type of crypto wallet has its own use case depending on the goals of the user, although they all accomplish the same things.
Alyssa Powell/Insider



CRYPTOCURRENCY EXCHANGES

CEX (CENTRALISED EXCHANGE)

Controlled by a middle man and act like a broker between buyer and seller. Some examples are:

DEX (DECENTRALISED EXCHANGE)

Controlled by the users. Enables peer to peer transactions using smart contracts. Some examples are:

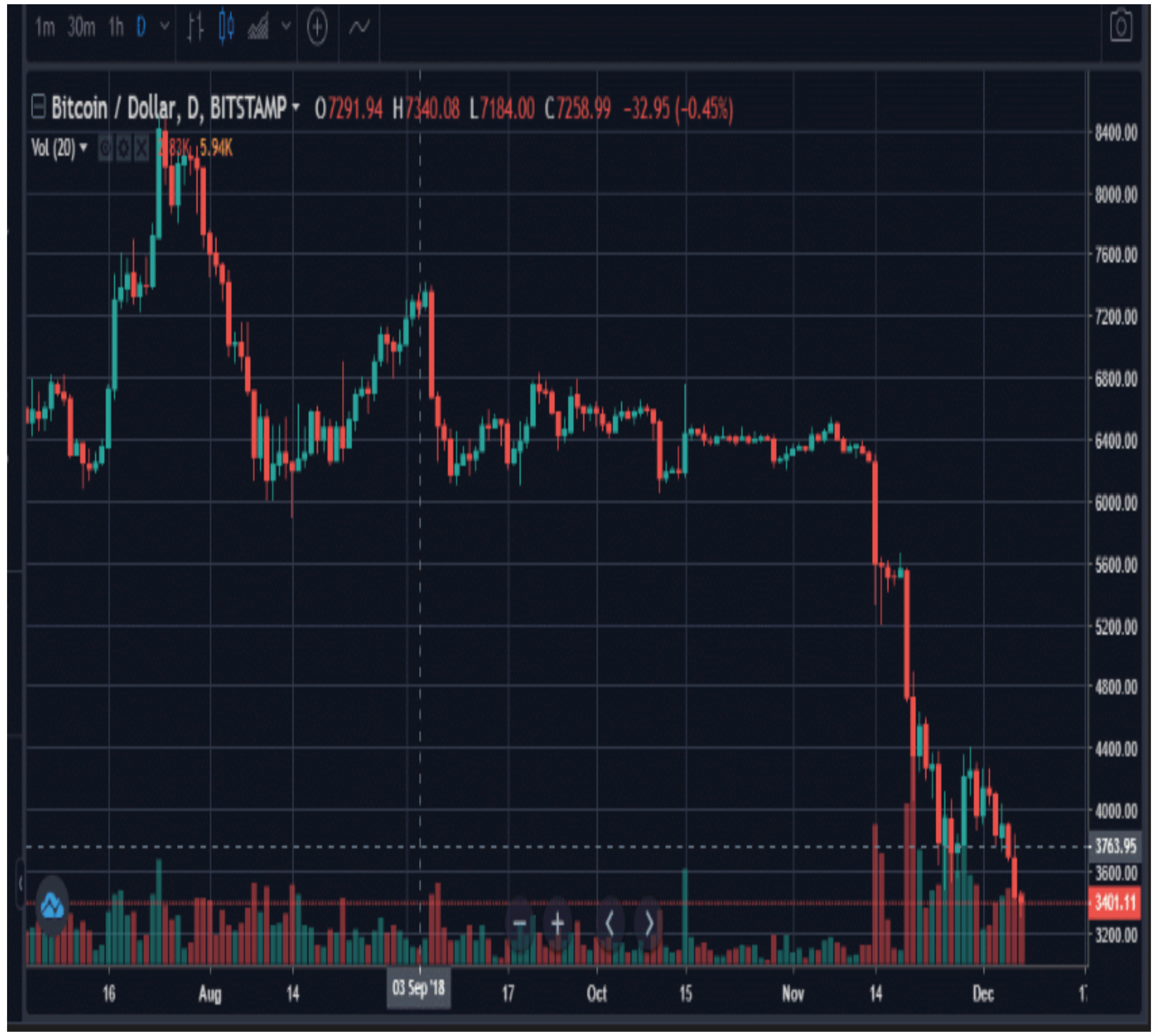
HYBRID

Brings together the positive features of both centralised and decentralised platforms. Some examples are:

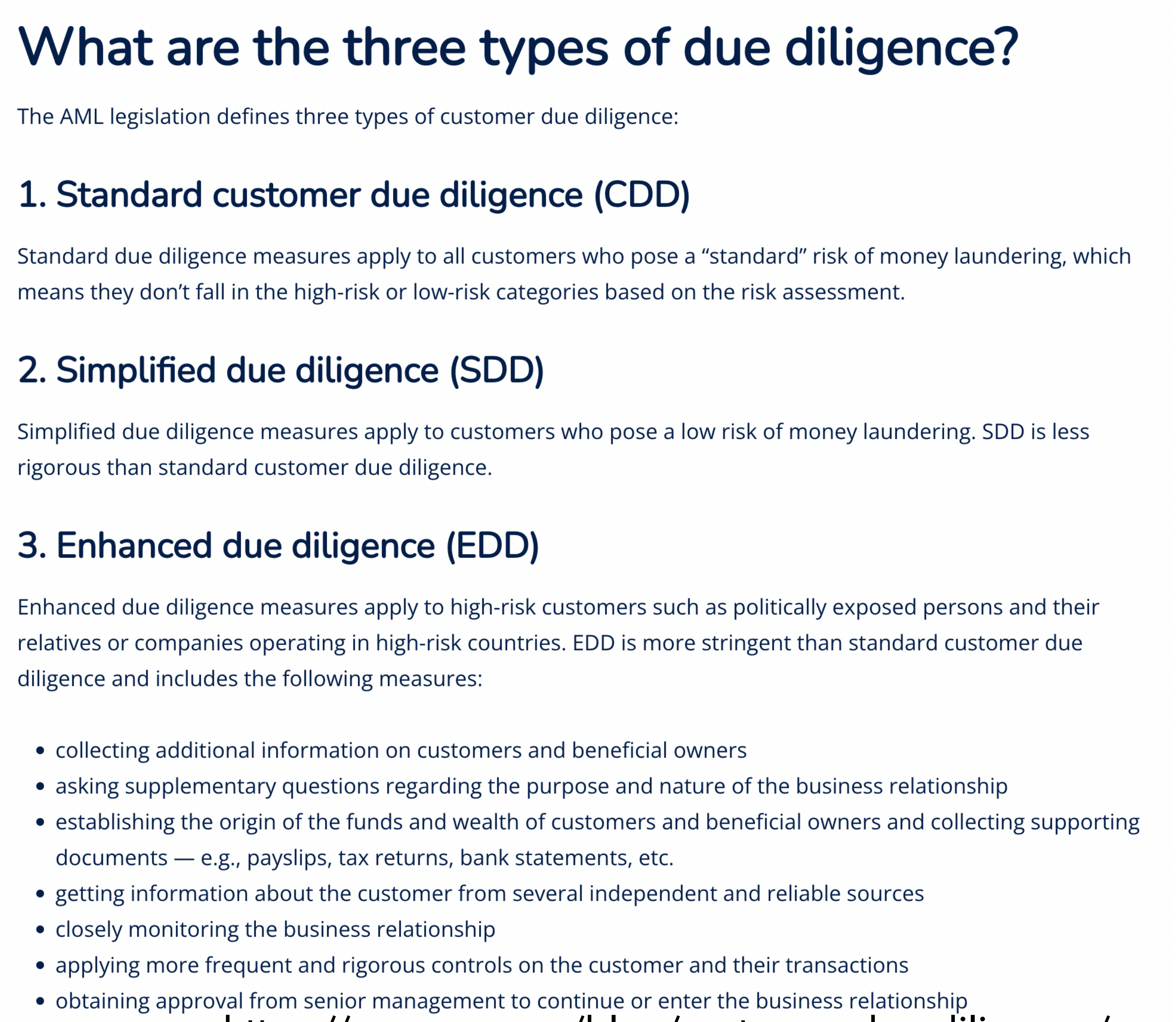
Cryptocurrency Infographic: Crypto Exchanges From A to Z!

Cryptocurrency Elements!?!

- Cryptocurrency = Crypto + Currency
- Distributed Ledger
- Blockchain
- Node
- Coin
- Wallet
- Sevice Model



- **Security Elements**



What are the three types of due diligence?

The AML legislation defines three types of customer due diligence:

1. Standard customer due diligence (CDD)

Standard due diligence measures apply to all customers who pose a "standard" risk of money laundering, which means they don't fall in the high-risk or low-risk categories based on the risk assessment.

2. Simplified due diligence (SDD)

Simplified due diligence measures apply to customers who pose a low risk of money laundering. SDD is less rigorous than standard customer due diligence.

3. Enhanced due diligence (EDD)

Enhanced due diligence measures apply to high-risk customers such as politically exposed persons and their relatives or companies operating in high-risk countries. EDD is more stringent than standard customer due diligence and includes the following measures:

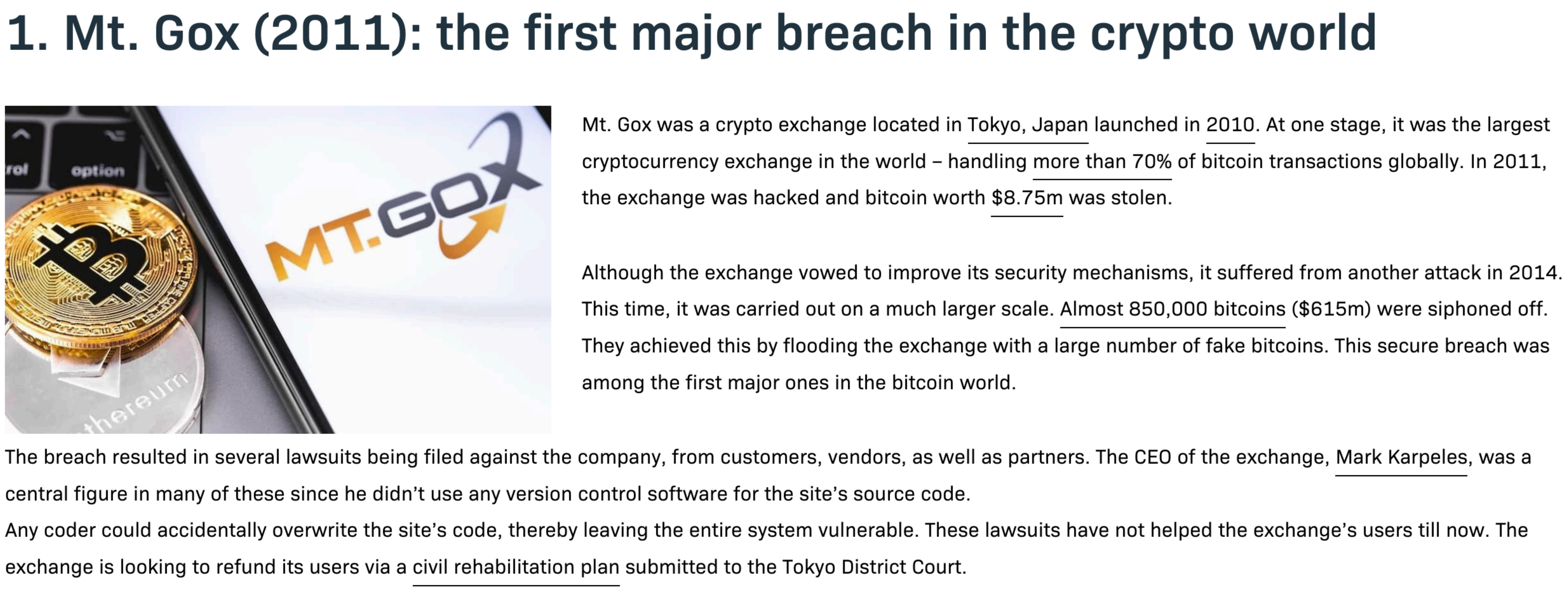
- collecting additional information on customers and beneficial owners
- asking supplementary questions regarding the purpose and nature of the business relationship
- establishing the origin of the funds and wealth of customers and beneficial owners and collecting supporting documents — e.g., payslips, tax returns, bank statements, etc.
- getting information about the customer from several independent and reliable sources
- closely monitoring the business relationship
- applying more frequent and rigorous controls on the customer and their transactions
- obtaining approval from senior management to continue or enter the business relationship

https://penneo.com/blog/customer-due-diligence/

Why is blockchain targeted by crime?

- Anonymous
- The source of the funds is not verified
- Global trading regardless of distance
- Net service (No Cybersecurity)

A typical case of crime



1. Mt. Gox (2011): the first major breach in the crypto world

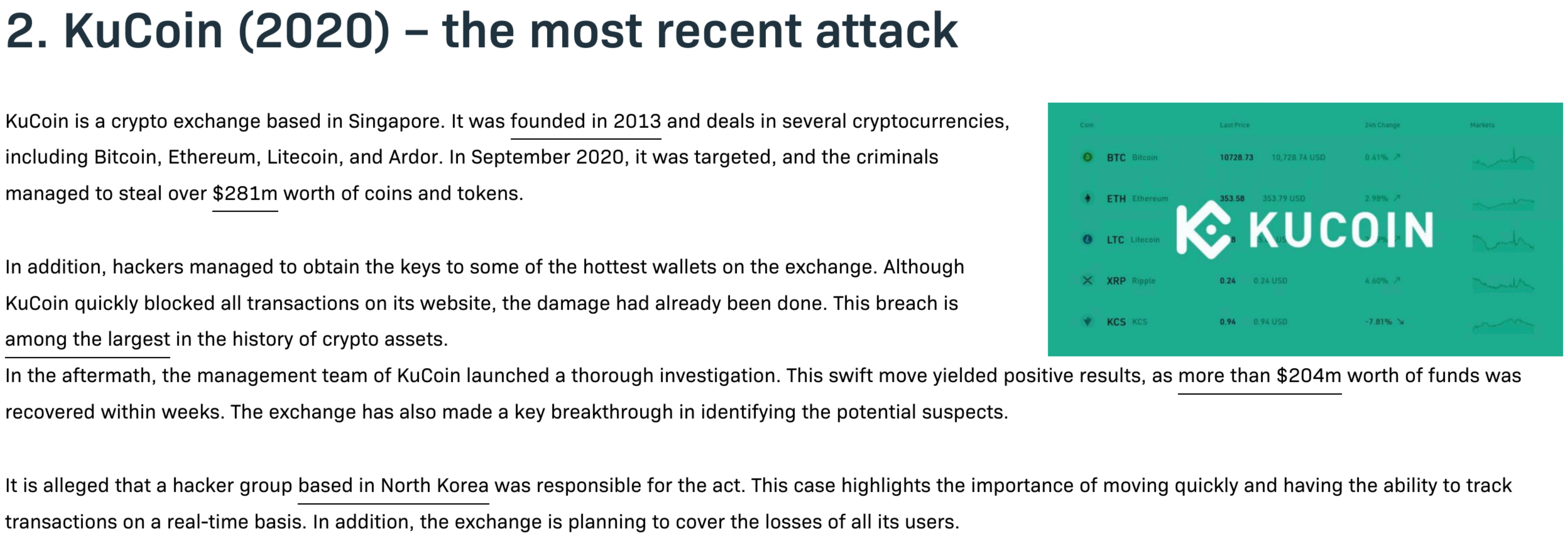
Mt. Gox was a crypto exchange located in Tokyo, Japan launched in 2010. At one stage, it was the largest cryptocurrency exchange in the world – handling more than 70% of bitcoin transactions globally. In 2011, the exchange was hacked and bitcoin worth $8.75m was stolen.

Although the exchange vowed to improve its security mechanisms, it suffered from another attack in 2014. This time, it was carried out on a much larger scale. Almost 850,000 bitcoins ($615m) were siphoned off. They achieved this by flooding the exchange with a large number of fake bitcoins. This secure breach was among the first major ones in the bitcoin world.

The breach resulted in several lawsuits being filed against the company, from customers, vendors, as well as partners. The CEO of the exchange, Mark Karpeles, was a central figure in many of these since he didn't use any version control software for the site's source code.
Any coder could accidentally overwrite the site's code, thereby leaving the entire system vulnerable. These lawsuits have not helped the exchange's users till now. The exchange is looking to refund its users via a civil rehabilitation plan submitted to the Tokyo District Court.

https://crystalblockchain.com/articles/the-10-biggest-crypto-exchange-hacks-in-history/

A typical case of crime



2. KuCoin (2020) – the most recent attack

KuCoin is a crypto exchange based in Singapore. It was founded in 2013 and deals in several cryptocurrencies, including Bitcoin, Ethereum, Litecoin, and Ardor. In September 2020, it was targeted, and the criminals managed to steal over $281m worth of coins and tokens.

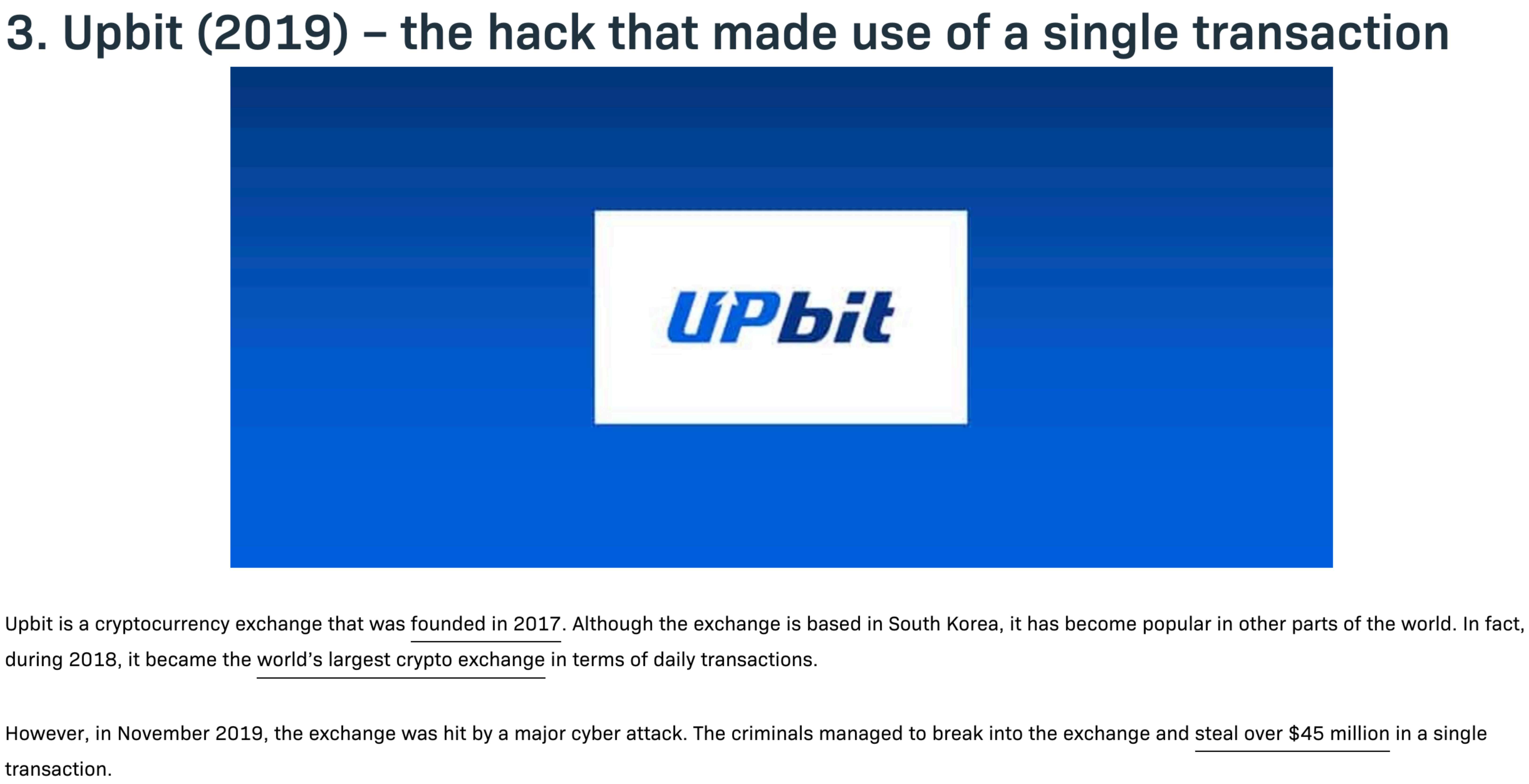
In addition, hackers managed to obtain the keys to some of the hottest wallets on the exchange. Although KuCoin quickly blocked all transactions on its website, the damage had already been done. This breach is among the largest in the history of crypto assets.

In the aftermath, the management team of KuCoin launched a thorough investigation. This swift move yielded positive results, as more than $204m worth of funds was recovered within weeks. The exchange has also made a key breakthrough in identifying the potential suspects.

It is alleged that a hacker group based in North Korea was responsible for the act. This case highlights the importance of moving quickly and having the ability to track transactions on a real-time basis. In addition, the exchange is planning to cover the losses of all its users.

https://crystalblockchain.com/articles/the-10-biggest-crypto-exchange-hacks-in-history/

A typical case of crime



3. Upbit (2019) – the hack that made use of a single transaction

Upbit is a cryptocurrency exchange that was founded in 2017. Although the exchange is based in South Korea, it has become popular in other parts of the world. In fact, during 2018, it became the world's largest crypto exchange in terms of daily transactions.

However, in November 2019, the exchange was hit by a major cyber attack. The criminals managed to break into the exchange and steal over $45 million in a single transaction.

https://crystalblockchain.com/articles/the-10-biggest-crypto-exchange-hacks-in-history/

A typical case of crime

4. BINANCE (2019) – the biggest name to be hit

Binance is one of the biggest names in the business. The exchange is headquartered in the Cayman Islands and is the world's largest cryptocurrency exchange (by volume). The exchange offers over 360 different cryptocurrencies and is active in more than 1200 markets.

https://crystalblockchain.com/articles/the-10-biggest-crypto-exchange-hacks-in-history/

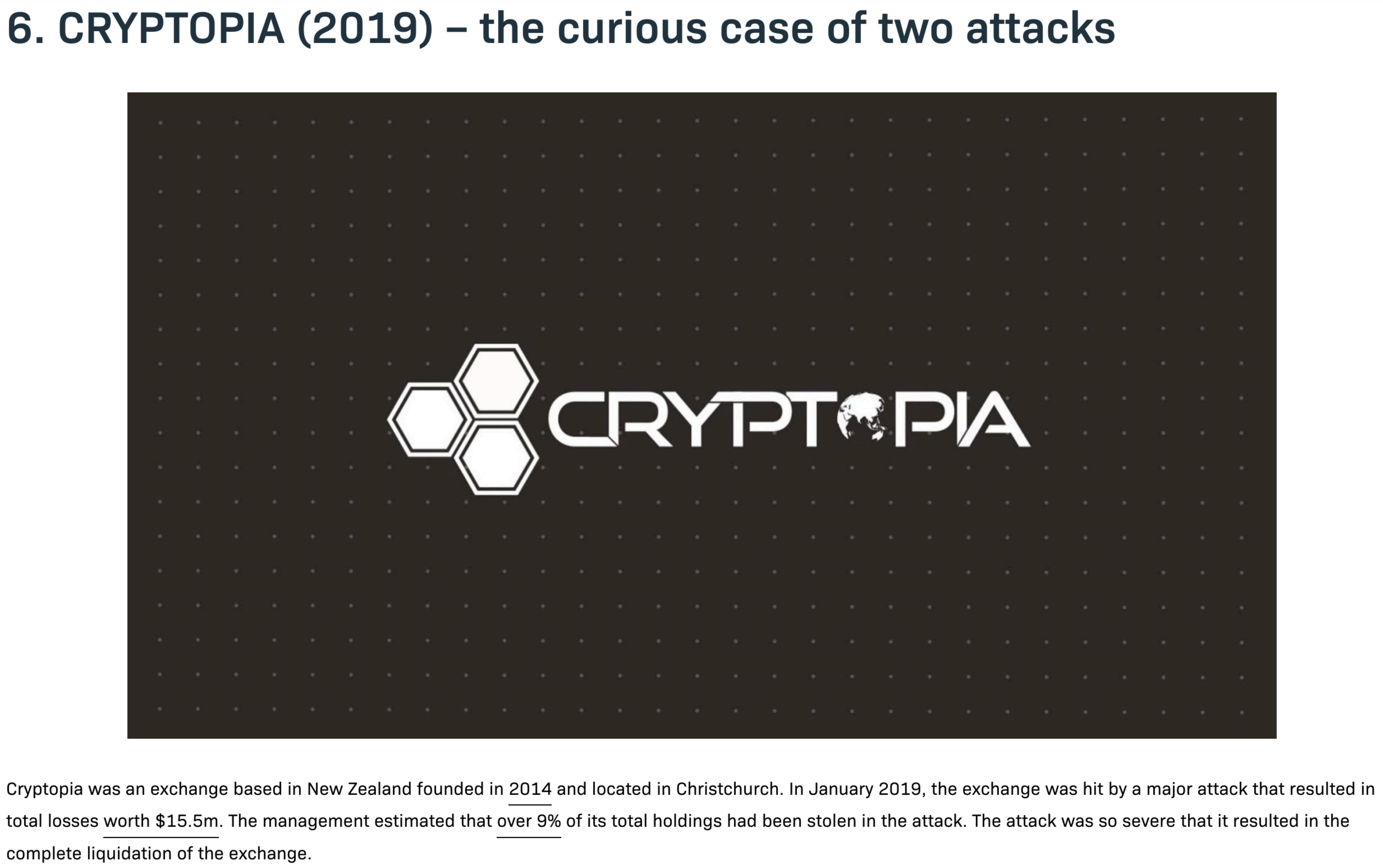
A typical case of crime

5. Bitfinex (2016) – the hack where losses were distributed

Bitfinex is a Hong Kong-based crypto exchange that was founded in the year 2012. It is owned by iFinex Inc., a company that has also developed a stablecoin known as Tether. In 2016, the crypto exchange was attacked by hackers, who managed to steal coins worth over $60 million.

https://crystalblockchain.com/articles/the-10-biggest-crypto-exchange-hacks-in-history/

A typical case of crime

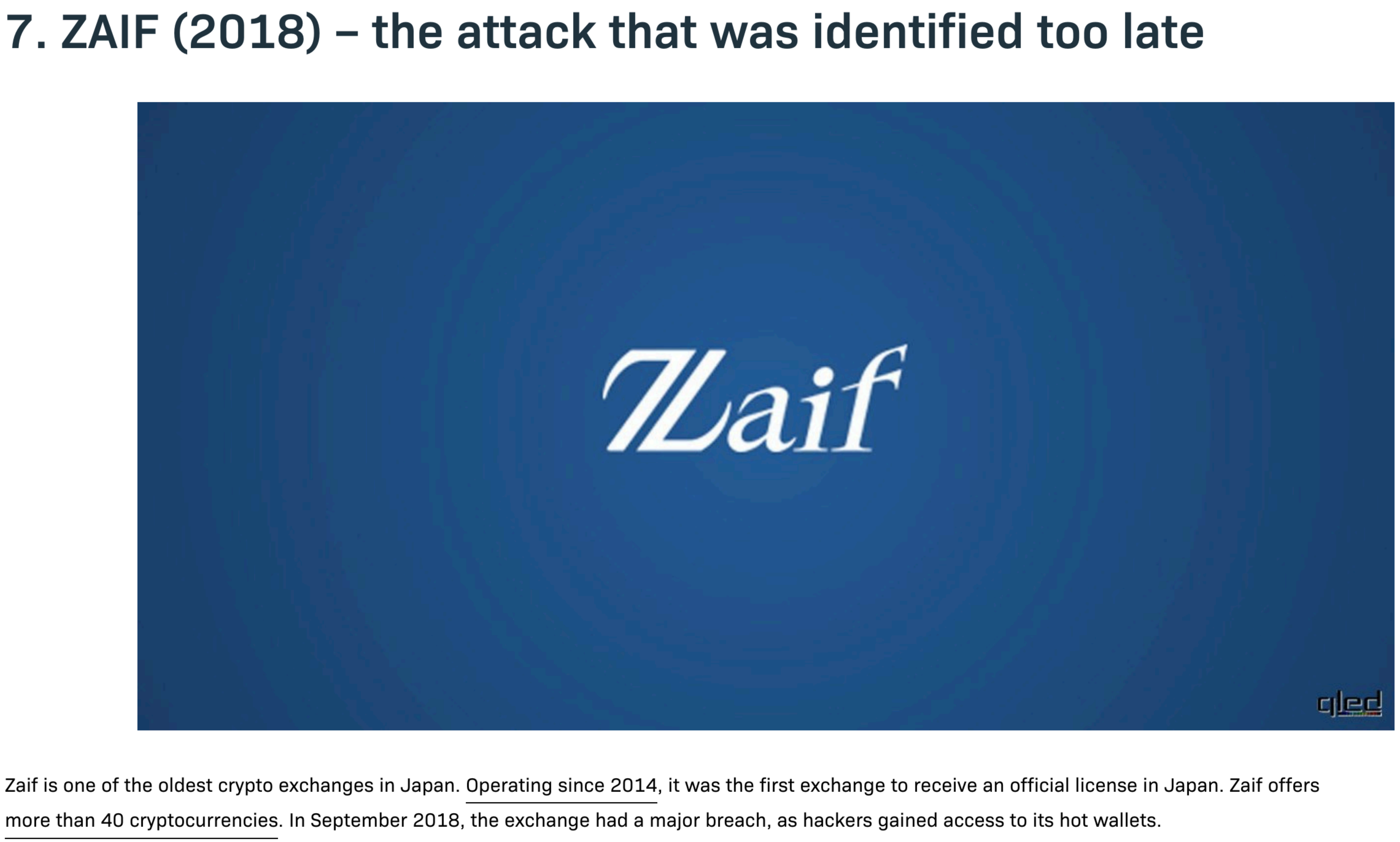


6. CRYPTOPIA (2019) – the curious case of two attacks

Cryptopia was an exchange based in New Zealand founded in 2014 and located in Christchurch. In January 2019, the exchange was hit by a major attack that resulted in total losses worth $15.5m. The management estimated that over 9% of its total holdings had been stolen in the attack. The attack was so severe that it resulted in the complete liquidation of the exchange.

https://crystalblockchain.com/articles/the-10-biggest-crypto-exchange-hacks-in-history/

A typical case of crime

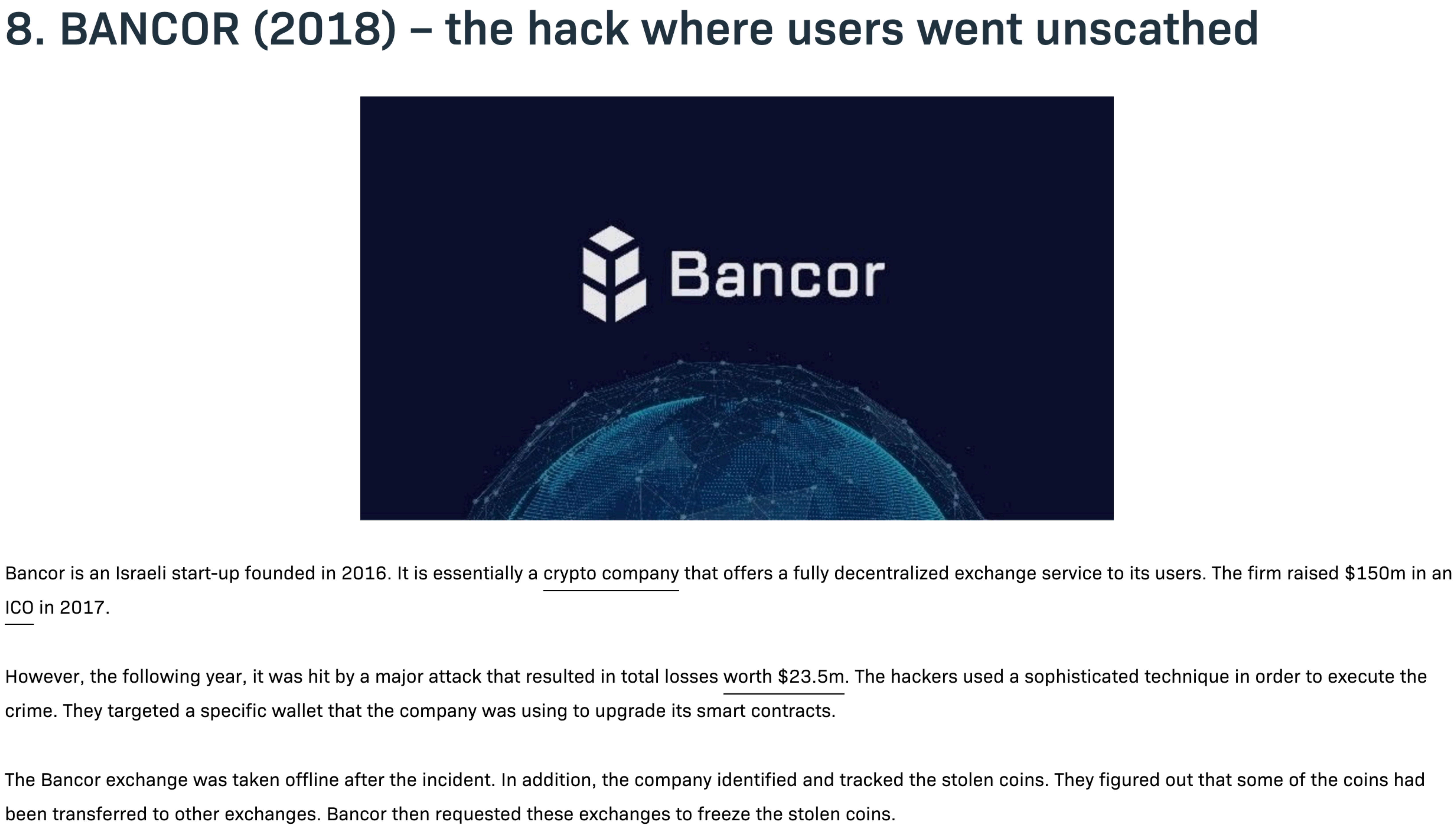


7. ZAIF (2018) – the attack that was identified too late

Zaif is one of the oldest crypto exchanges in Japan. Operating since 2014, it was the first exchange to receive an official license in Japan. Zaif offers more than 40 cryptocurrencies. In September 2018, the exchange had a major breach, as hackers gained access to its hot wallets.

https://crystalblockchain.com/articles/the-10-biggest-crypto-exchange-hacks-in-history/

A typical case of crime



8. BANCOR (2018) – the hack where users went unscathed

Bancor is an Israeli start-up founded in 2016. It is essentially a crypto company that offers a fully decentralized exchange service to its users. The firm raised $150m in an ICO in 2017.

However, the following year, it was hit by a major attack that resulted in total losses worth $23.5m. The hackers used a sophisticated technique in order to execute the crime. They targeted a specific wallet that the company was using to upgrade its smart contracts.

The Bancor exchange was taken offline after the incident. In addition, the company identified and tracked the stolen coins. They figured out that some of the coins had been transferred to other exchanges. Bancor then requested these exchanges to freeze the stolen coins.

https://crystalblockchain.com/articles/the-10-biggest-crypto-exchange-hacks-in-history/

A typical case of crime

9. COINCHECK (2018) – the biggest hack so far

Coincheck, a crypto exchange headquartered in Japan, was founded in 2012 and is considered to be among the top 20 exchanges in the world. The exchange offers a wide range of crypto, including bitcoin and Ethereum. In January 2018, bad actors managed to break into the exchange and steal crypto worth $534m.

This was confirmed as the largest crypto attack in history. As soon as the breach took place, Coincheck froze all deposits and withdrawals. However, the damage had already been done and the exchange admitted that it may not be able to cover the losses suffered by its users.

https://crystalblockchain.com/articles/the-10-biggest-crypto-exchange-hacks-in-history/

A typical case of crime

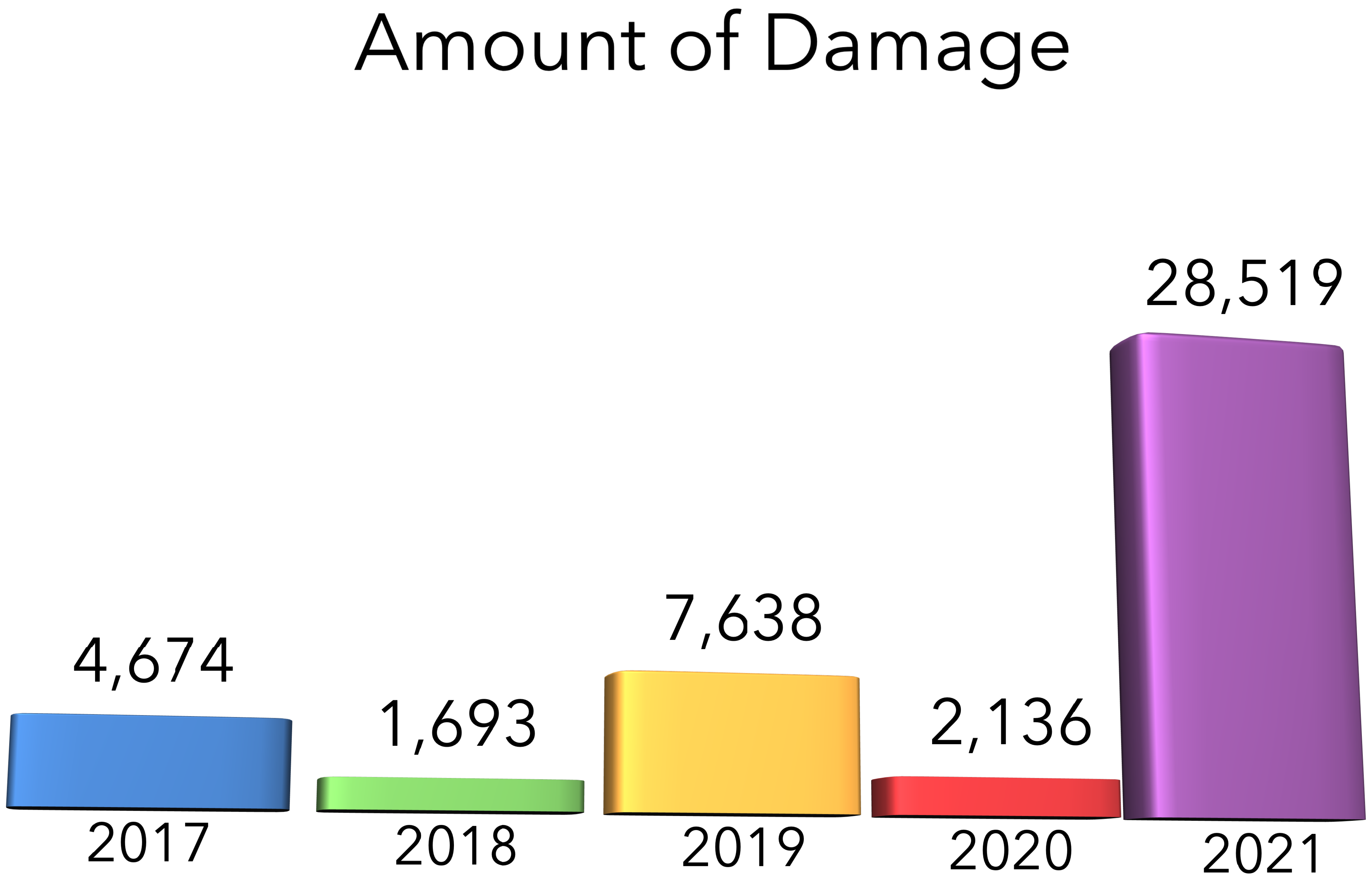
10. COINBENE (2019) – the hack that wasn't admitted at first

CoinBene is a Singapore-based crypto exchange that is operated by Chinese employees. It is considered to be among the top 10 crypto exchanges in the world by trading volume. The exchange serves the crypto community in over 192 countries.

In March 2019, CoinBene was attacked by cybercriminals who managed to walk away with over $105 million in cryptocurrencies. However, the exchange stated that it was closing down for maintenance activities, instead of accepting that the attack took place.

https://crystalblockchain.com/articles/the-10-biggest-crypto-exchange-hacks-in-history/

A typical case of crime



https://crystalblockchain.com/articles/the-10-biggest-crypto-exchange-hacks-in-history/

https://bloomingbit.io/news/6877479591032651840

The legal crime technique

- SCAM
- AML
- SIM Swapping
- Ransomware

SCAM

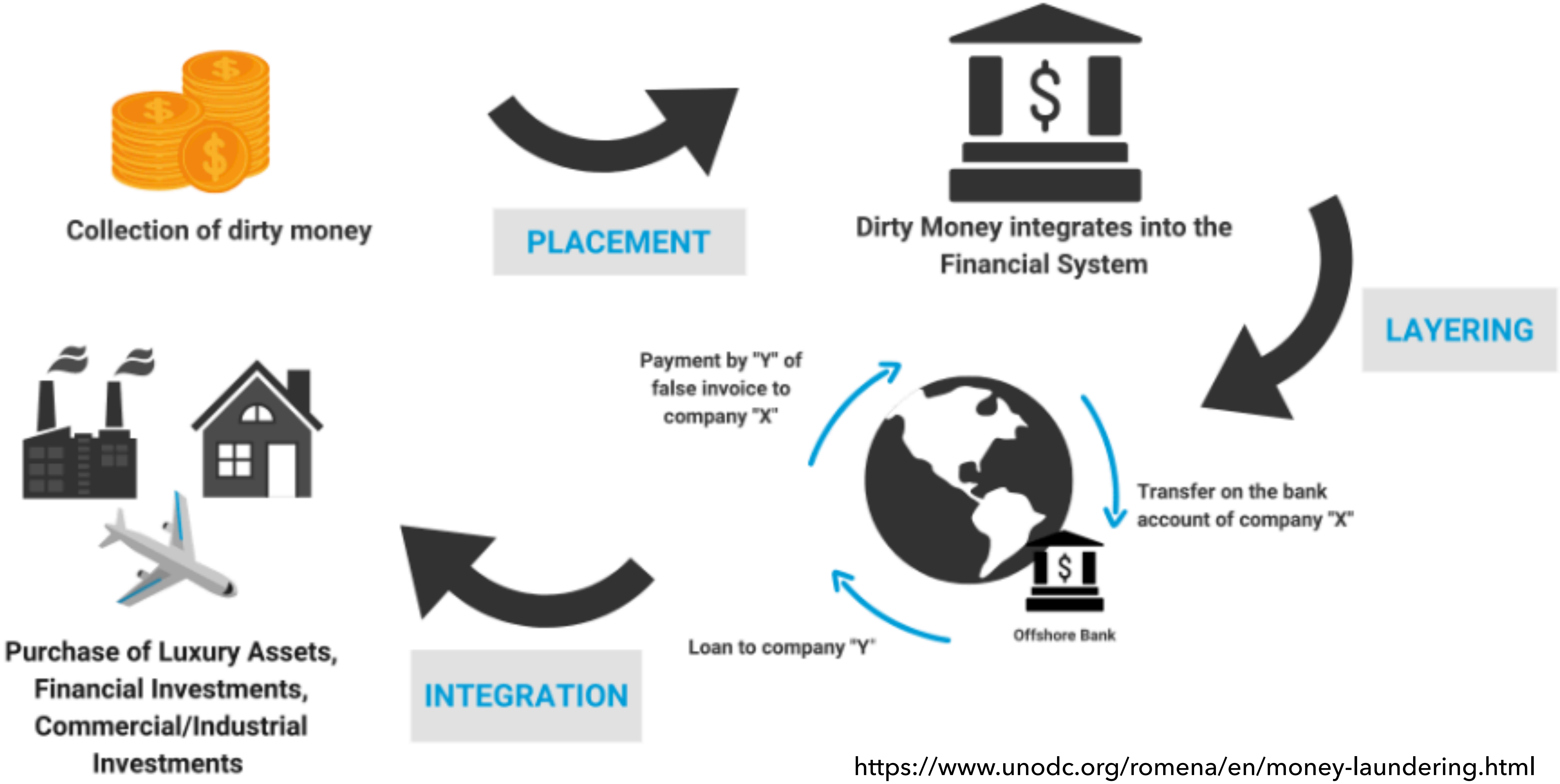
https://time.com/6162350/crypto-scams-online-crime-boom/

SCAM

https://www.coindeskkorea.com/news/articleView.html?idxno=77908

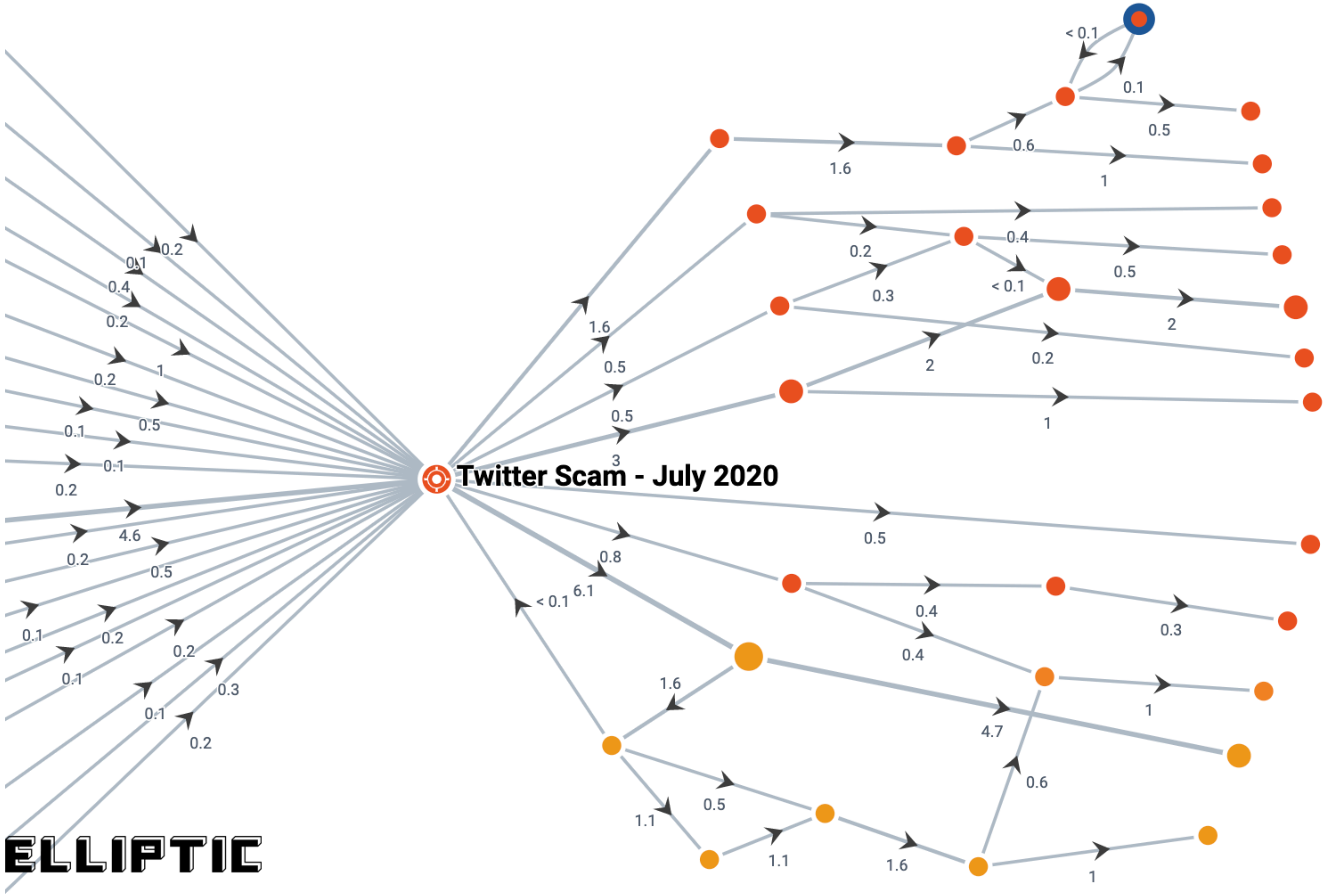
SCAM

Money Laundering


Collection of dirty money
PLACEMENT
Dirty Money integrates into the Financial System
LAYERING
Payment by "Y" of false invoice to company "X"
Transfer on the bank account of company "X"
Offshore Bank
Loan to company "Y"
INTEGRATION
Purchase of Luxury Assets, Financial Investments, Commercial/Industrial Investments

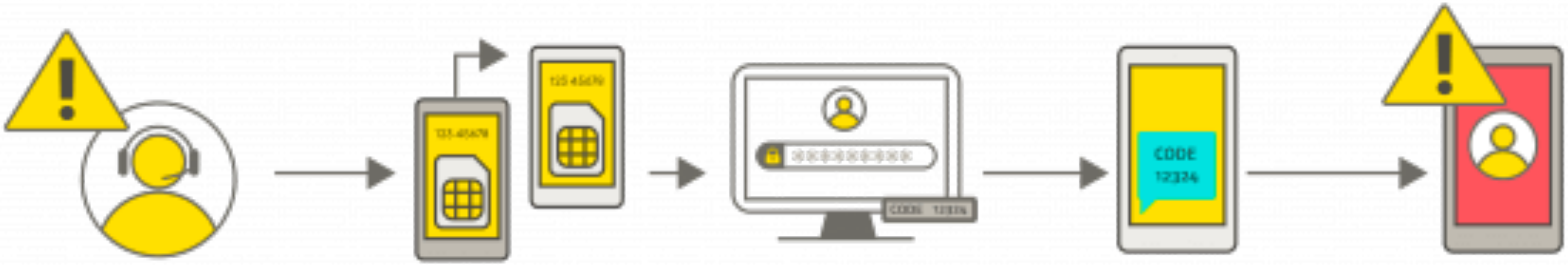
https://www.unodc.org/romena/en/money-laundering.html

Money Laundering



ELLIPTIC

SIM Swapping



1. Attacker calls target's mobile provider and requests that the target's mobile number is transferred

2. Number is transferred to a different SIM, target unaware

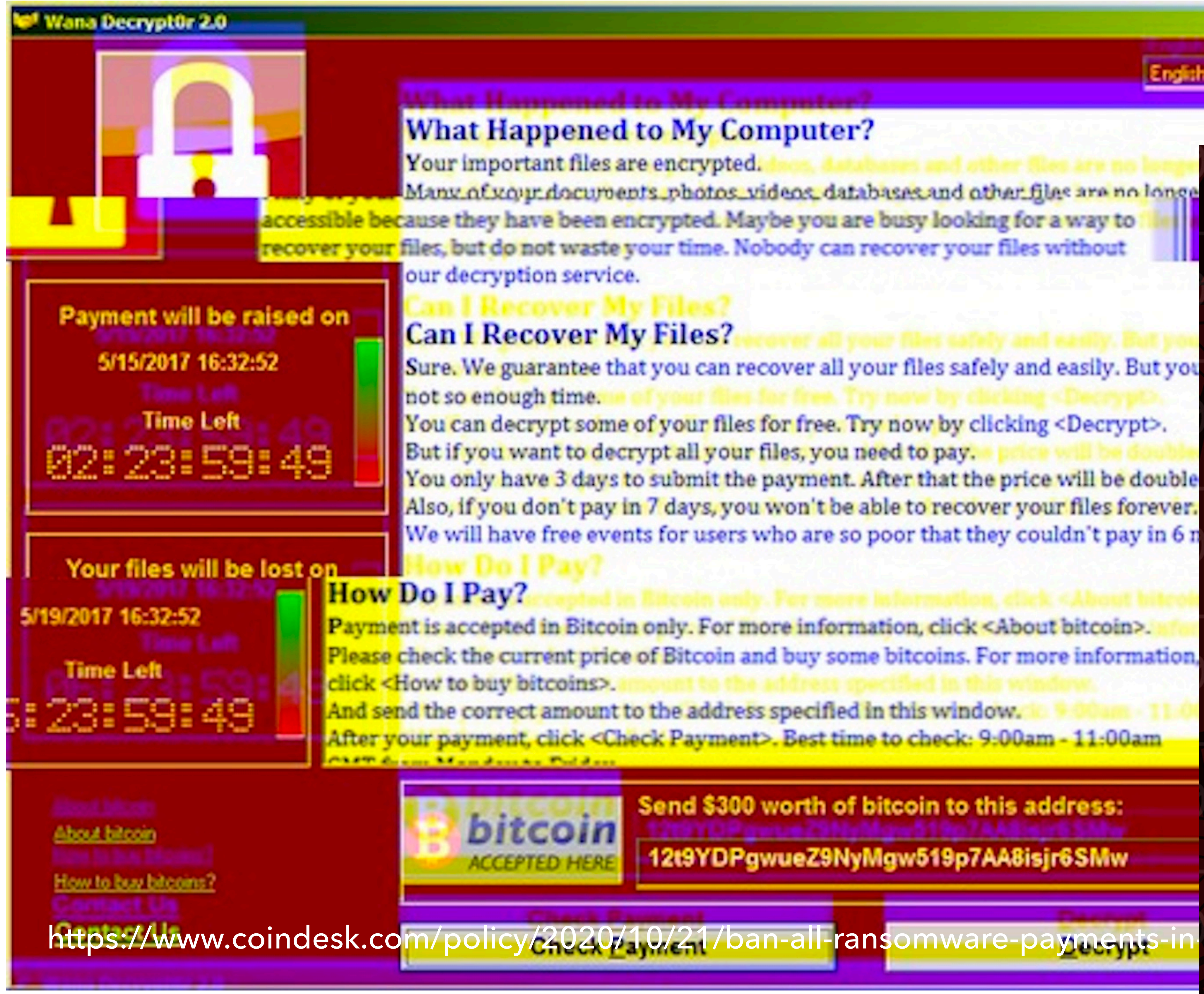
3. Attacker tries to access target's account, either using stolen credentials or requesting a password reset

4. The 2FA code is sent via SMS to the attacker and they can access the account

5. Target only becomes aware when their phone is disconnected or they're locked out of an account

https://heimdalsecurity.com/blog/what-is-sim-swapping/

Ransomware



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longe 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 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 double
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 m

How Do I Pay?

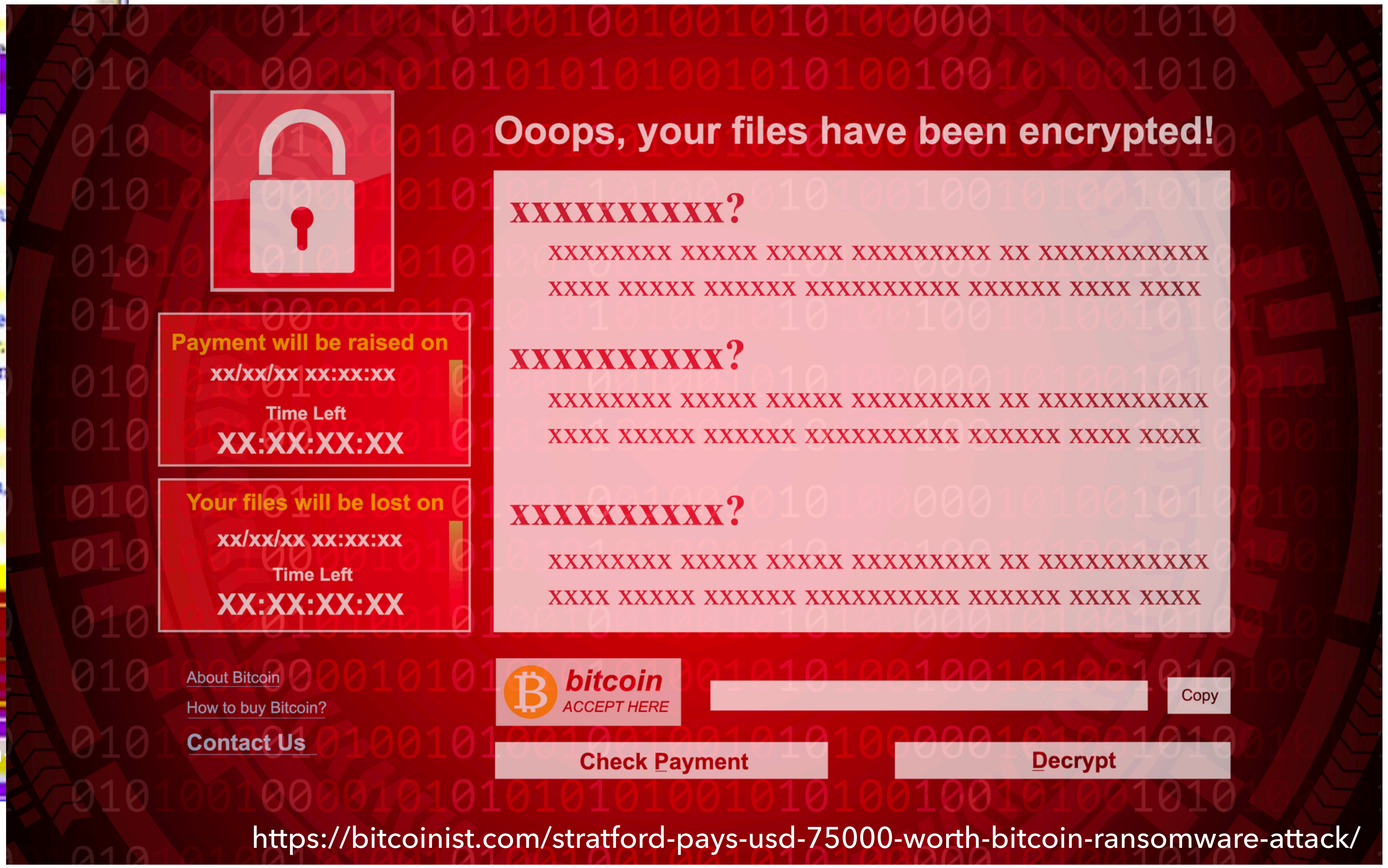
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/15/2017 16:32:52
Time Left
02:23:59:49

Your files will be lost on
5/19/2017 16:32:52
Time Left
6:23:59:49

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

https://www.coindesk.com/policy/2020/10/21/ban-all-ransomware-payments-in



Ooops, your files have been encrypted!

xxxxxxxxxx?
xxxxxxxx xxxxx xxxxx xxxxxxxxx xx xxxxxxxxxxx
xxxx xxxxx xxxxxx xxxxxxxxxx xxxxxx xxxx xxxx

xxxxxxxxxx?
xxxxxxxx xxxxx xxxxx xxxxxxxxx xx xxxxxxxxxxx
xxxx xxxxx xxxxxx xxxxxxxxxx xxxxxx xxxx xxxx

xxxxxxxxxx?
xxxxxxxx xxxxx xxxxx xxxxxxxxx xx xxxxxxxxxxx
xxxx xxxxx xxxxxx xxxxxxxxxx xxxxxx xxxx xxxx

Payment will be raised on
xx/xx/xx xx:xx:xx
Time Left
XX:XX:XX:XX

Your files will be lost on
xx/xx/xx xx:xx:xx
Time Left
XX:XX:XX:XX

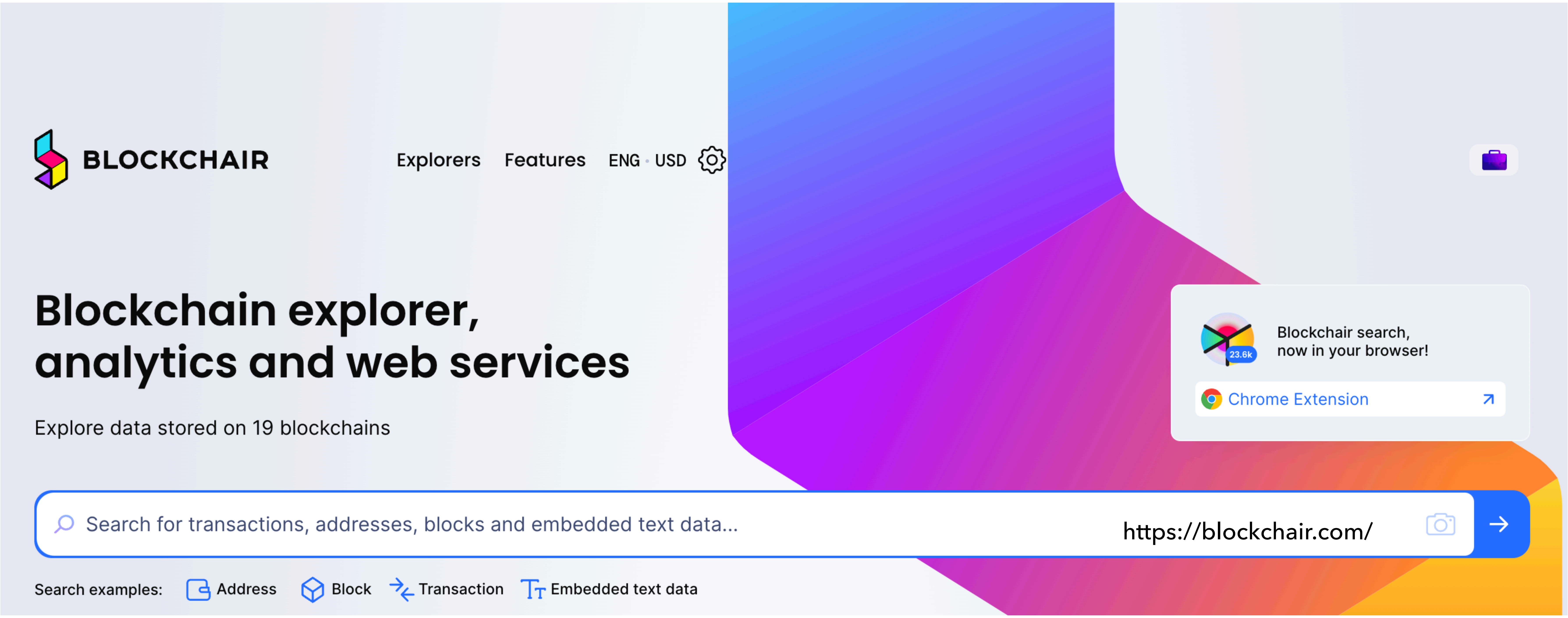
https://bitcoinist.com/stratford-pays-usd-75000-worth-bitcoin-ransomware-attack/

https://bloomingbit.io/news/6877479591032651840

To analyze transactions

- Blockchain explorer
- Solution
- Making analysis solution

Blockchain explorer



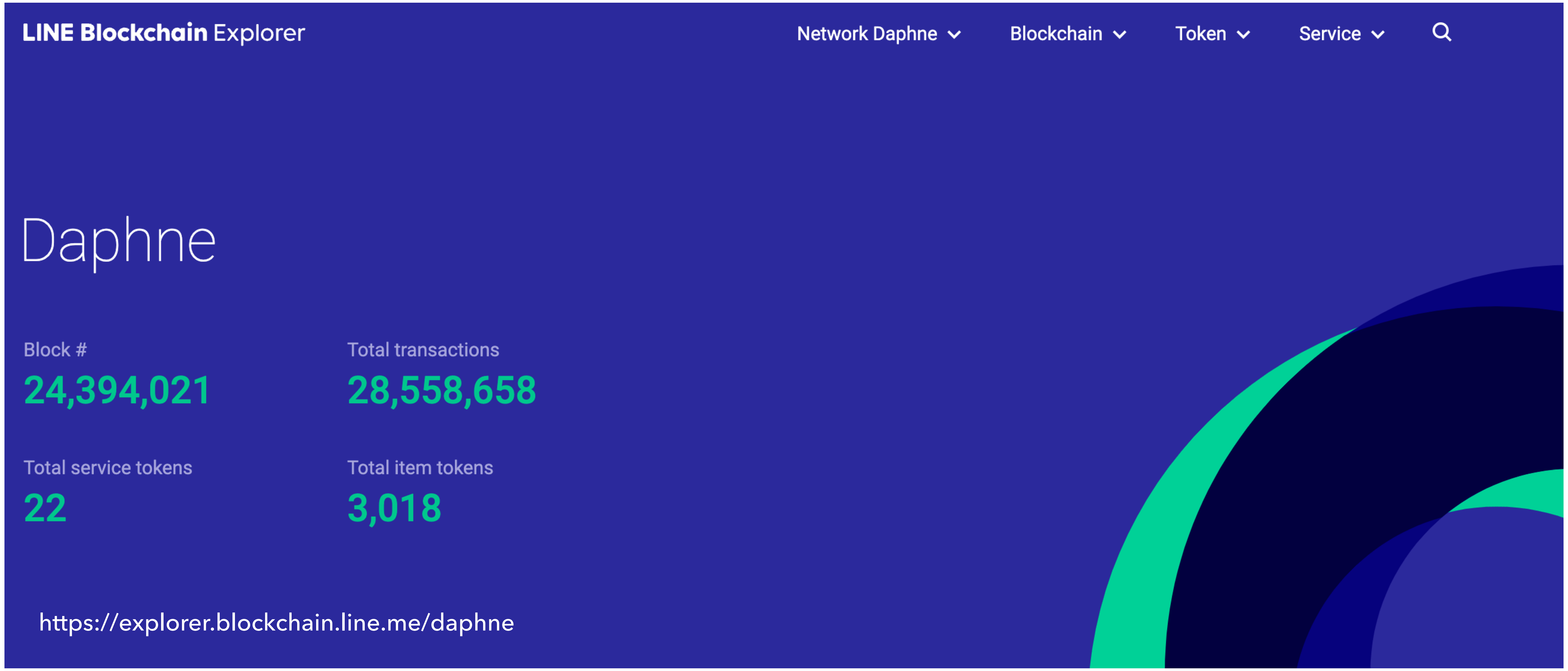
Blockchain explorer, analytics and web services

Explore data stored on 19 blockchains

Blockchair search, now in your browser!
23.6k
Chrome Extension
Search for transactions, addresses, blocks and embedded text data...
Search examples:
Address
Block
Transaction
Embedded text data

https://blockchair.com/

Blockchain explorer



Daphne

Block #

24,394,021

Total transactions

28,558,658

Total service tokens

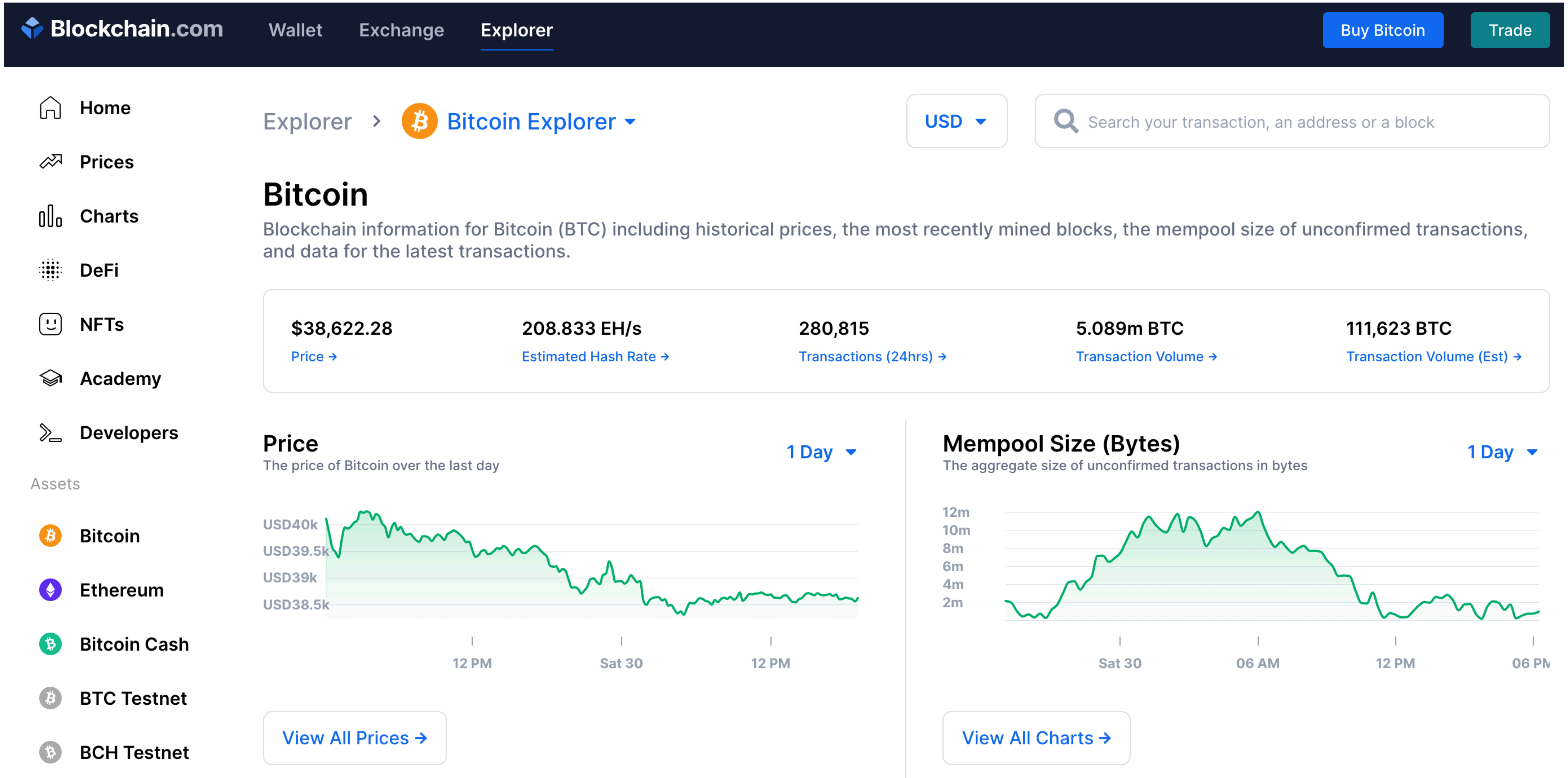
22

Total item tokens

3,018

https://explorer.blockchain.line.me/daphne

Blockchain explorer



Bitcoin

Blockchain information for Bitcoin (BTC) including historical prices, the most recently mined blocks, the mempool size of unconfirmed transactions, and data for the latest transactions.

$38,622.28	208.833 EH/s	280,815	5.089m BTC	111,623 BTC
Price →	Estimated Hash Rate →	Transactions (24hrs) →	Transaction Volume →	Transaction Volume (Est) →

Price

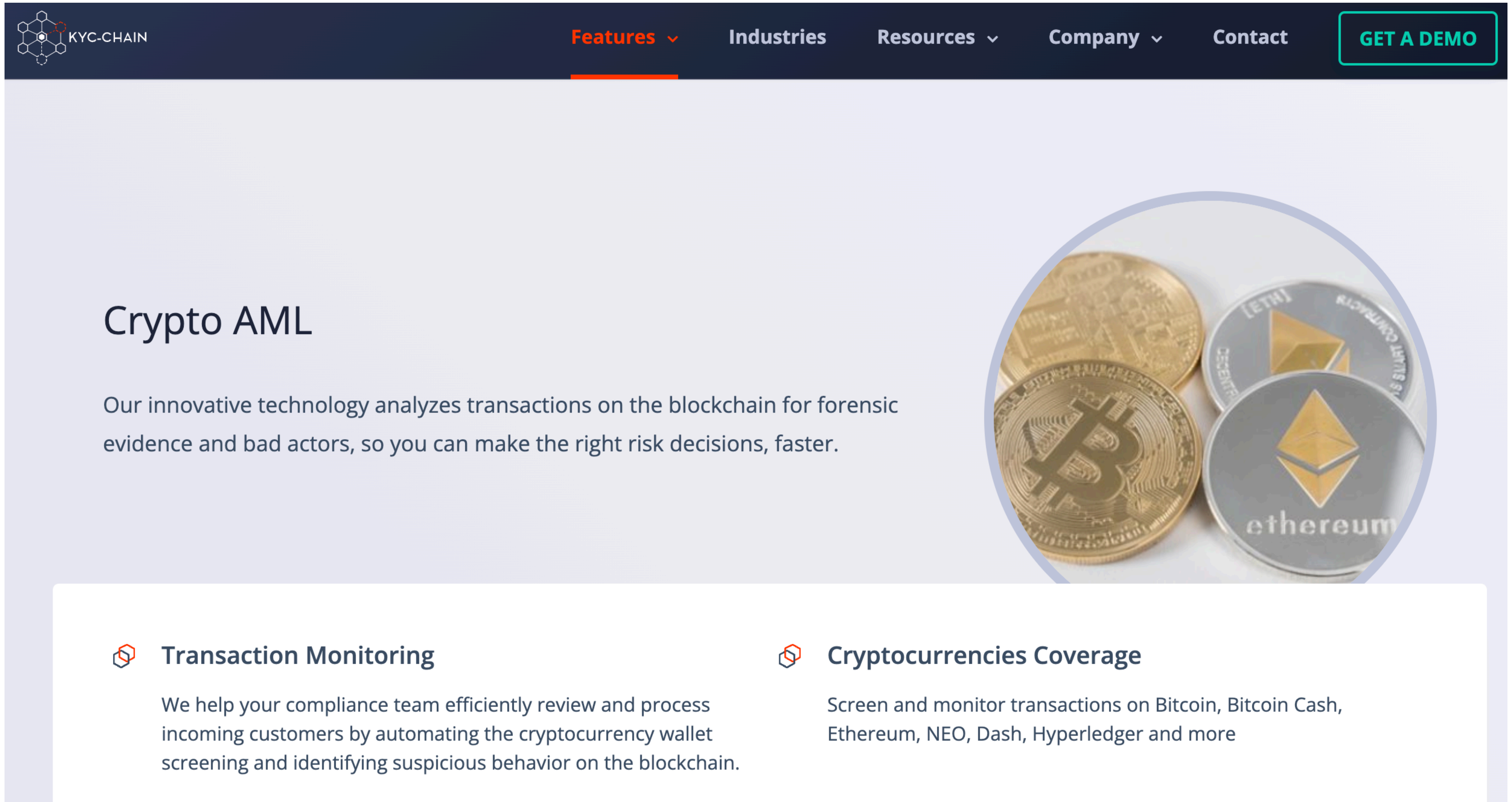
The price of Bitcoin over the last day

Mempool Size (Bytes)

The aggregate size of unconfirmed transactions in bytes

https://www.blockchain.com/explorer

Solution



Crypto AML

Our innovative technology analyzes transactions on the blockchain for forensic evidence and bad actors, so you can make the right risk decisions, faster.

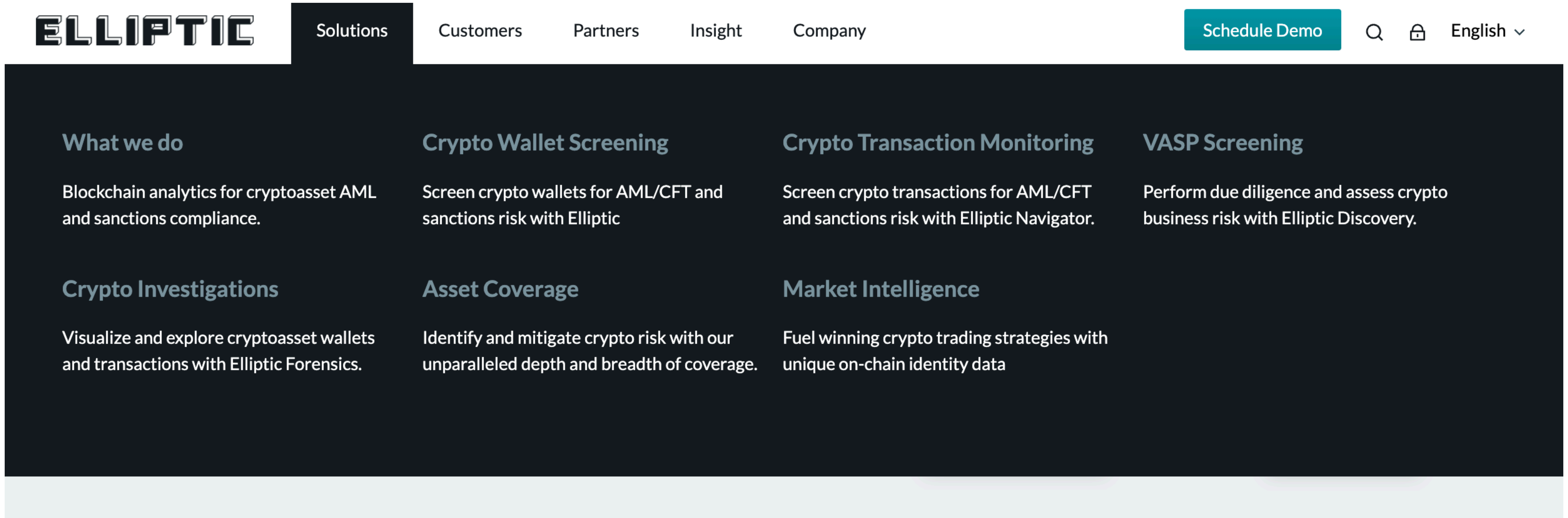
Transaction Monitoring

We help your compliance team efficiently review and process incoming customers by automating the cryptocurrency wallet screening and identifying suspicious behavior on the blockchain.

Cryptocurrencies Coverage

Screen and monitor transactions on Bitcoin, Bitcoin Cash, Ethereum, NEO, Dash, Hyperledger and more

Solution



What we do

Blockchain analytics for cryptoasset AML and sanctions compliance.

Crypto Wallet Screening

Screen crypto wallets for AML/CFT and sanctions risk with Elliptic

Crypto Transaction Monitoring

Screen crypto transactions for AML/CFT and sanctions risk with Elliptic Navigator.

VASP Screening

Perform due diligence and assess crypto business risk with Elliptic Discovery.

Crypto Investigations

Visualize and explore cryptoasset wallets and transactions with Elliptic Forensics.

Asset Coverage

Identify and mitigate crypto risk with our unparalleled depth and breadth of coverage.

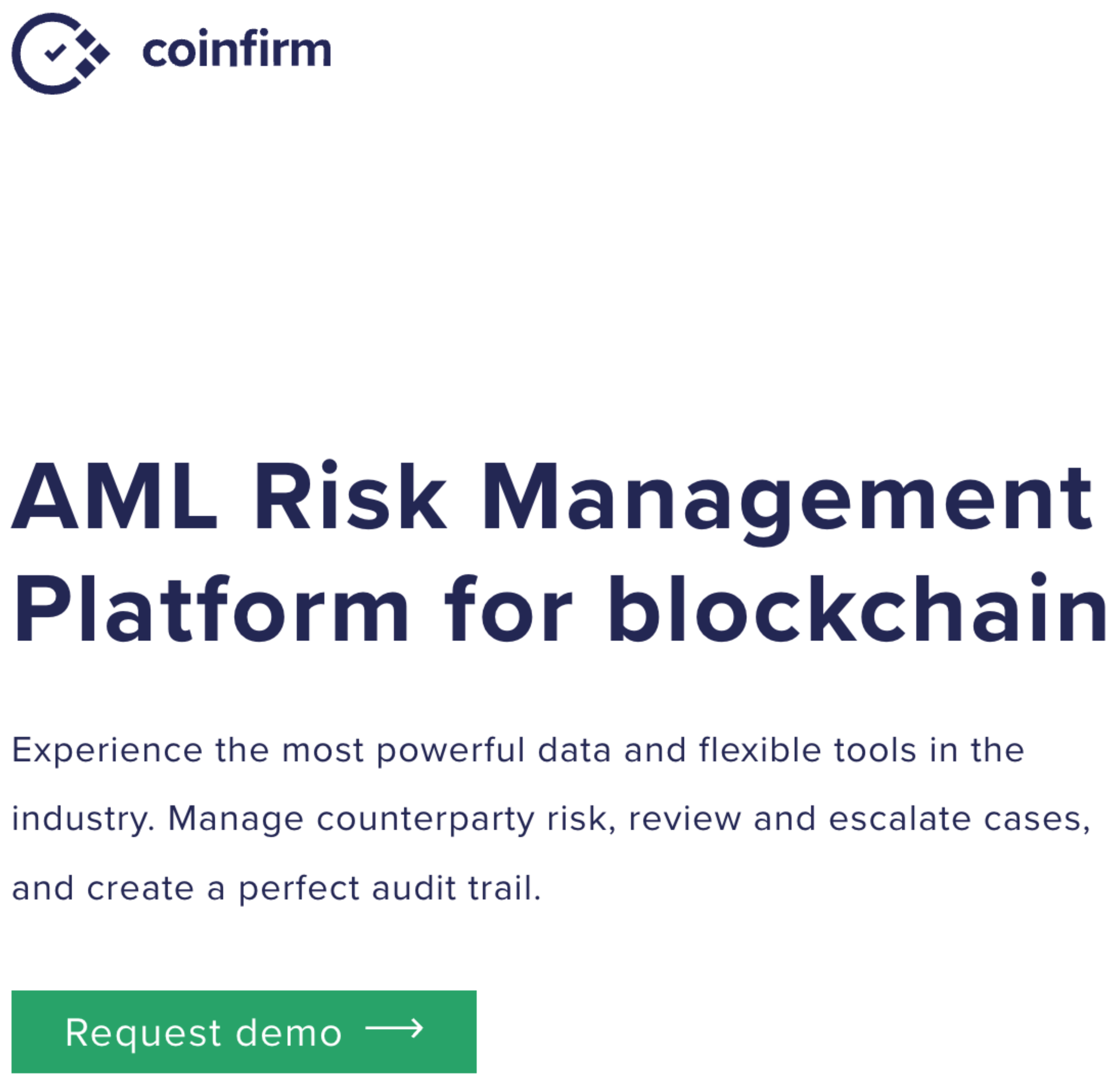
Market Intelligence

Fuel winning crypto trading strategies with unique on-chain identity data

Compliance Drives Growth

Compliance is a competitive advantage that builds trust with regulators, customers, and partners. Having the most accurate AML monitoring solutions is critical, as is investing in your team to build the knowledge needed to remain compliant.

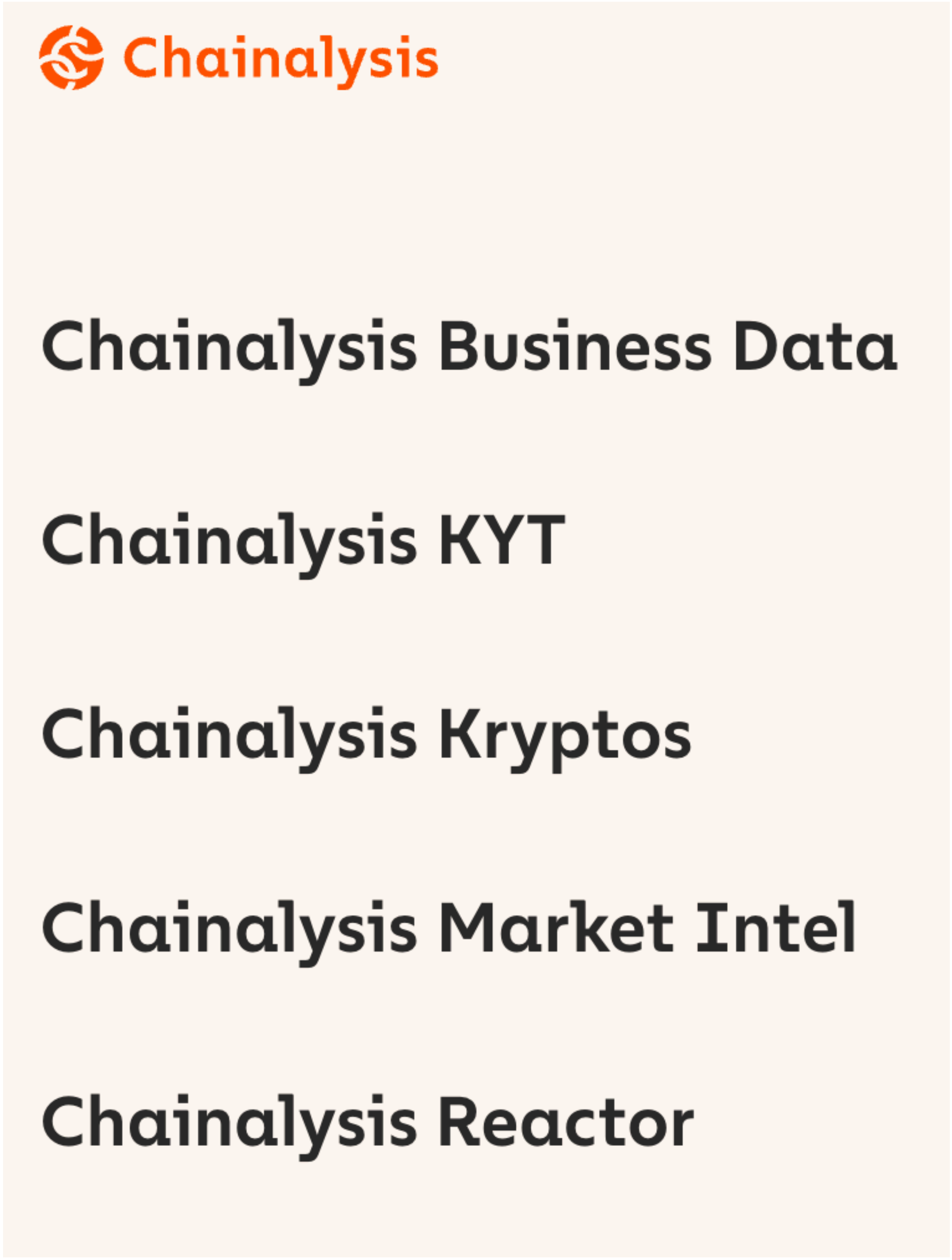
Solution



coinfirm

AML Risk Management Platform for blockchain

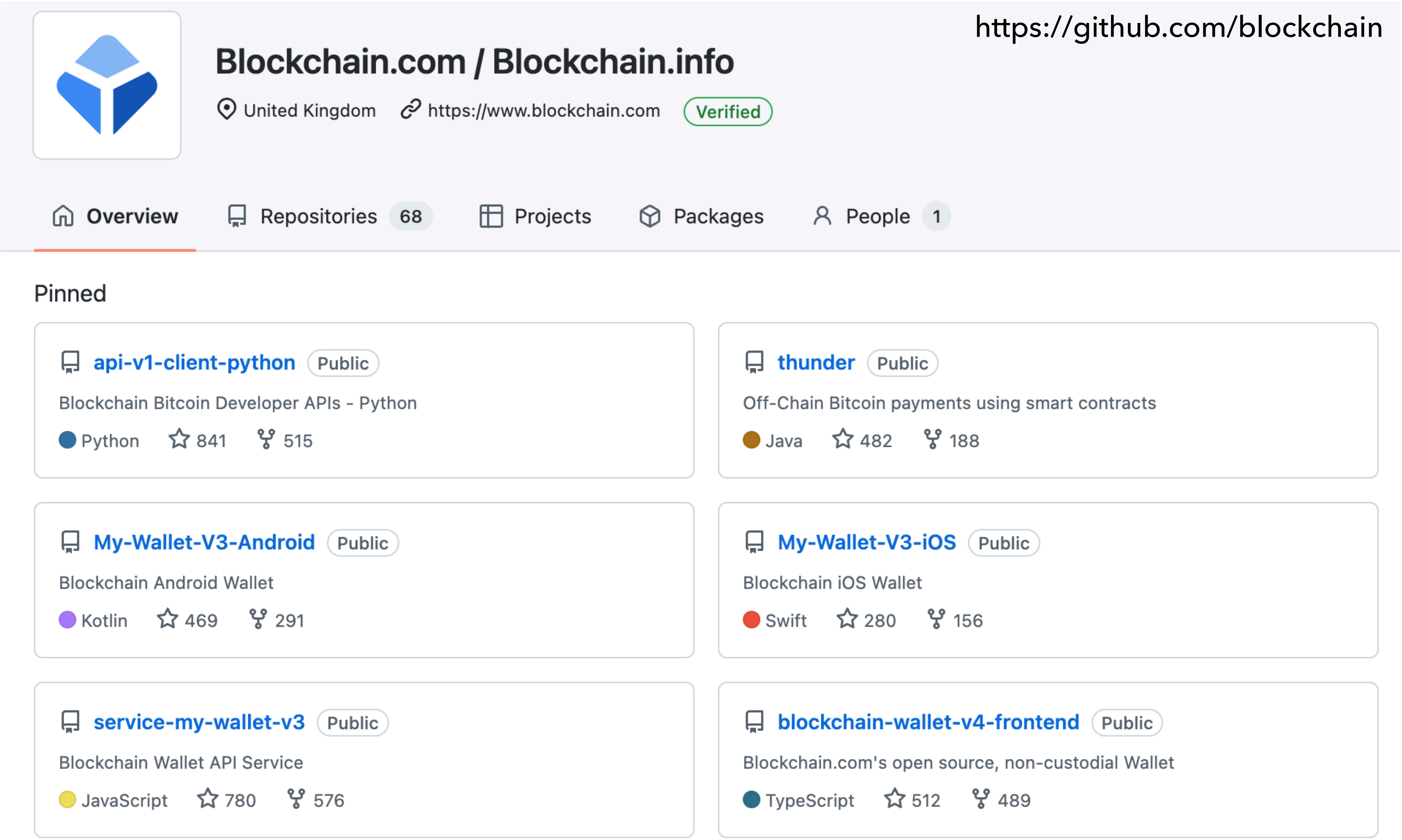
Experience the most powerful data and flexible tools in the industry. Manage counterparty risk, review and escalate cases, and create a perfect audit trail.



Chainalysis

- Chainalysis Business Data
- Chainalysis KYT
- Chainalysis Kryptos
- Chainalysis Market Intel
- Chainalysis Reactor

Making analysis solution



https://github.com/blockchain

Blockchain.com / Blockchain.info

United Kingdom https://www.blockchain.com Verified

Overview | Repositories 68 | Projects | Packages | People 1

Pinned

api-v1-client-python Public
Blockchain Bitcoin Developer APIs - Python
● Python ☆ 841 ⑂ 515

thunder Public
Off-Chain Bitcoin payments using smart contracts
● Java ☆ 482 ⑂ 188

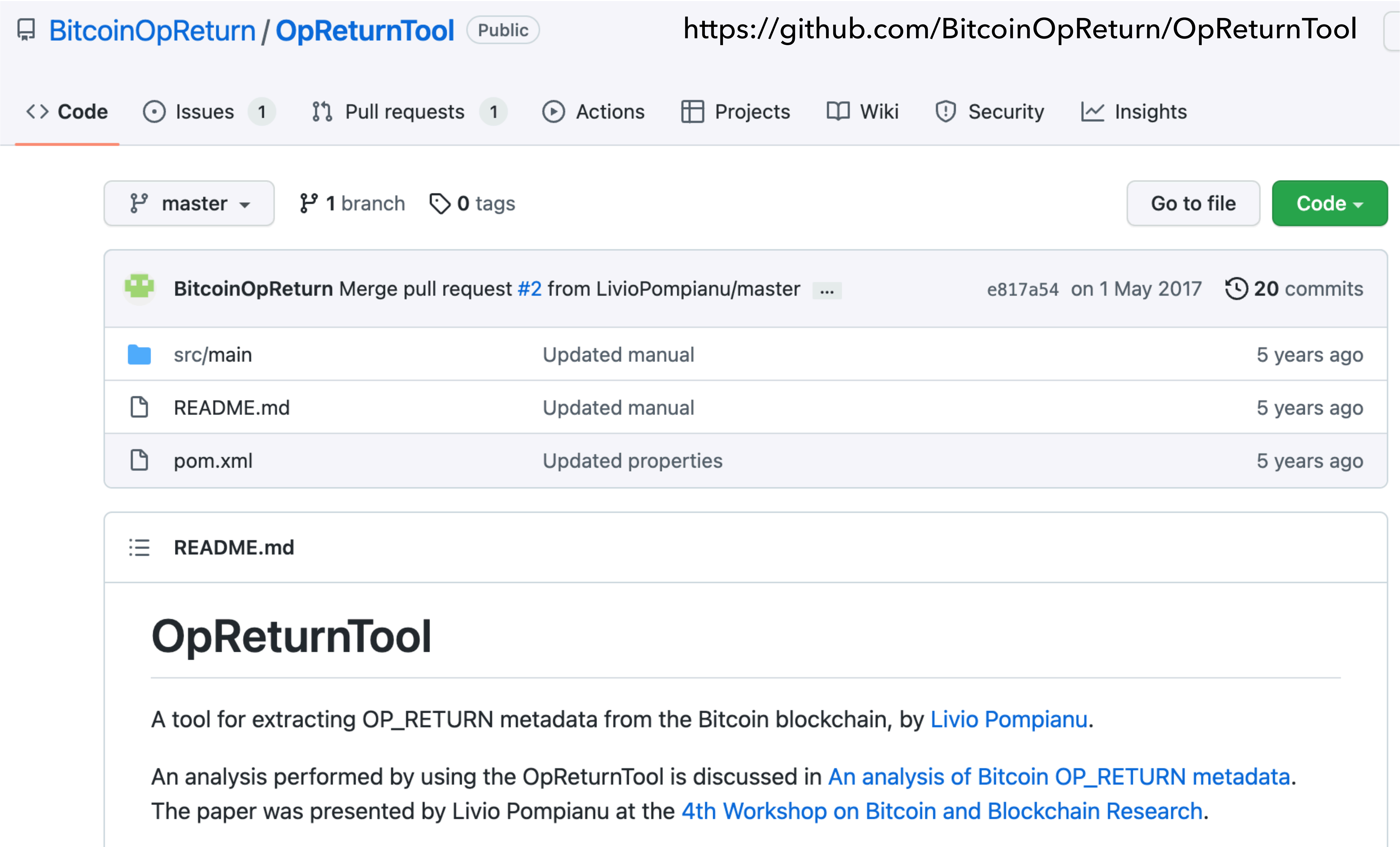
My-Wallet-V3-Android Public
Blockchain Android Wallet
● Kotlin ☆ 469 ⑂ 291

My-Wallet-V3-iOS Public
Blockchain iOS Wallet
● Swift ☆ 280 ⑂ 156

service-my-wallet-v3 Public
Blockchain Wallet API Service
● JavaScript ☆ 780 ⑂ 576

blockchain-wallet-v4-frontend Public
Blockchain.com's open source, non-custodial Wallet
● TypeScript ☆ 512 ⑂ 489

Making analysis solution



https://github.com/BitcoinOpReturn/OpReturnTool

BitcoinOpReturn Merge pull request #2 from LivioPompianu/master ... e817a54 on 1 May 2017 20 commits

src/main	Updated manual	5 years ago
README.md	Updated manual	5 years ago
pom.xml	Updated properties	5 years ago

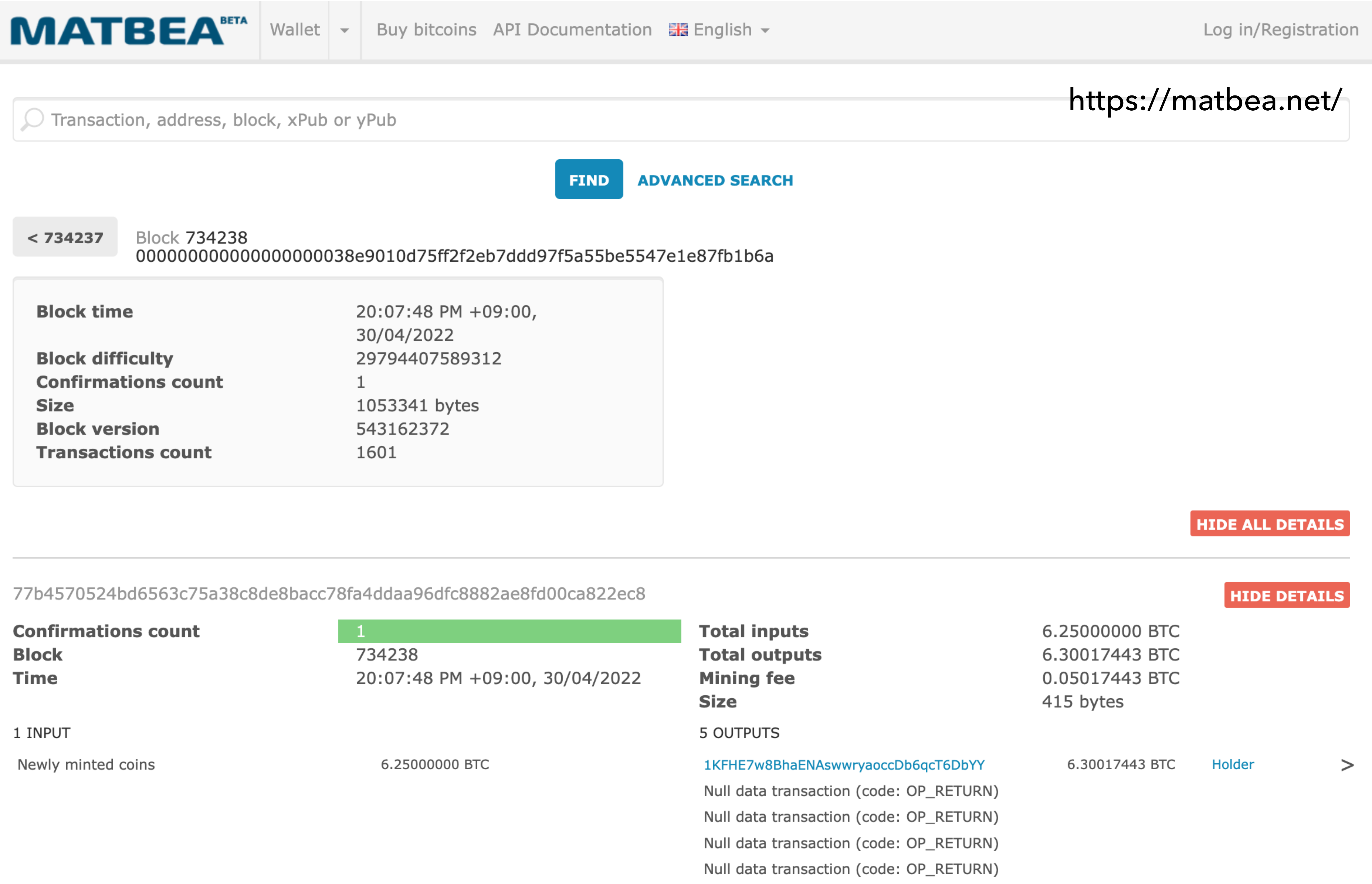
README.md

OpReturnTool

A tool for extracting OP_RETURN metadata from the Bitcoin blockchain, by Livio Pompianu.

An analysis performed by using the OpReturnTool is discussed in An analysis of Bitcoin OP_RETURN metadata. The paper was presented by Livio Pompianu at the 4th Workshop on Bitcoin and Blockchain Research.

Making analysis solution



https://matbea.net/

Block 734238
0000000000000000000038e9010d75ff2f2eb7ddd97f5a55be5547e1e87fb1b6a

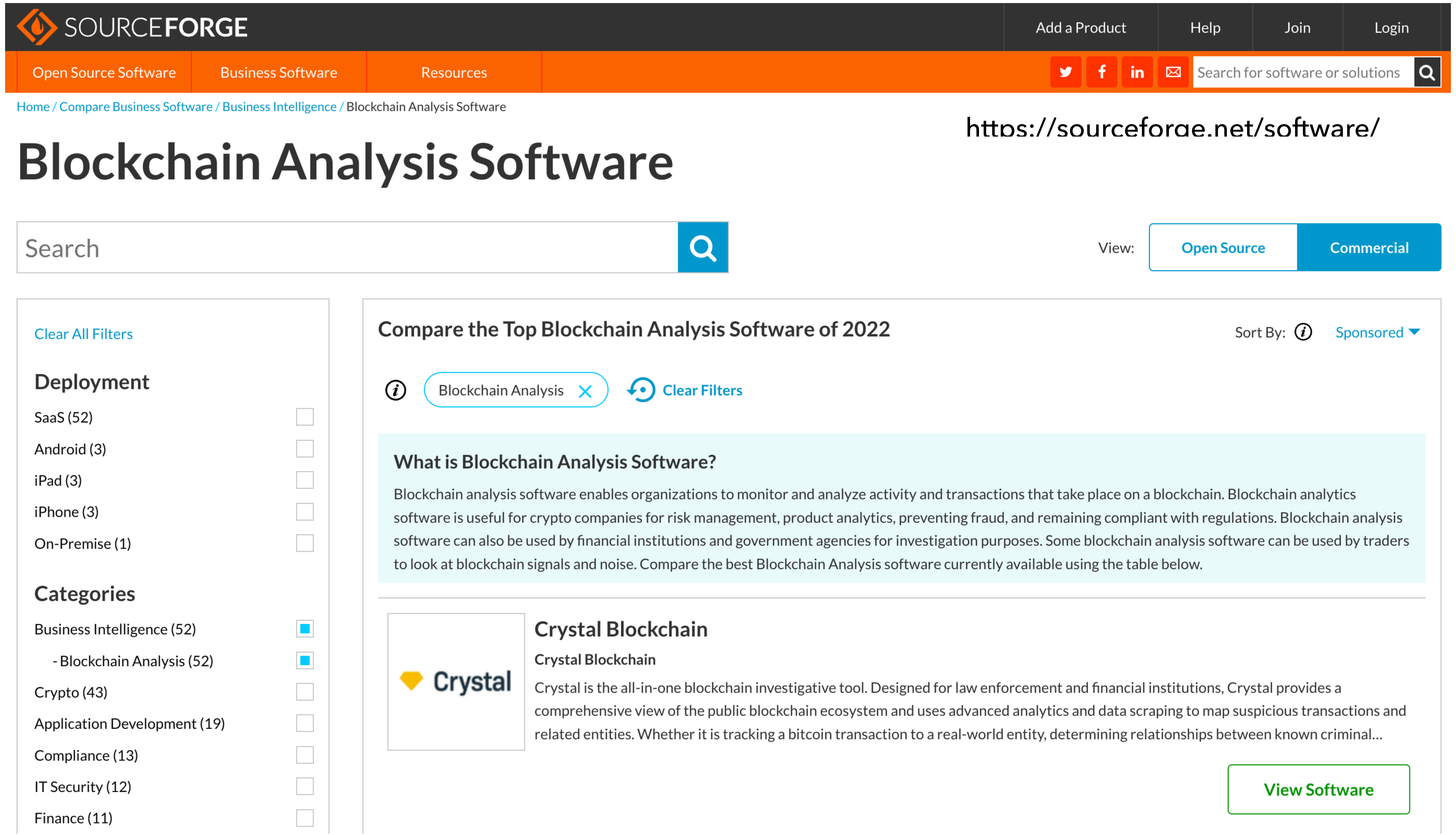
Block time	20:07:48 PM +09:00, 30/04/2022
Block difficulty	29794407589312
Confirmations count	1
Size	1053341 bytes
Block version	543162372
Transactions count	1601

77b4570524bd6563c75a38c8de8bacc78fa4ddaa96dfc8882ae8fd00ca822ec8

Confirmations count	1	**Total inputs**	6.25000000 BTC
Block	734238	**Total outputs**	6.30017443 BTC
Time	20:07:48 PM +09:00, 30/04/2022	**Mining fee**	0.05017443 BTC
		Size	415 bytes

1 INPUT		5 OUTPUTS	
Newly minted coins	6.25000000 BTC	1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY	6.30017443 BTC
		Null data transaction (code: OP_RETURN)	
		Null data transaction (code: OP_RETURN)	
		Null data transaction (code: OP_RETURN)	
		Null data transaction (code: OP_RETURN)	

Making analysis solution



https://sourceforge.net/software/

Home / Compare Business Software / Business Intelligence / Blockchain Analysis Software

Blockchain Analysis Software

Clear All Filters

Deployment

- SaaS (52) □
- Android (3) □
- iPad (3) □
- iPhone (3) □
- On-Premise (1) □

Categories

- Business Intelligence (52) ☑
- - Blockchain Analysis (52) ☑
- Crypto (43) □
- Application Development (19) □
- Compliance (13) □
- IT Security (12) □
- Finance (11) □

Compare the Top Blockchain Analysis Software of 2022

Sort By: Sponsored

Blockchain Analysis ✕ Clear Filters

What is Blockchain Analysis Software?

Blockchain analysis software enables organizations to monitor and analyze activity and transactions that take place on a blockchain. Blockchain analytics software is useful for crypto companies for risk management, product analytics, preventing fraud, and remaining compliant with regulations. Blockchain analysis software can also be used by financial institutions and government agencies for investigation purposes. Some blockchain analysis software can be used by traders to look at blockchain signals and noise. Compare the best Blockchain Analysis software currently available using the table below.

Crystal Blockchain

Crystal Blockchain

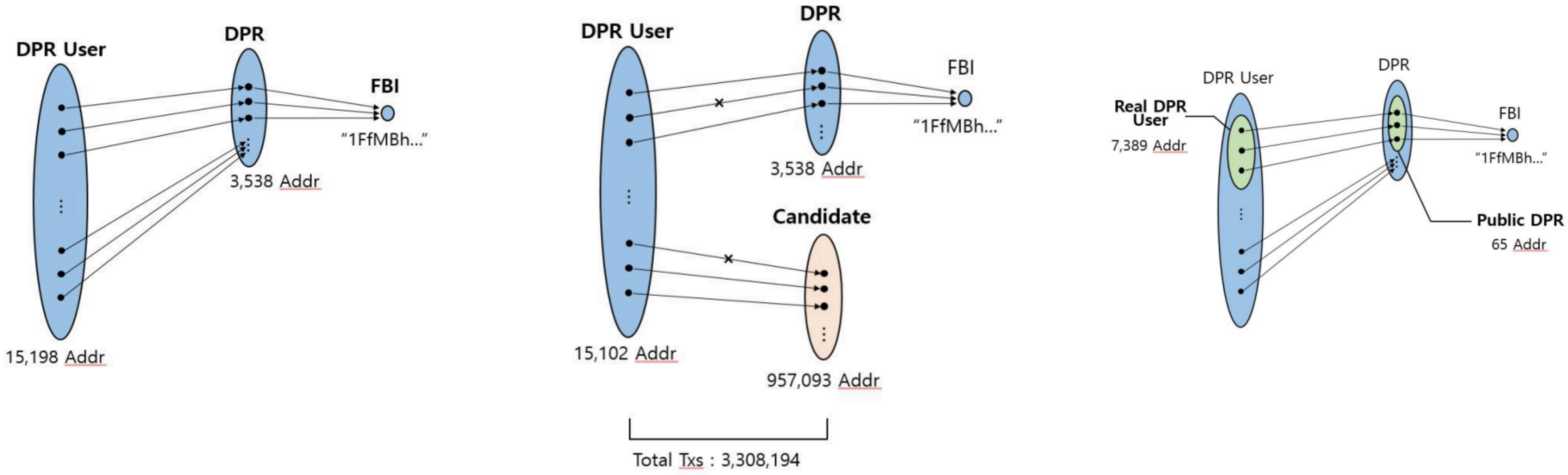
Crystal is the all-in-one blockchain investigative tool. Designed for law enforcement and financial institutions, Crystal provides a comprehensive view of the public blockchain ecosystem and uses advanced analytics and data scraping to map suspicious transactions and related entities. Whether it is tracking a bitcoin transaction to a real-world entity, determining relationships between known criminal...

A method of dealing with crime

- Block transaction
- Management of Wallet & User
- Communication global finance group
- Share crime pattern for Government

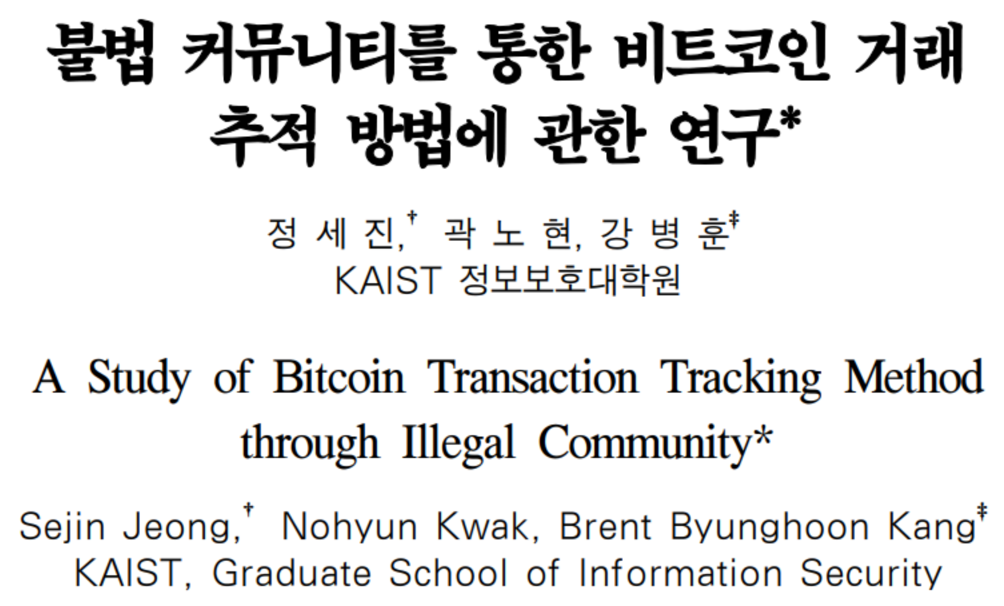
https://bloomingbit.io/news/6877479591032651840

Block transaction



https://www.koreascience.or.kr/article/JAKO201820765436753.pdf

Block transaction

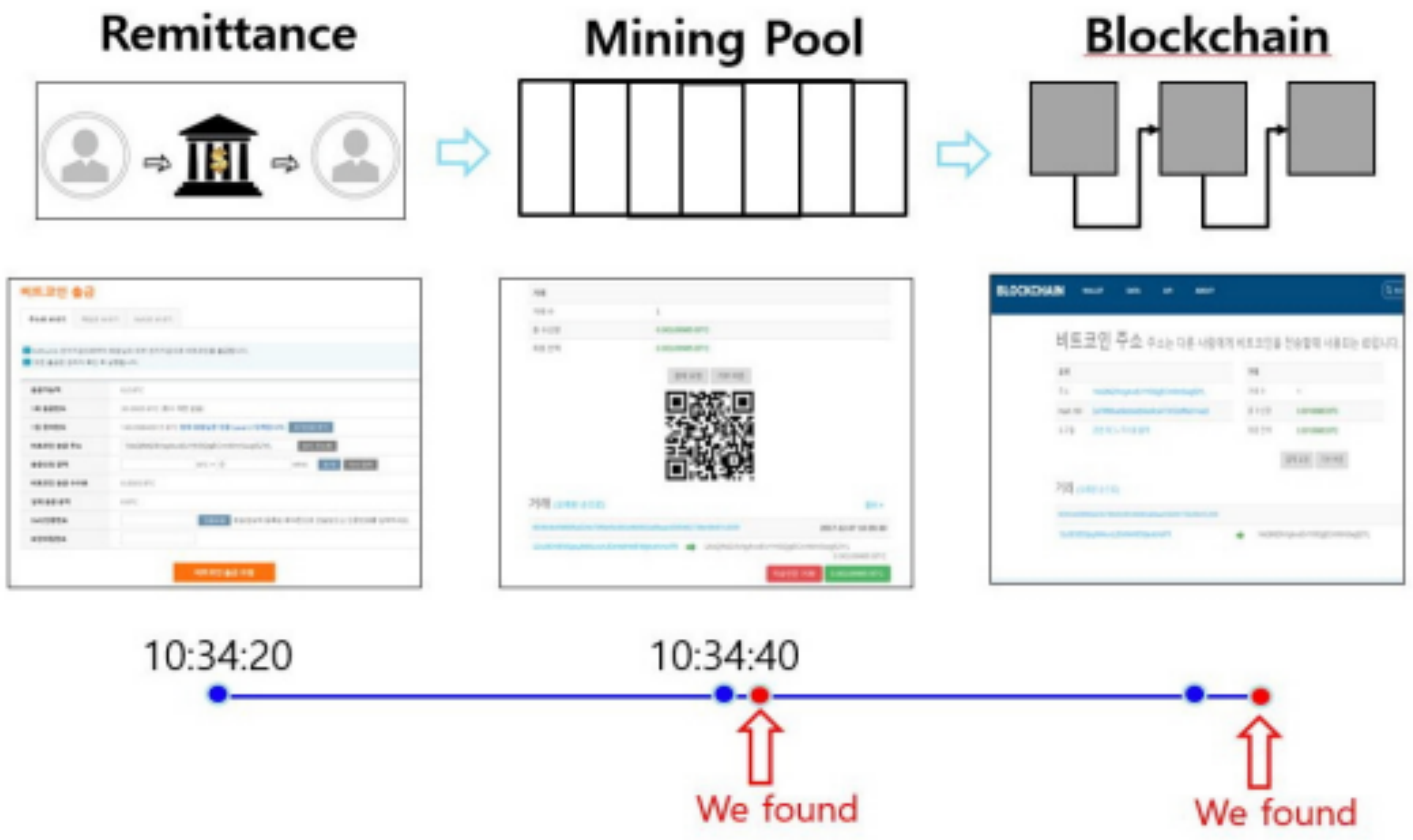


불법 커뮤니티를 통한 비트코인 거래 추적 방법에 관한 연구*

정세진,[†] 곽노현, 강병훈[‡]
KAIST 정보보호대학원

A Study of Bitcoin Transaction Tracking Method through Illegal Community*

Sejin Jeong,[†] Nohyun Kwak, Brent Byunghoon Kang[‡]
KAIST, Graduate School of Information Security



https://www.koreascience.or.kr/article/JAKO201820765436753.pdf

Management of Wallet & User

CDD/EDD	Development	Solution
User	Transaction	Wallet
Block	Block	Block
Suspicious	Suspicious	Suspicious
Monitoring	Monitoring	Monitoring
Normal	Normal	Normal

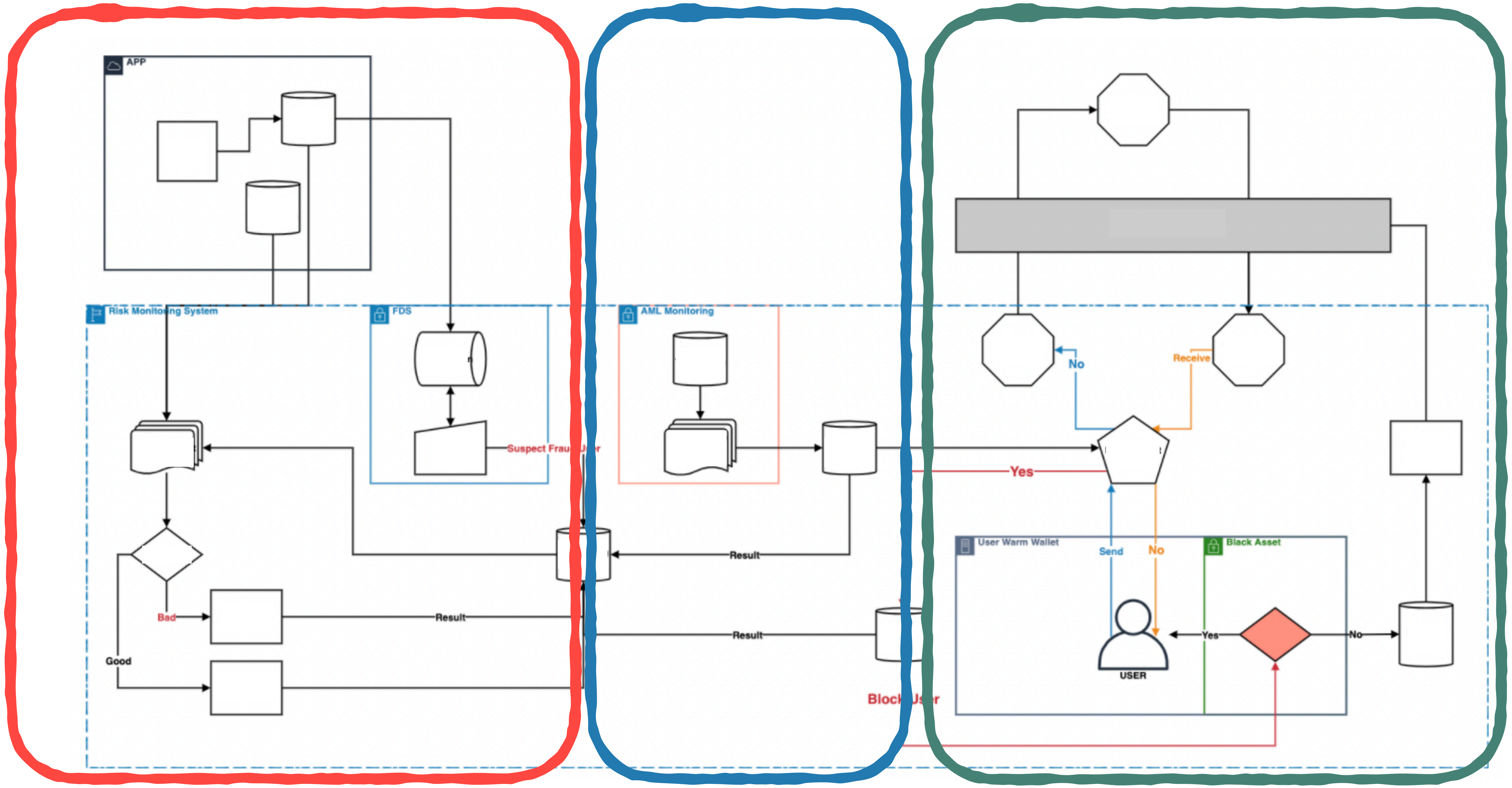
CDD : Customer Due Diligence

EDD : Enhanced Due Diligence

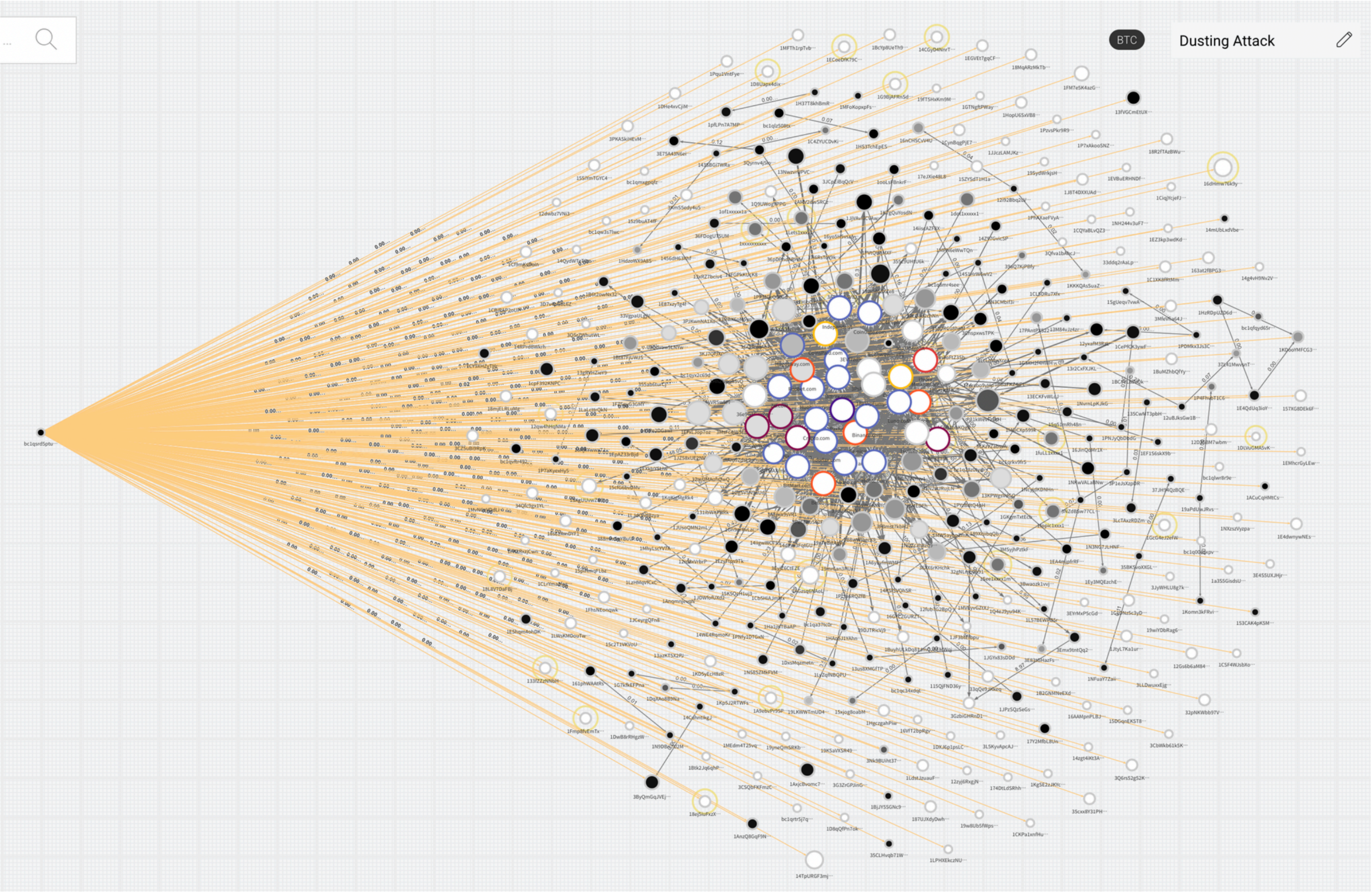
Communication of global finance group

- FATF (The Financial Action Task Force)
- APG (The Asia Pacific Group on Money Laundering)
- CFATF (The Caribbean Financial Action Track Force)
- ESAAMLG (The Eastern and Southern Africa Anti-Money Laundering Group)
- GAFILAT (El Grupo de Acción Financiera de Latinoamérica - Financial Action Task Force of Latin America)
- MENAFATF (Middle East And North Africa Financial Action Task Force)
- Moneyval

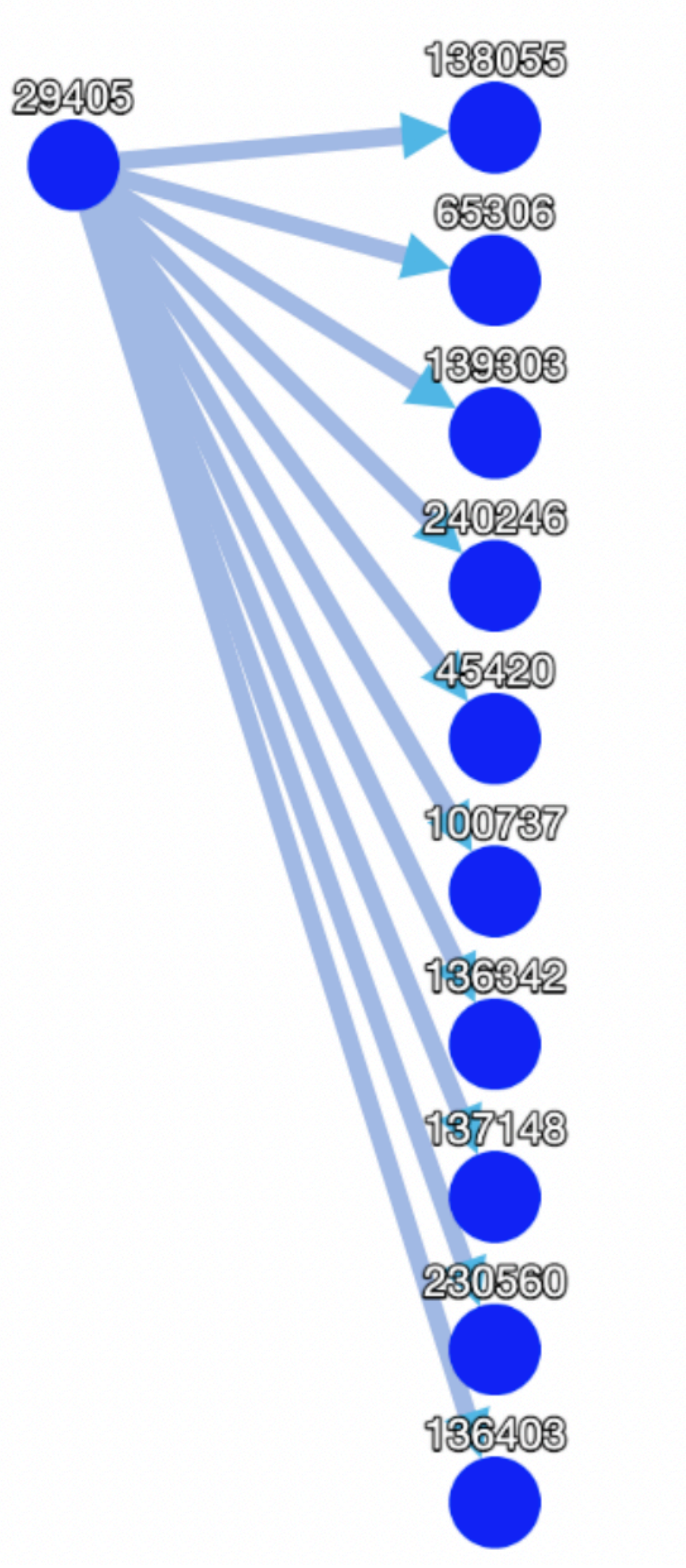
Risk Management System

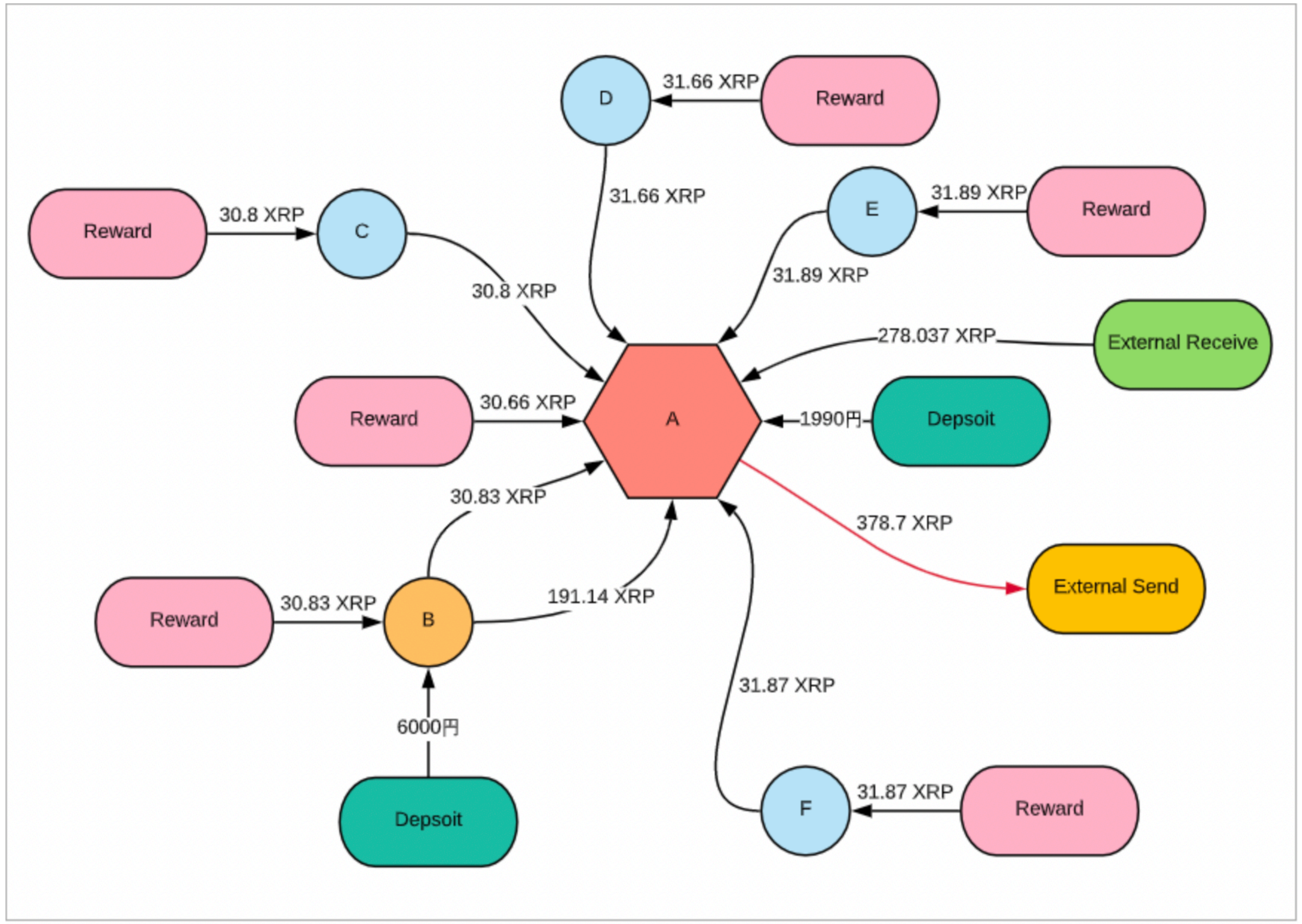


Risk Management System

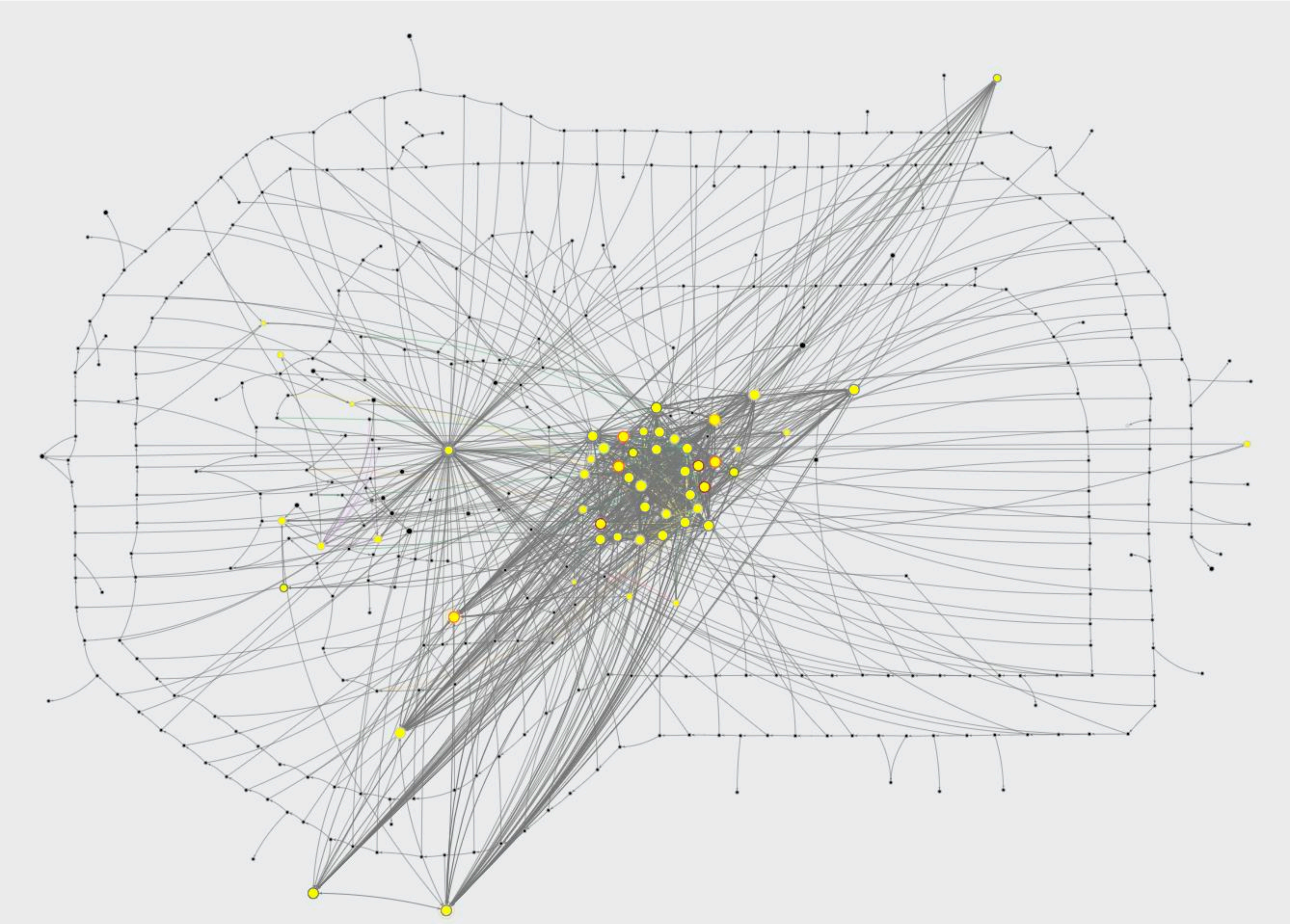


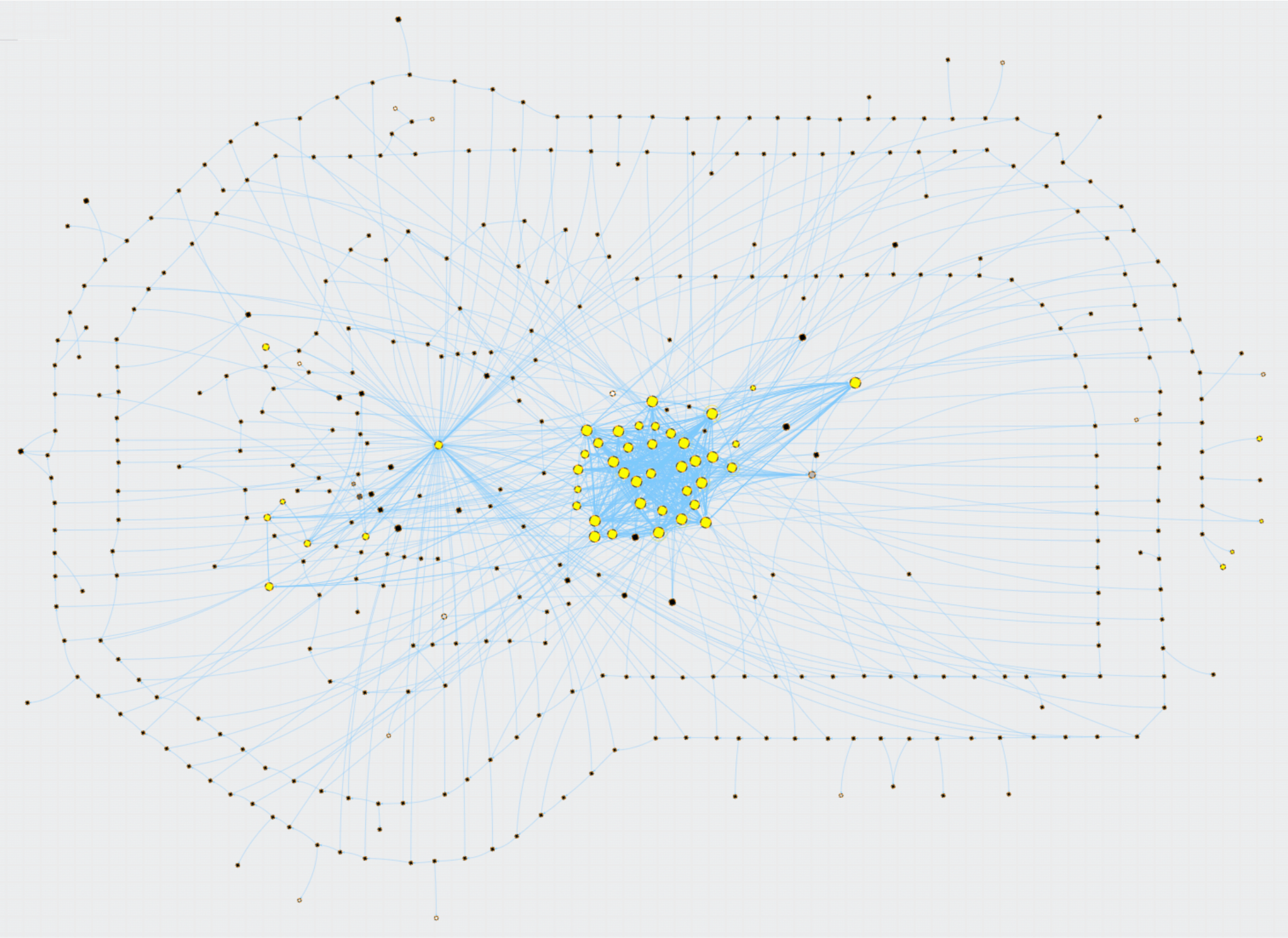
Risk Management System





Risk Management System





Share crime pattern of government

- Share crime of guide line
- Trend of crime case
- Informality of seminar
- Formality of Meeting

Thanks for listening

- Do you have any questions for me?
  - crattack@gmail.com
- Shout out to @Roy and @Gracemj

https://www.linkedin.com/in/crattack/