TxMon: Tool for monitoring illegal Bitcoin transactions

IS593

[Do it] SeJin Jeong, Nohyun Kwak

KAIST

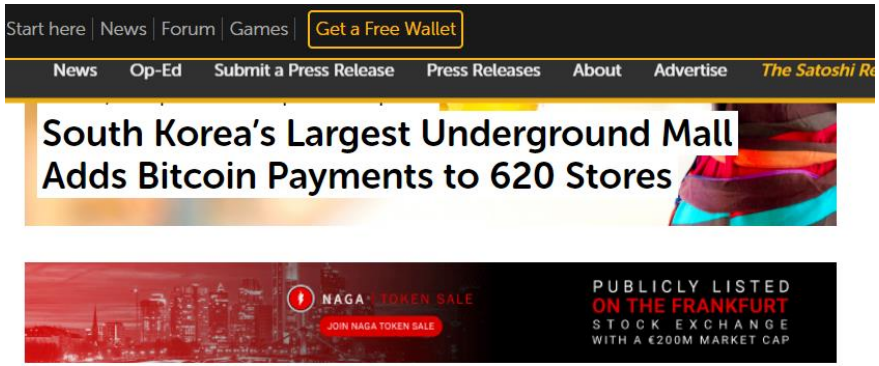
KAIST 한국과학기술원

Contents

- Introduction
- Background
- Design
- Implementation
- Evaluation
- Related work
- Limitation & Discussion
- Conclusion

Motivation

- Beginning this mid-December, shoppers can pay with bitcoin at the 620 stores in Seoul shopping mall
- As many bitcoin users spend bitcoin in open place, possible to track illegal bitcoin transaction



The largest underground shopping mall in South Korea, Goto Mall, has partnered with a local cryptocurrency exchange to enable its 620 stores to accept bitcoin. Spanning 880 meters long, about half a million people walk through the mall each day.

Also read: *Hong Kong Company Set to Build Crypto Mining Farm and Museum on Russian Island*

Goto Mall, a Bitcoin Mecca?

The largest underground shopping center in South Korea called Goto Mall recently announced that it will start accepting bitcoin. Beginning mid-December, shoppers can pay with bitcoin at the mall's 620 stores, according to local publications.

Travel guide website *Travel Vui* describes:

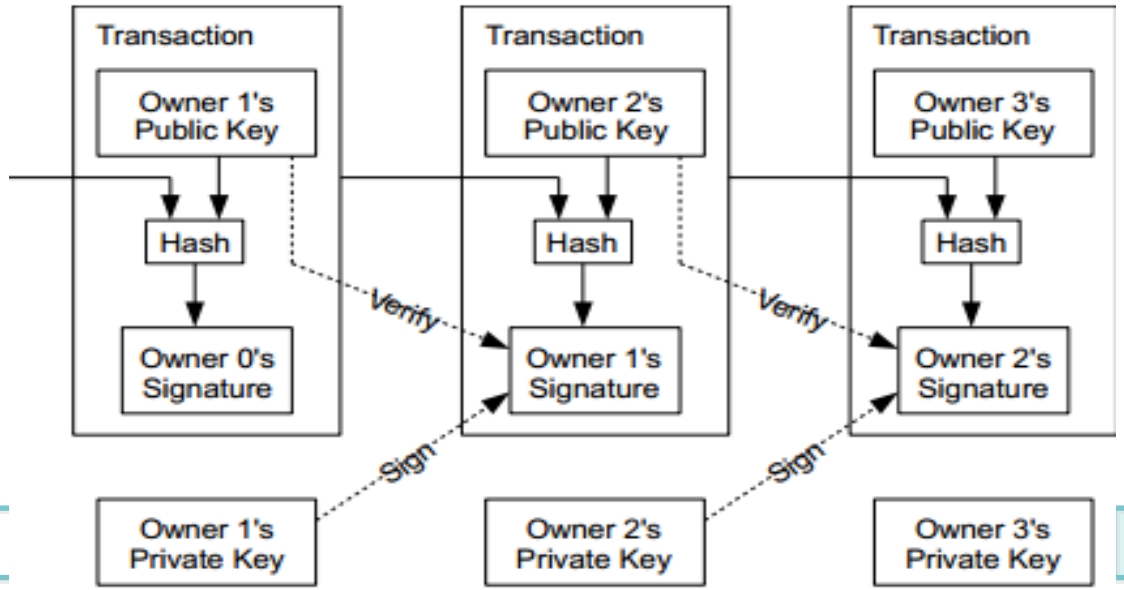
What is Bitcoin?

- Decentralized, crypto-currency described by Satoshi Nakamoto in 2008 and introduced as open-source software in 2009

- Bitcoin has several characteristics
  - peer-to-peer protocol
  - decentralized production of Bitcoins by the proof of work(PoW) protocol
  - prevention of double spending by transparent transactions
  - pseudo-anonymity and personal privacy protection

What is Blockchain?

- Blockchain is growing list of records, called blocks, which is linked and secured using cryptography
- Each block contains hash as a link to a previous block, a timestamp and transaction data
- Once recorded, the data in block cannot be altered without the alteration of all subsequent blocks
- In Bitcoin protocol, each block is mined on average every 10 minutes



Anonymity of Bitcoin

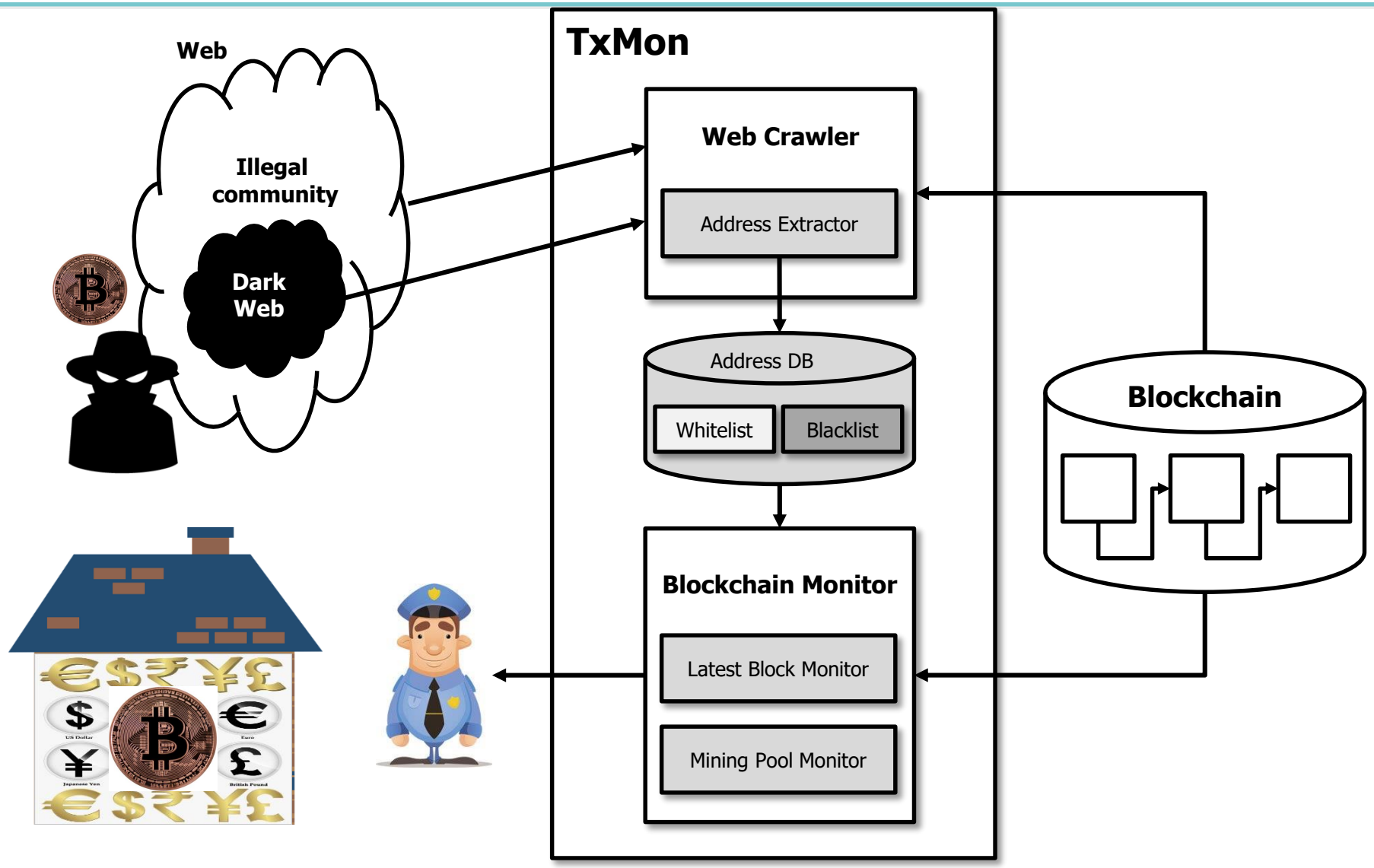
- Anonymity
  - Address and transaction cannot be mapped to the real identity
  - Transaction is spread radially, user's IP address will not be exposed
- Weakness
  - Authentication helps bitcoin service providers to find addresses
  - Address exposed on the internet can be related to its owner
  - Chain of transaction is transparent and traceable

Assumption & Goal

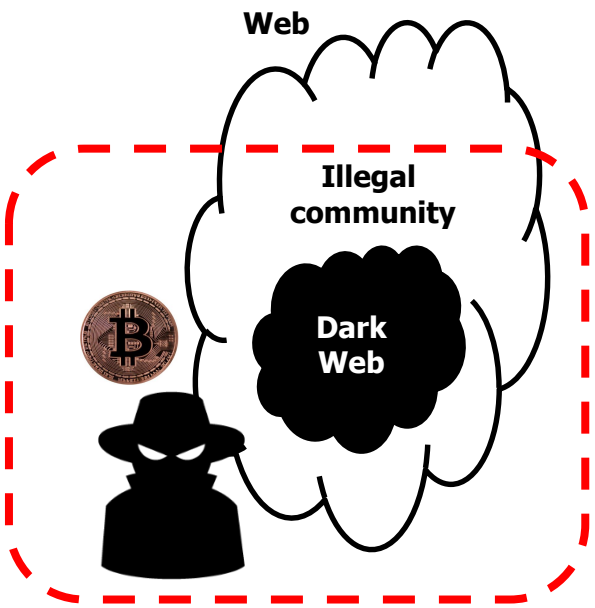
- Assumption
  - Bitcoin addresses in open place denoted as *whitelist* are easily finded by Police
    - We can easily get *whitelist as web surfing "Youtube"*

      ex) private bitcoin exchange, Paris-Baguette shops
  - Bitcoin addresses suspected of illegal transactions denoted as *blacklist* can be identified by police through investigation or web surfing
- Goal
  - Make the tool for monitoring illegal bitcoin transaction
    - Web crawl bitcoin address for monitoring blacklist and whitelist
    - Monitor all transaction from latest block
    - Watch unconfirmed transaction from mining pool in real-time

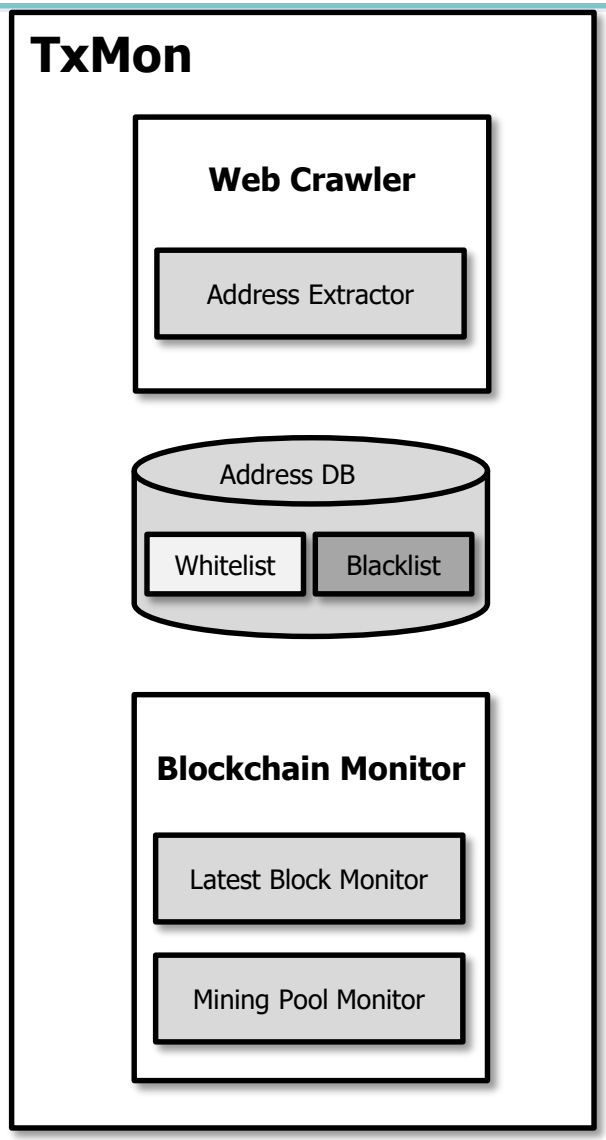
Design

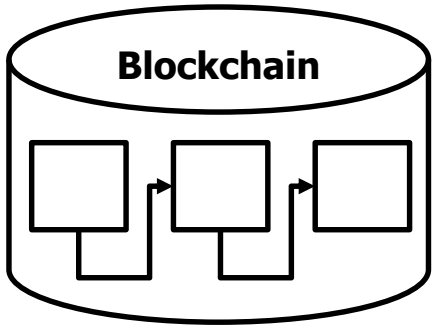

Web
Illegal community
Dark Web
TxMon
Web Crawler
Address Extractor
Address DB
Whitelist
Blacklist
Blockchain
Blockchain Monitor
Latest Block Monitor
Mining Pool Monitor

Scenario (1/5)

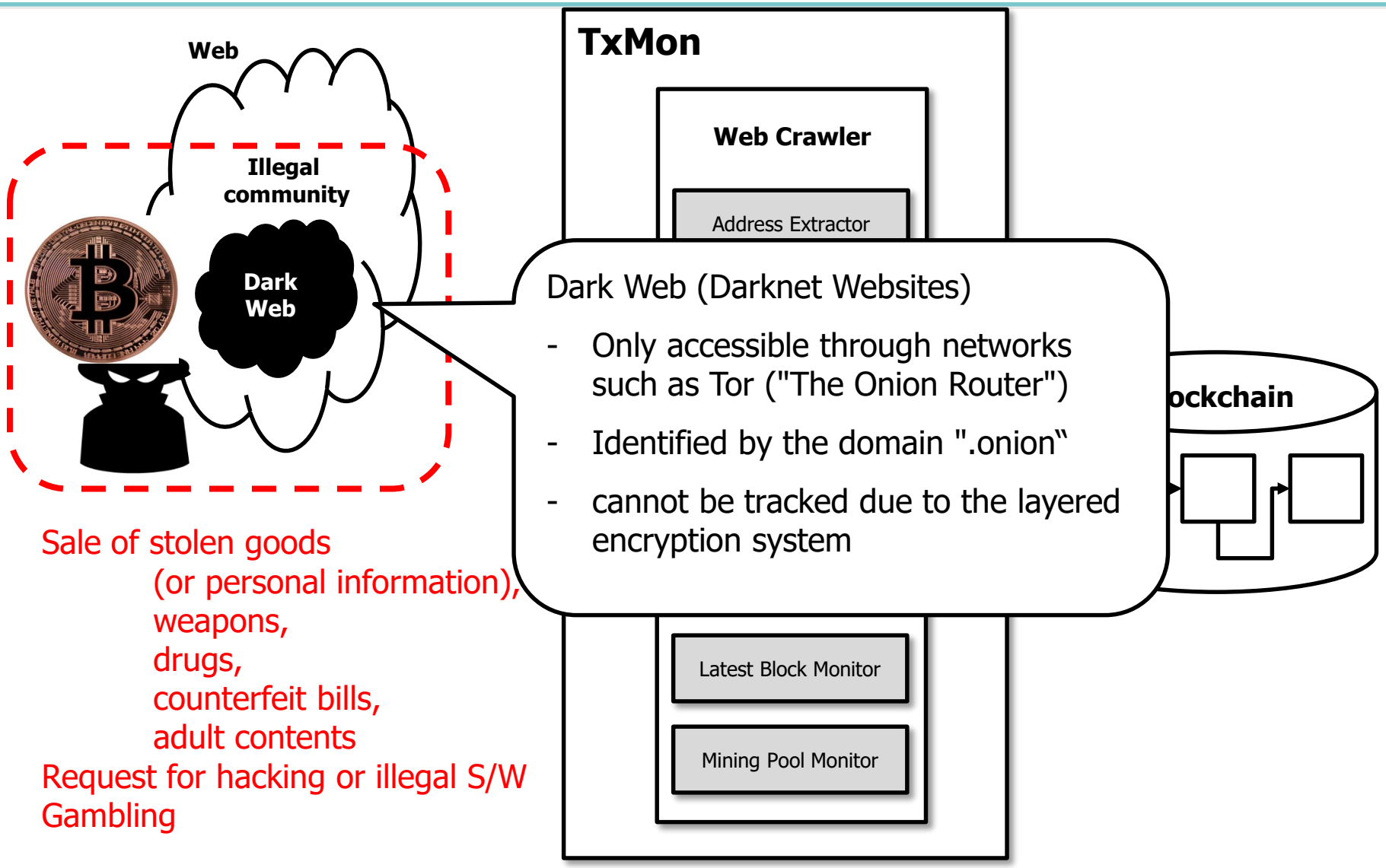


Sale of stolen goods
(or personal information),
weapons,
drugs,
counterfeit bills,
adult contents
Request for hacking or illegal S/W
Gambling

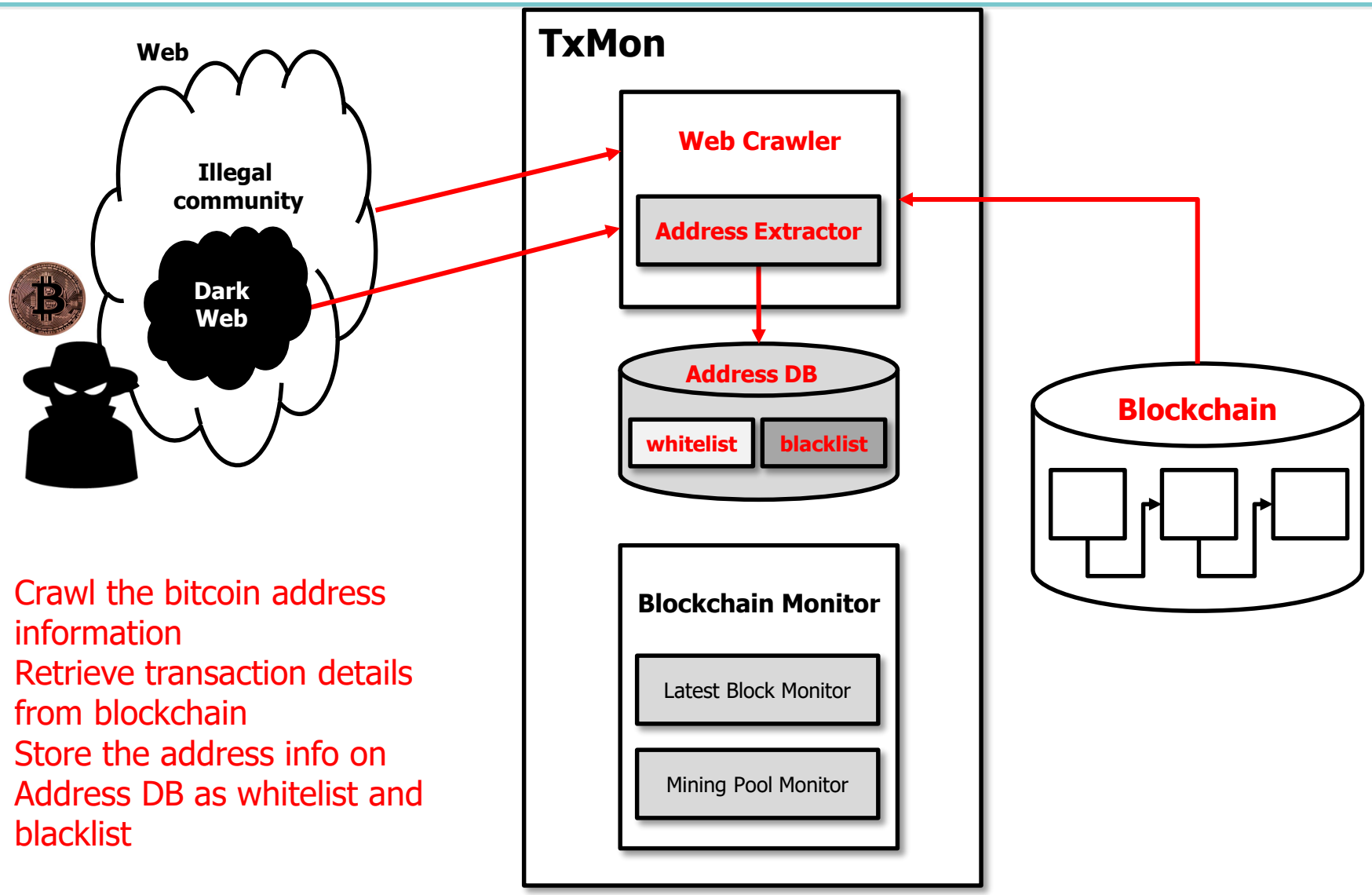




Scenario (1/5)

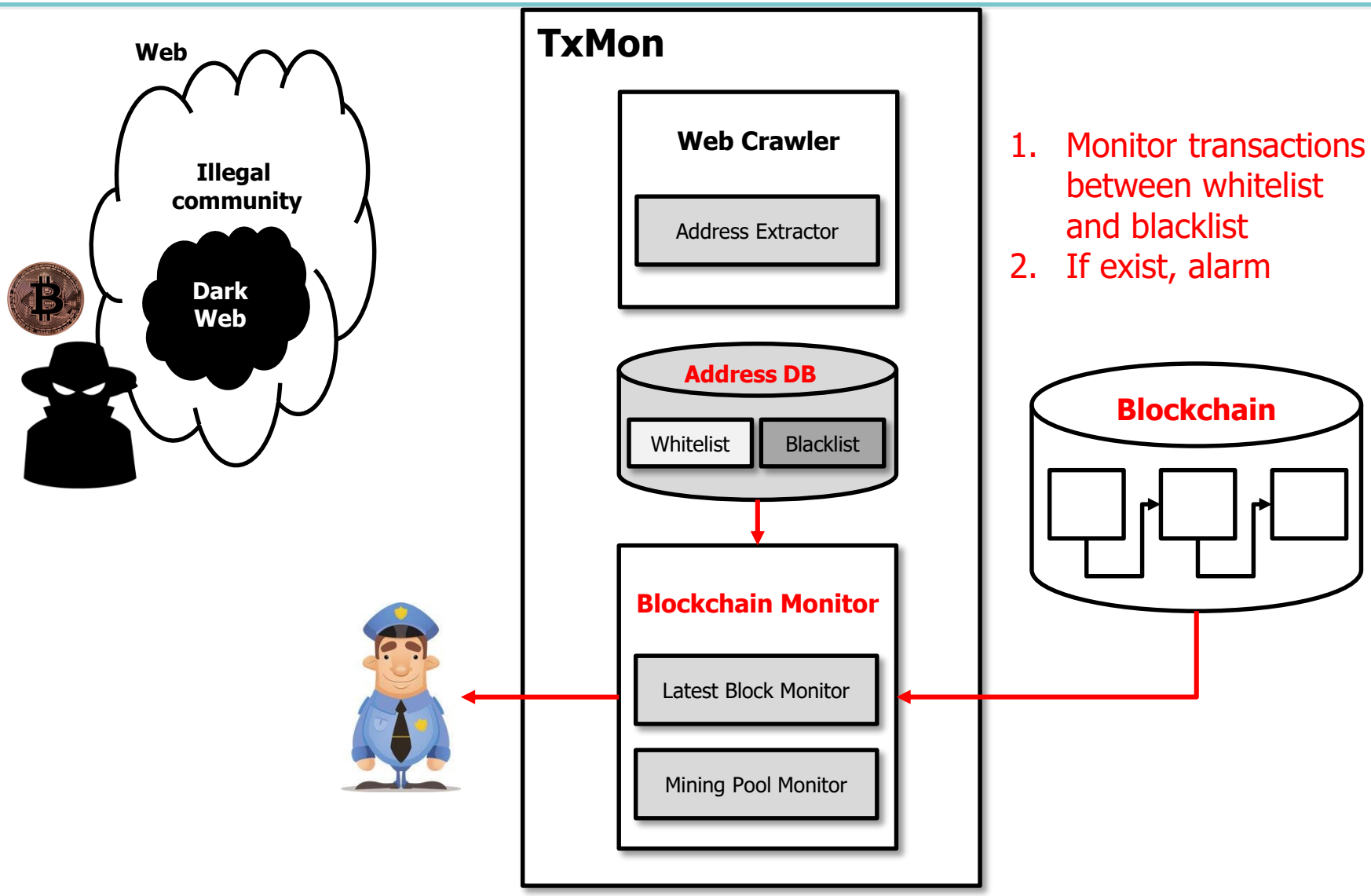

Web
Illegal community
Dark Web
TxMon
Web Crawler
Address Extractor
Dark Web (Darknet Websites)
- Only accessible through networks such as Tor ("The Onion Router")
- Identified by the domain ".onion"
- cannot be tracked due to the layered encryption system
ockchain
Latest Block Monitor
Mining Pool Monitor
Sale of stolen goods
(or personal information),
weapons,
drugs,
counterfeit bills,
adult contents
Request for hacking or illegal S/W
Gambling

Scenario (2/5)



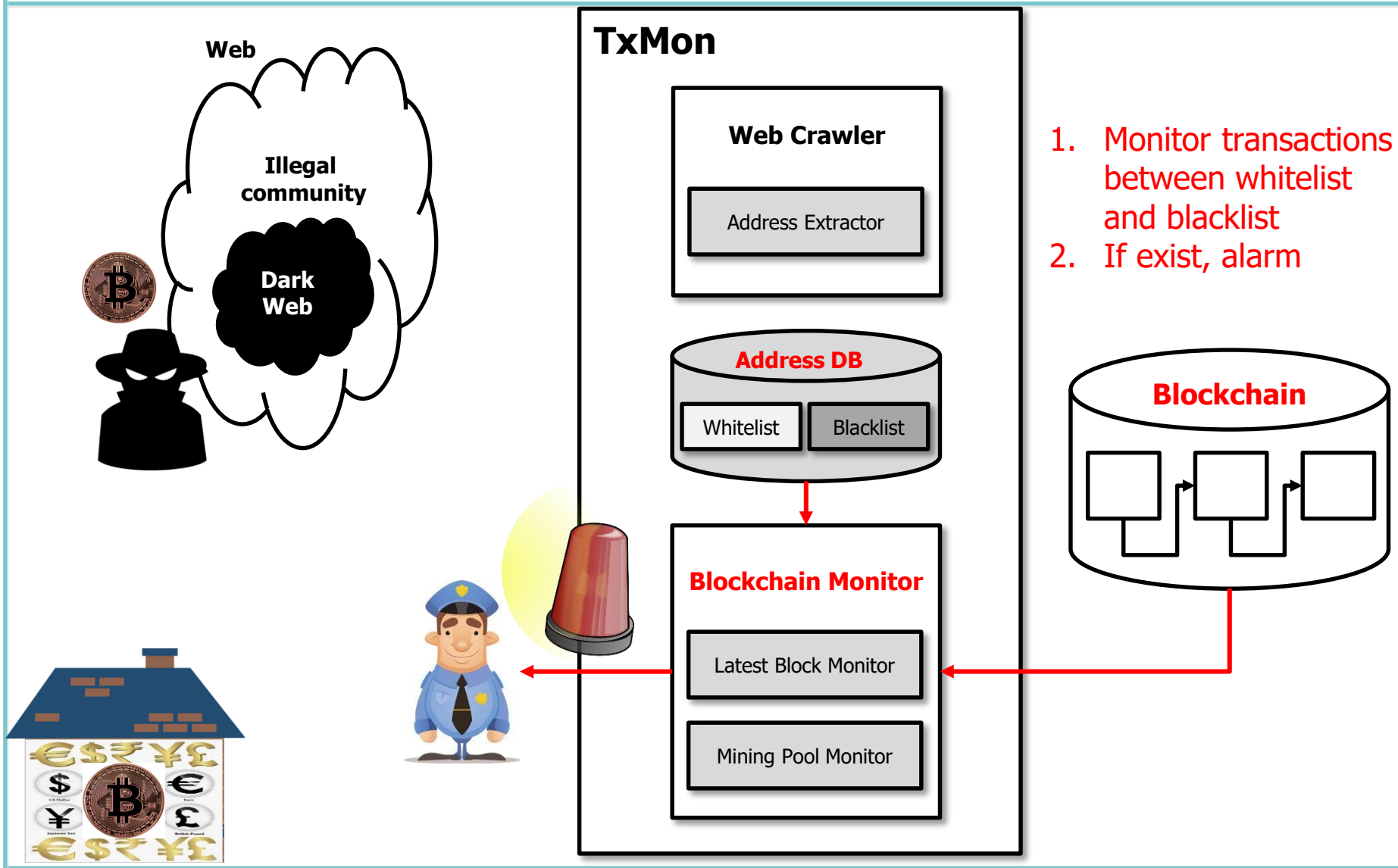
1. Crawl the bitcoin address information
2. Retrieve transaction details from blockchain
3. Store the address info on Address DB as whitelist and blacklist

Scenario (3/5)



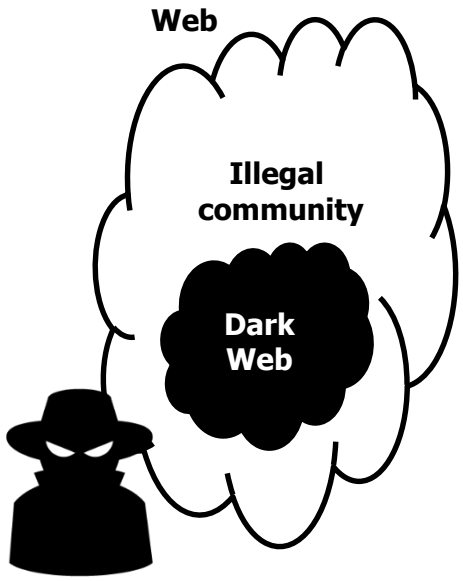
1. Monitor transactions between whitelist and blacklist
2. If exist, alarm

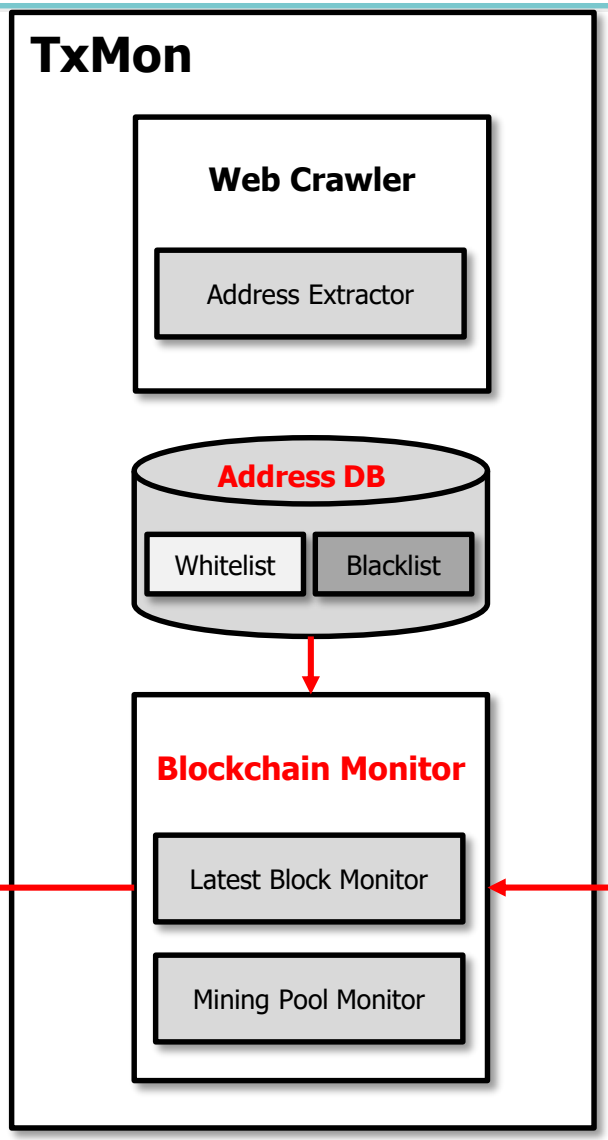
Scenario (4/5)

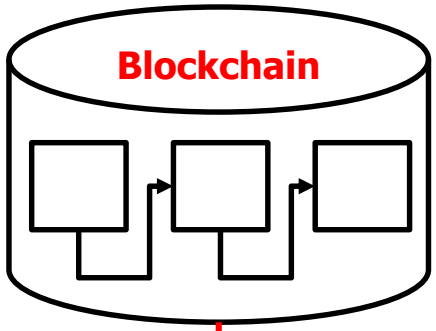


1. Monitor transactions between whitelist and blacklist
2. If exist, alarm

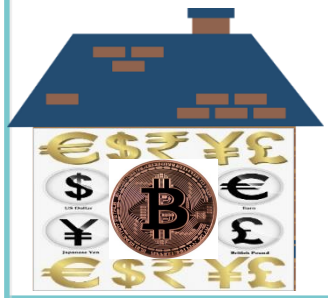
Scenario (5/5)



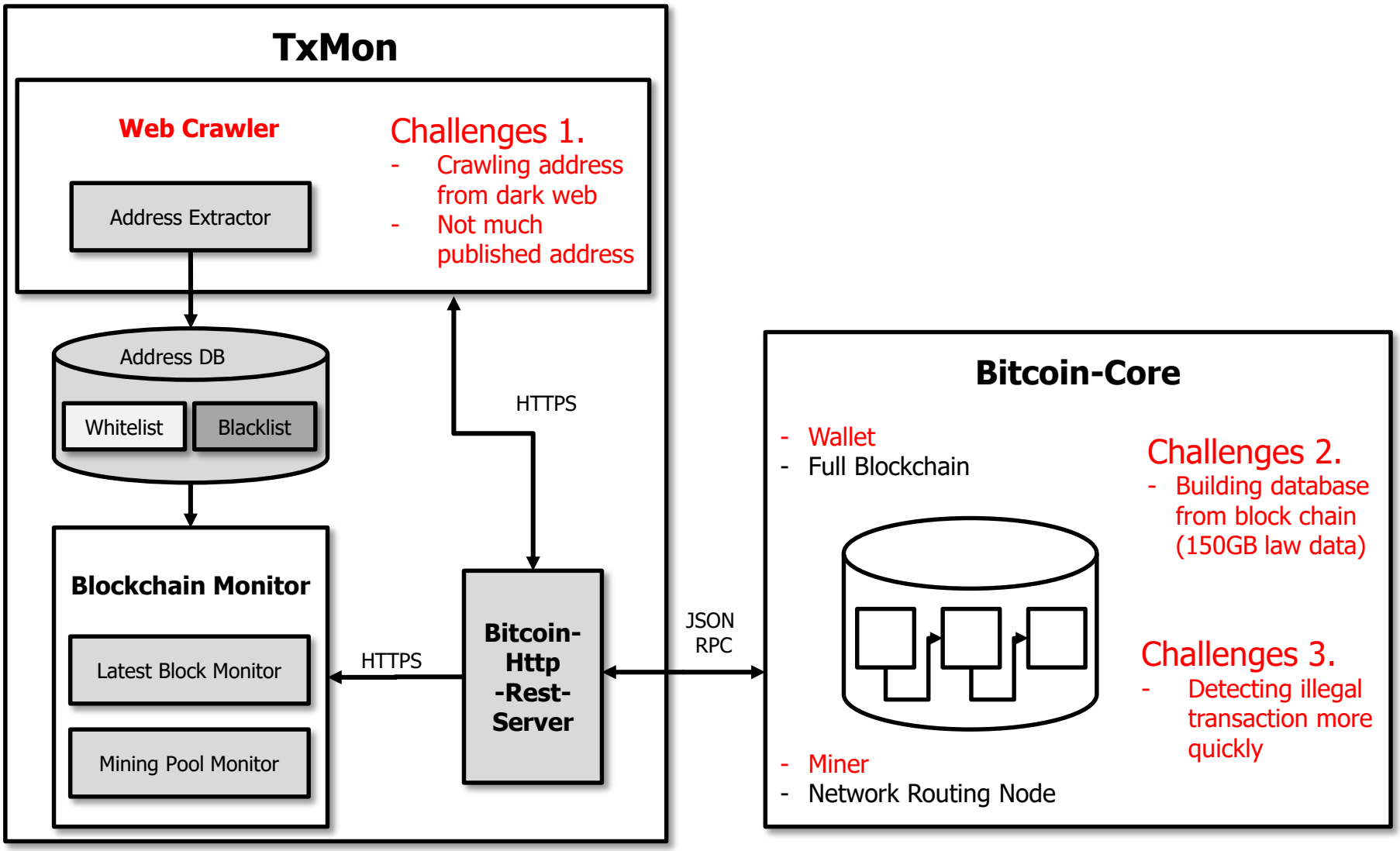




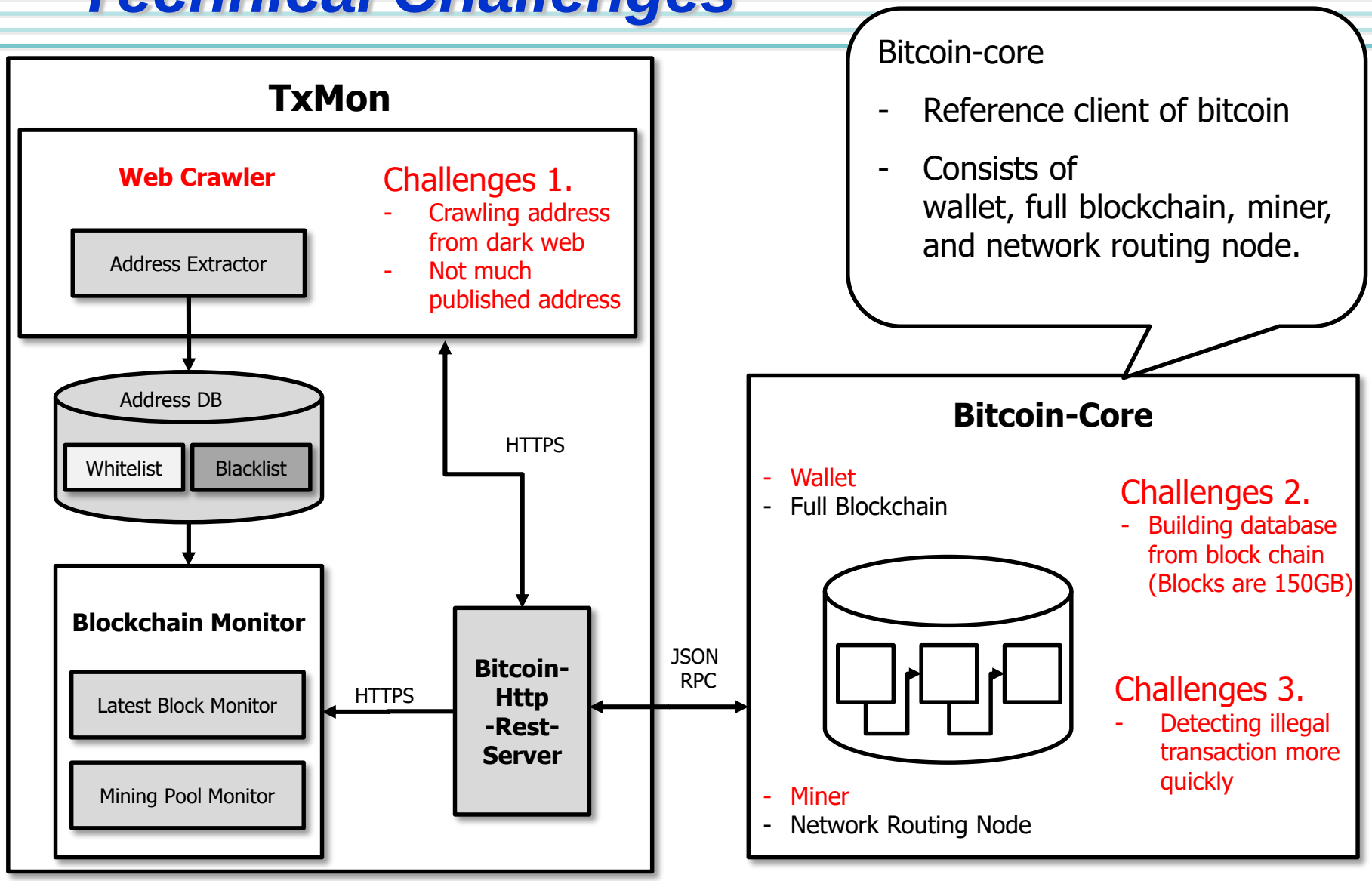
1. Monitor transactions between whitelist and blacklist
2. If exist, alarm



Technical Challenges

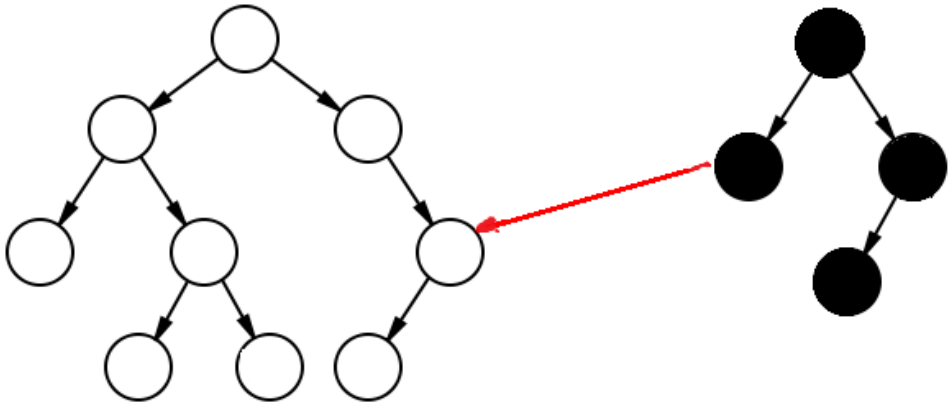


Technical Challenges



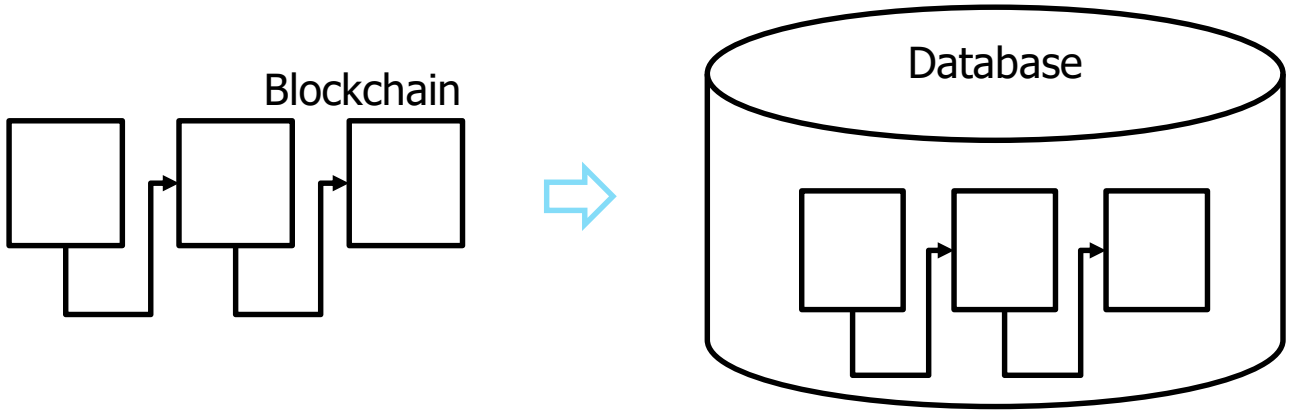
Overcoming Challenges (1/3)

- Web Crawling
  - Bitcoin address is confidential
    e.g. Dark website checks the identity on facebook.
  - The published bitcoin address is not much
- Used the manually-found bitcoin address, and expanded
- (Addresses, Transactions) -> tree data structure
  - Addresses -> nodes
  - Transactions -> edges



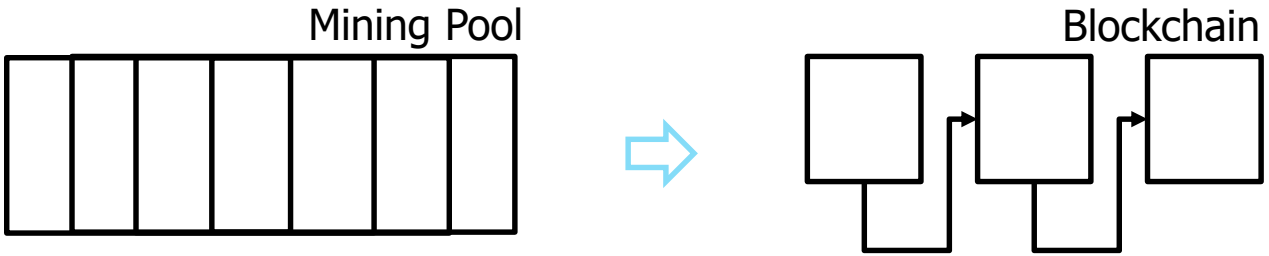
Overcoming Challenges (2/3)

- Building database(DB) from block chain
  - Blockchain is not DBMS but raw data
  - Additional meta-data(DB) must be created for blockchain
  - Need to manage large DB with a lot of operational know-how
- We used Open API Service (https://blockchain.info)
  - Easy to implement
  - But, limited number of requests to send a query

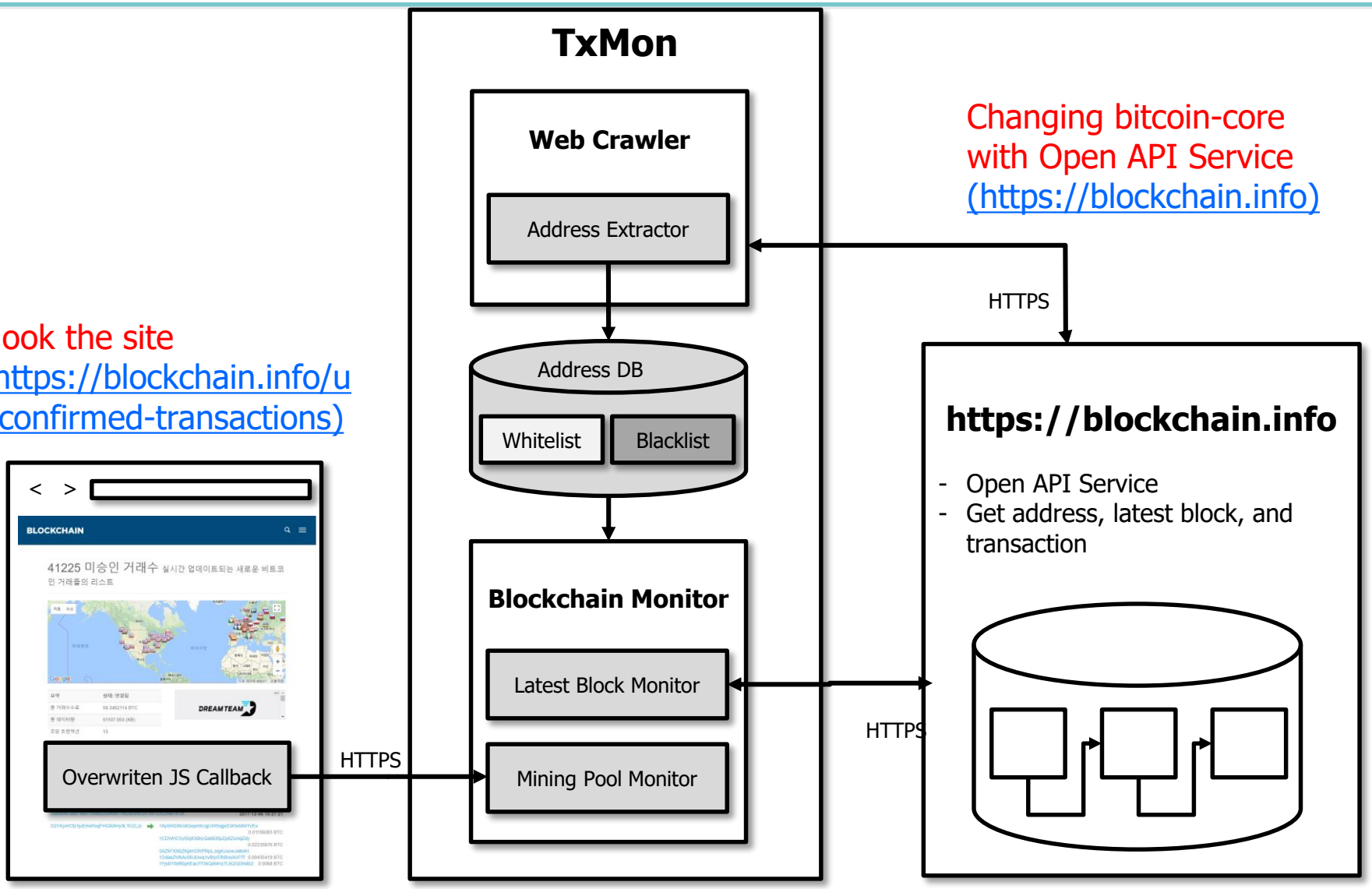


Overcoming Challenges (3/3)

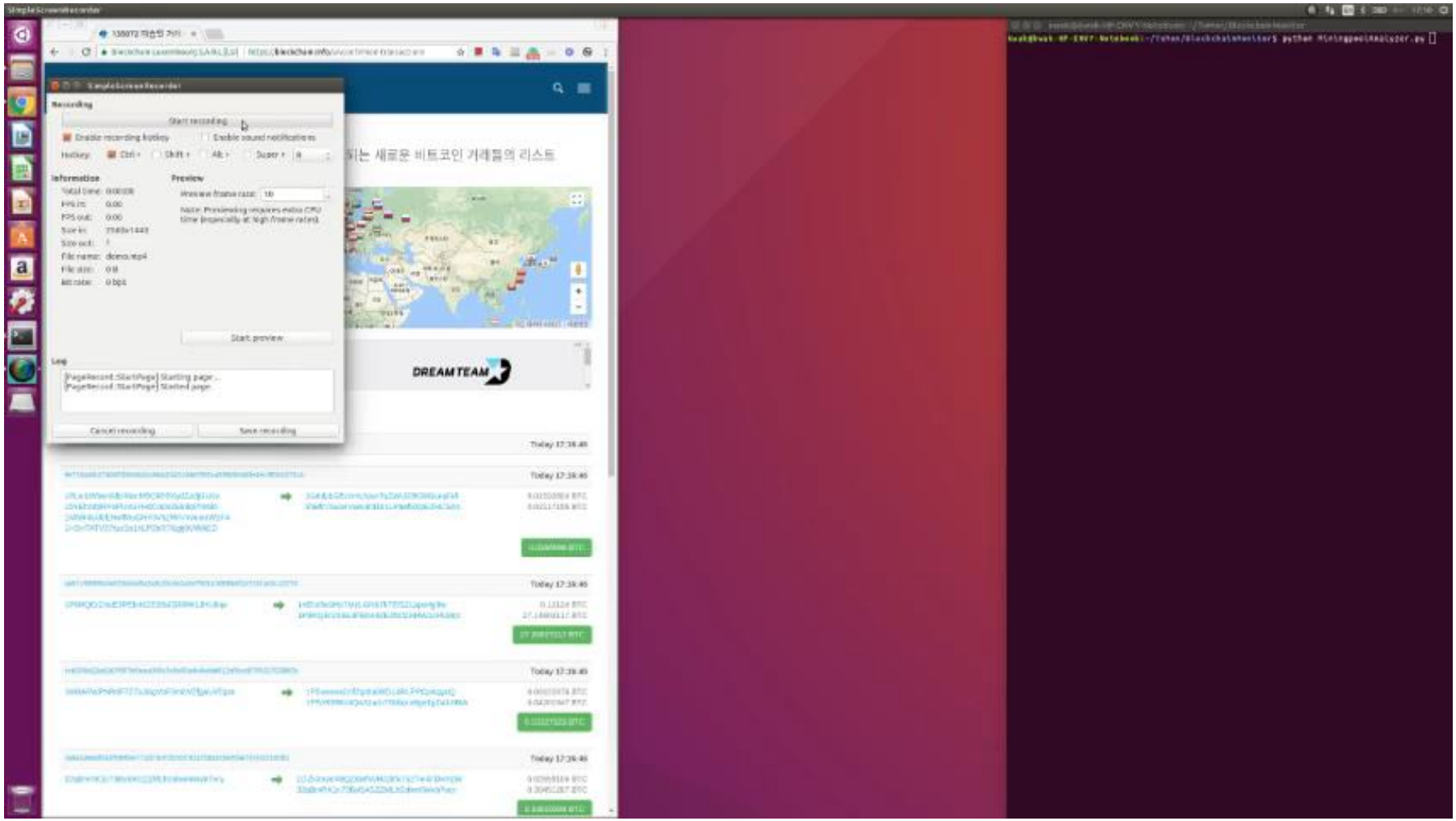
- Detecting an illegal transaction more quickly
  - It takes 10 minutes until being included in the blockchain
  - Unconfirmed transaction waits in the mining pool
- So, if monitor the mining pool, we can get a faster warning
  - But limited to send many requests
- Hook the site (https://blockchain.info/unconfirmed-transactions)
  - Overwrite the JavaScript callback function
  - Disable CSP (Contents Security Policy)



Implementation



Demo



Basic Dataset

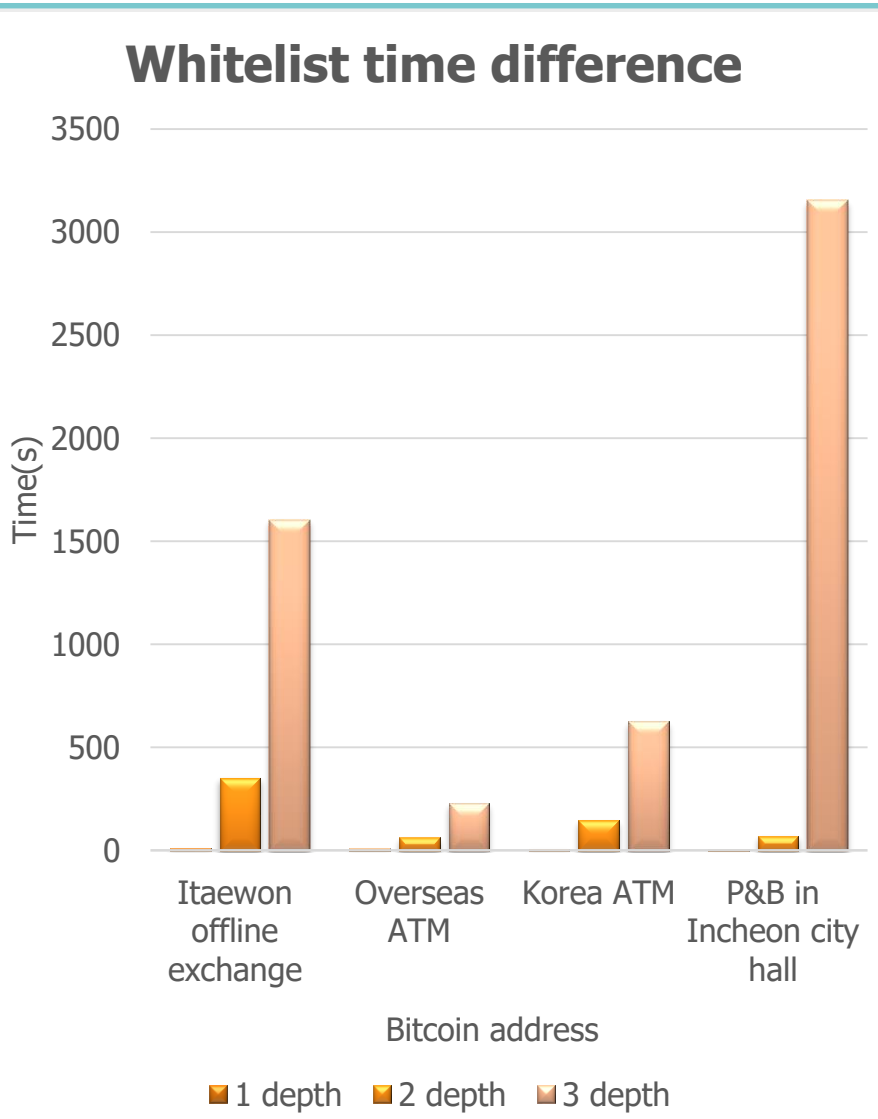
- Whitelist

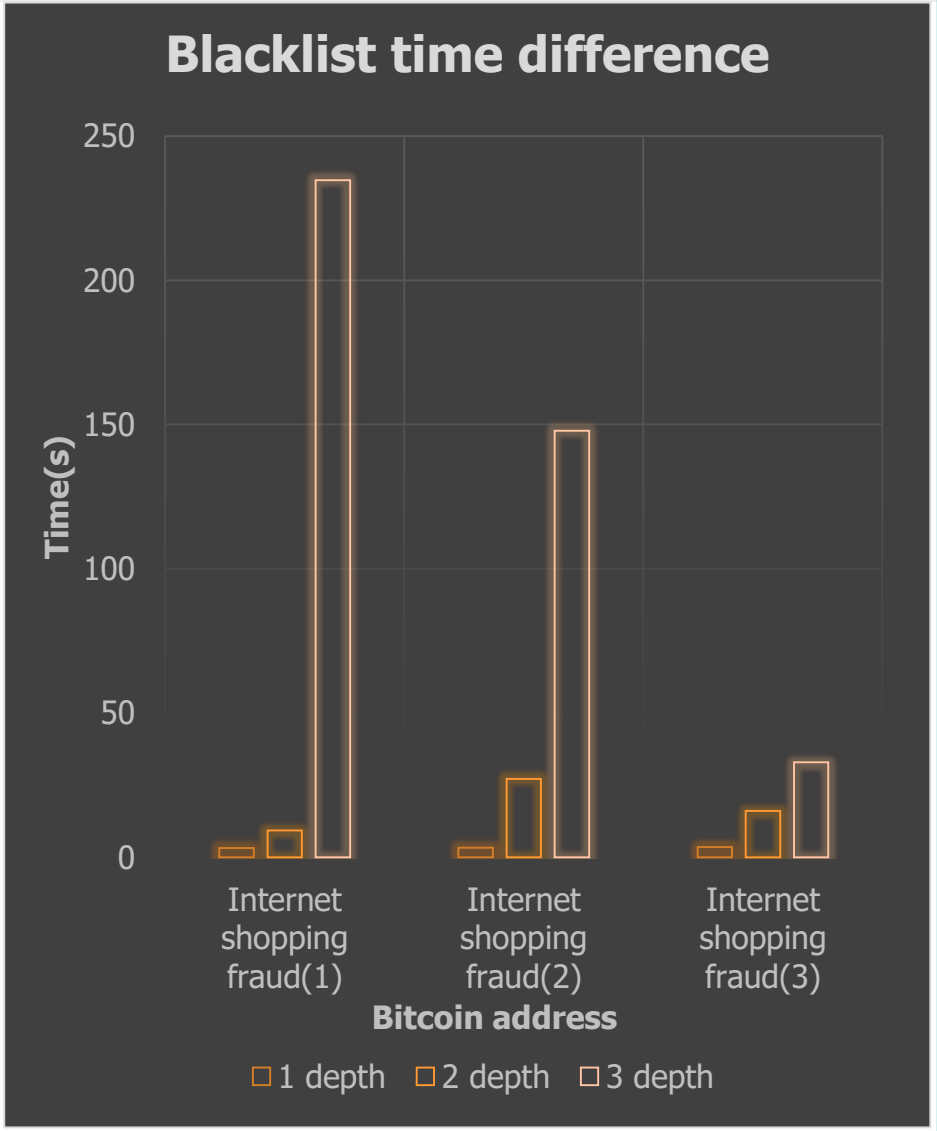
Place	total received	Method
Itawon offline exchange shop	81.25BTC	Youtube
Overseas ATM	1778.6BTC	
ATM in Korea	12.2BTC	
P&B shop in Incheon	0.85BTC	

- Blacklist

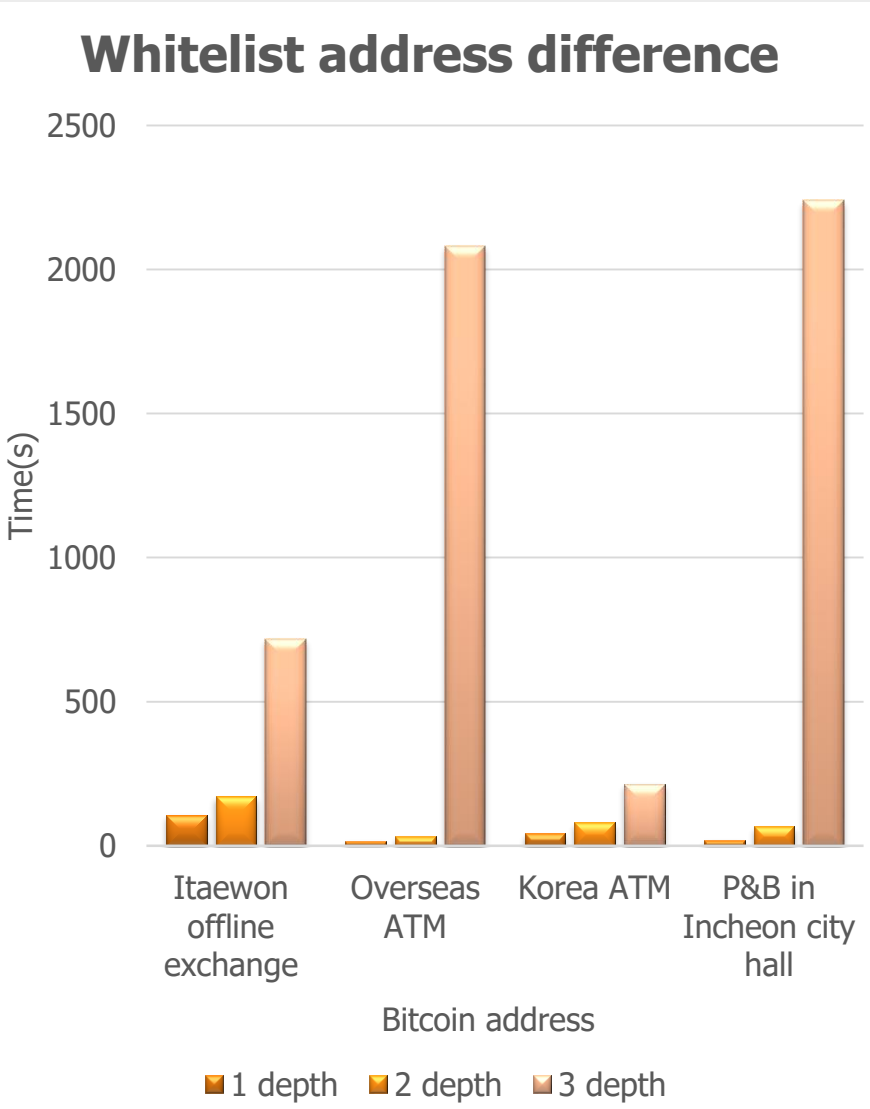
Place	total received	Method
Internet shopping fraud	81.25BTC	By Police
Clothing sales fraud	1778.6BTC	
I-phone sales fraud	12.2BTC	

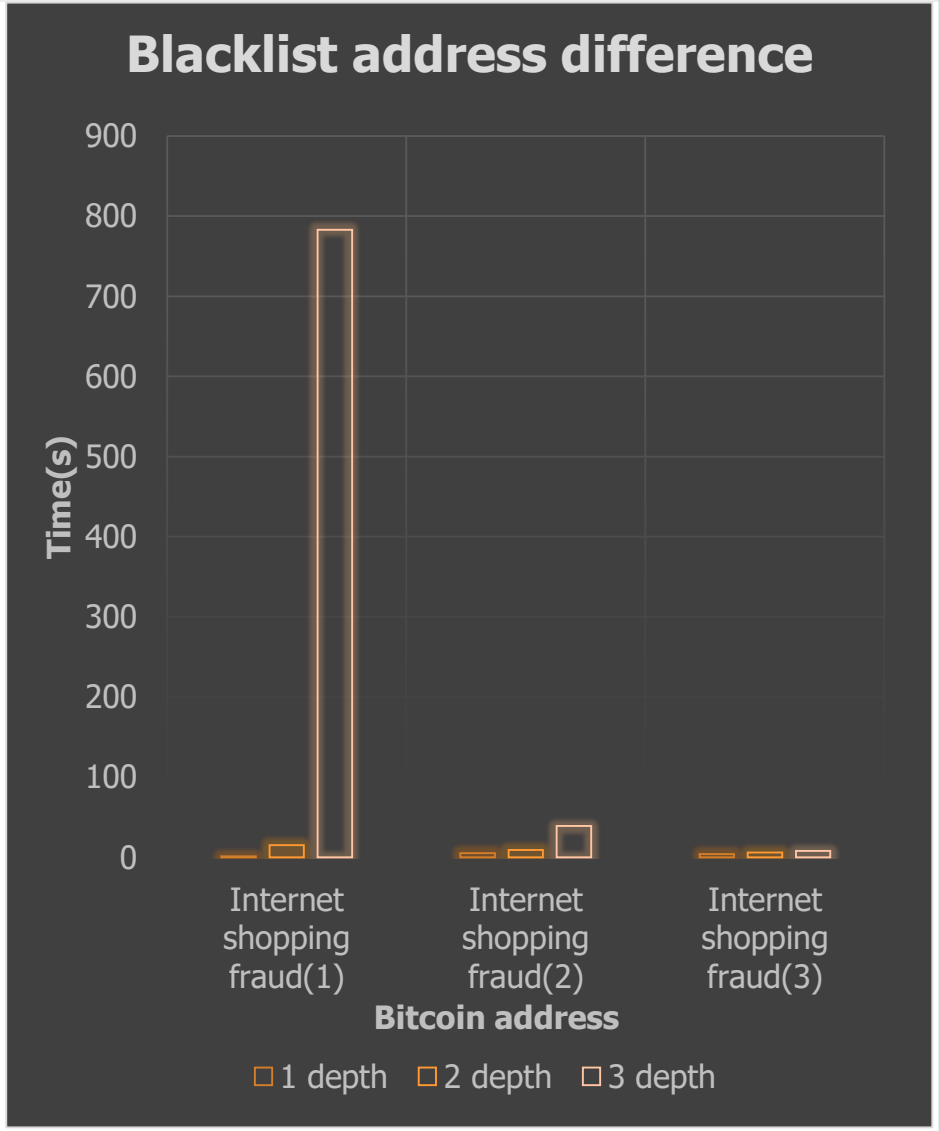
Evaluation : web crawl bitcoin address (1)



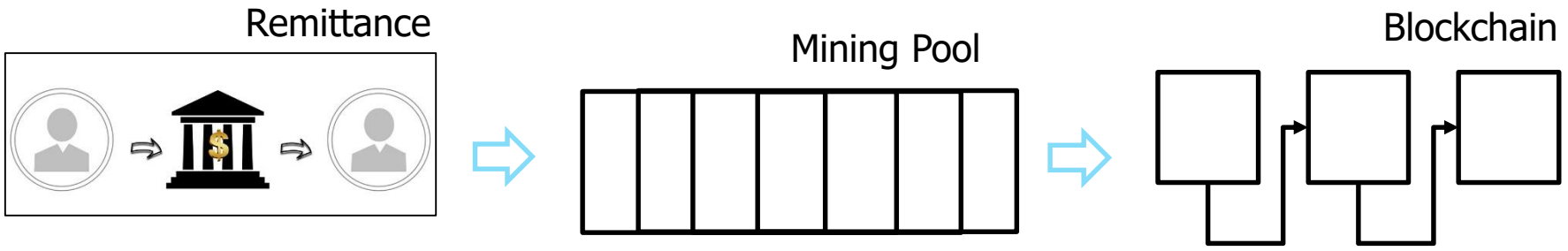


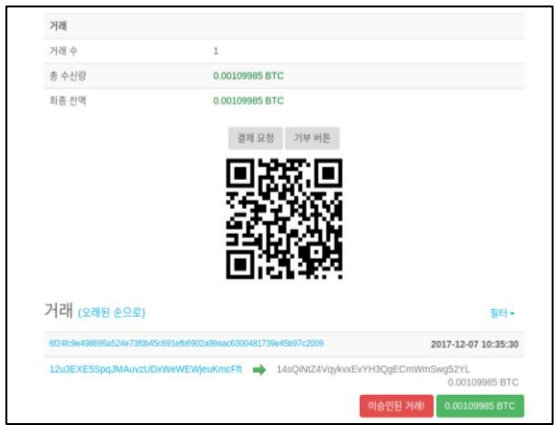
Evaluation : web crawl bitcoin address (2)

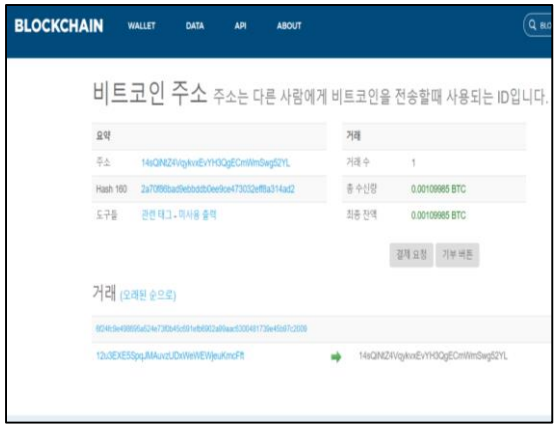


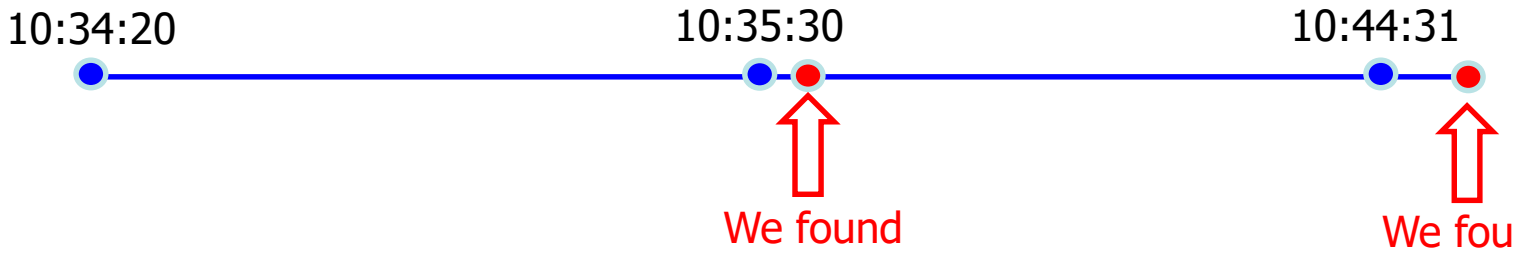


Evaluation : Monitor mining pool & latest block









Related Work : ATC

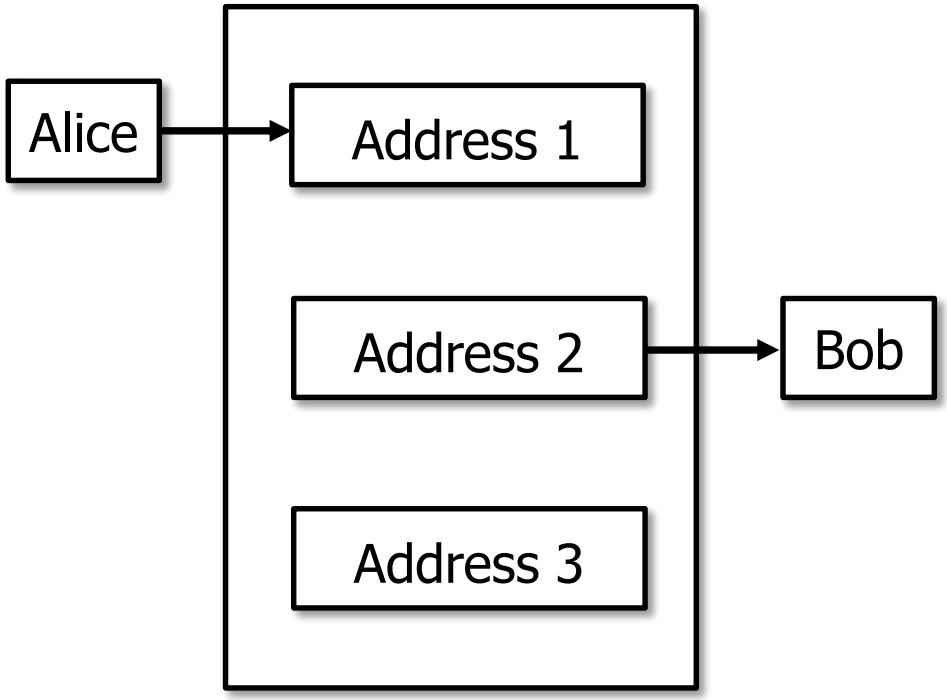
- Analysis of Transaction Chain (ATC)
  - Obtain transactions from public blockchain data to classify Bitcoin addresses based on the weakness of Bitcoin anonymity
  - And to relate Bitcoin addresses to personal
- Limitation of ATC
  - Coin-mixing obfuscates the transaction chain, and separate the corresponding relationship between the input and output of a bitcoin transaction and hide the amount of transaction

Related Work : Coin mixing against ATC

1. User send bitcoins to the addresses of Coin mixer owns

2. Payment has been confirmed, the amount of bitcoins is transferred to the destination address using a different

3. Alice and Bob's transaction is not linked



Related Work : Difference from ATC

- Related works are considering anonymity and deanonymity of bitcoin itself
- When using coin-mixing, ATC has limitation to track transaction because of no relationship between transaction
- Our perspective is when bitcoin is used in trackable or open place, we can monitor illegal bitcoin transaction
  - Even though coin-mixing is used, Our tool can extract all bitcoin addresses and investigate them if they have criminal charges
  - In addition, using coin mixing can be considered to be highly relevant to crime

Limitation & Discussion

- More difficult to crawl information from the dark web or illegal community
- Limited requests to Blockchain.info
  - Needs continuous web crawling to extract addresses at deeper depths

- Using blockchain technology does not guarantee safety
  - The blockchain technology does not replace the existing DBMS, but rather requires a higher level DBMS technique.

Conclusion

- Explored several aspects related to the blockchain and web app
- Propose a tool to monitor illegal bitcoin transaction
  - Crawling bitcoin address
  - Monitoring all transaction from latest block
  - Quickly finding illegal transaction by checking mining pool

Q & A

Reference

[1] RS Portnoff, et al. “Tools for Automated Analysis of Cybercriminal Markets.” WWW2017 (2017)

[2] QC ShenTu, et al. "Research on Anonymization and De-anonymization in the Bitcoin System." CoRR, vol. abs/1510.07782, 2015. [Online]. Available: http://arxiv.org/abs/1510.07782

[3] Malte Möser. "Anonymity of Bitcoin Transactions." Münster bitcoin conference, 2013 (2013)

[4] 정재원"비트코인 악용 범죄 수사에 대한 제도 및 기술적 문제점과 해결방안에 대한 연구." 서울대학교 석사학위논문 (2016)