Research on privacy and traceability of emerging blockchain based financial transactions

20th March, 2019

Financial Services Agency

MITSUBISHI RESEARCH INSTITUTE, INC.
Social ICT Innovation Division

Agenda

1. Background

1.1 Current status of AML/CFT concerning crypto-assets

1.2 Research objectives

2. Current situation of crypto-assets

2.1 Expansion of the crypto-asset economy

2.2 Expansion of crypto-crime

2.3 Crypto-laundering

3. Investigation on anonymization technology for crypto-asset transactions

3.1 Overview of assessed technologies

3.1.1 Overview of technologies

3.1.2 Examples of anonymization technology

3.1.3 Examples of de-anonymization technology

3.1.4 Examples of issues resolved through this research

3.2 Application layer (Blockchain)

3.2.1 Blockchain anonymization technologies

3.2.2 Blockchain de-anonymization technologies

Agenda

3. Investigation on anonymization technology for crypto-asset transactions (continued)

3.3 P2P layer/Internet layer

3.3.1 P2P layer/Internet layer anonymization technologies

3.3.2 P2P layer/Internet layer de-anonymization technologies

3.4 Physical layer

3.4.1 Physical layer anonymization technologies

3.4.2 Physical layer de-anonymization technologies

4. Experiments

4.1 List of experimental scenarios

4.2 Crypto-laundering using lightning networks

4.3 Crypto-laundering using mixing services

4.4 Countermeasures using risk scoring tools

5. Conclusions

5.1 Issues that have been identified through qualitative and quantitative assessments

5.2 Recommended countermeasures

Glossary

Term	Definition
AML/CFT	Anti-Money Laundering/Combating the Financing of Terrorism
DApps	Decentralized Applications Applications deployed on a blockchain network
DeFi	Decentralized Finance Financial services offered by applications deployed on a blockchain network
DEX	Decentralized Exchange
FATF	Financial Action Task Force
FATF non-compliant countries	Jurisdictions that are not fully compliant with FATF recommendations. * This term is only used in this report
KYC	Know Your Customer
Off-chain	Means other than blockchain (e.g., through a dedicated server or mail/SMS)
Custody Risk	Risk of loss of crypto-assets as a result of the failure of a private key custodian: bankruptcy, hacking, negligence, misuse, fraud, improper management etc.
Crypto-laundering	Money laundering using crypto-assets
Security	Protection from or resilience against potential harm caused by others
Dark Market	A marketplace on the dark web (often using Tor Hidden Services)
Fungibility	The property of goods or assets whose individual units are interchangeable regardless of the transaction contents and transfer routes. (The representative example is currency: 10,000 yen is equivalent to any other 10,000 yen.)

Glossary

Term	Definition
Privacy	The right or ability to disclose one's personal information selectively
Re-Identification De-anonymization	Identifying an anonymous subject by combining it with other data sources. * In this report, these terms are regarded as synonymous with tracking
Censorship Resistance	Resilience against forcible suppression by a public authority
Anonymity	A subject is not distinguishable within a set of subjects
Anonymity Set	A set of all possible subjects where every subject cannot be identified (The anonymity of a subject is where the subject cannot be identifiable within an anonymity set.)
Pseudonymity	An identifier of a subject other than the subject's real identity
Confidentiality	The state where information is not disclosed to unauthorized entities
Unlinkability	The state where the relationship of two or more items cannot sufficiently be distinguished
Untraceability	The state where the trace of the object cannot be followed
Undetectability	The state where the existence of an item cannot sufficiently be distinguished
Unobservability	The state that includes both undetectability and anonymity

Acknowledgement & Disclaimer

Acknowledgement

- This research was conducted with the expertise of Dr. Tetsutaro Uehara (Ritsumeikan University) and Dr. Shin'ichiro Matsuo (Georgetown University).

Disclaimer

- The views and opinions expressed in this report do not necessarily reflect the official policy or position of JFSA.

- The contents other than past or present facts described in this report are based on the information available at the time of writing. Therefore, it must be noted that actual trends may fluctuate due to various factors.

1. Background

1.1 Current status of AML/CFT concerning crypto-assets
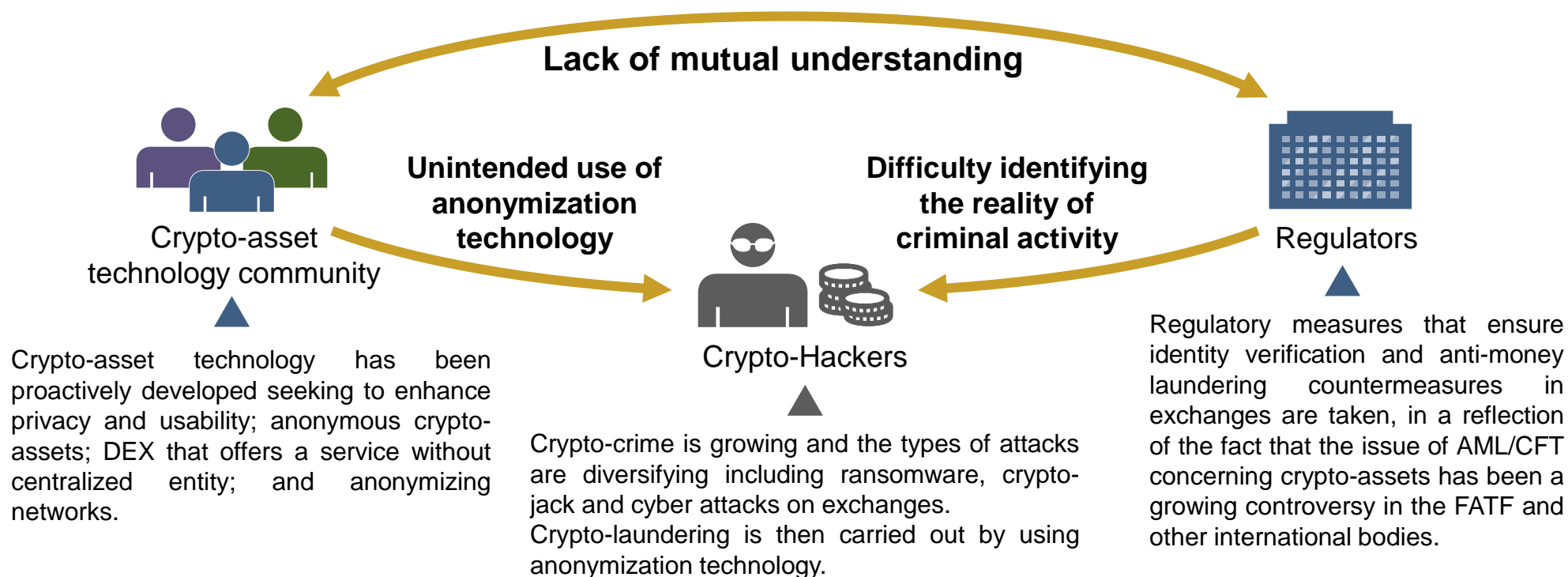
1.2 Research objectives

Summary of this chapter

- The risk of crypto-crime is increasing with the expansion of crypto-asset markets but, on the other hand, the rapid development of privacy protection technologies makes it difficult to identify and trace crypto-asset transactions. Thus, it is becoming more difficult for regulators to prevent money laundering and the financing of terrorism using crypto-assets.

- Crypto-assets are processed electronically and in a decentralized manner. This prevents links to individuals and their information in the real world and real-life criminal activity. Furthermore, crypto-asset anonymization technologies have been proactively developed seeking to enhance privacy and usability.

- The expansion of crypto-asset trading and the progress of crypto-asset technologies will increase the risk of crypto-laundering. Such concerns have grown in recent years as these risks have become a reality.

- The development of risks like this in the crypto-asset market are likely to prevent the realization of a safe, fair and reliable crypto-asset ecosystem with customer protection and the moderation of crypto-asset trading etc.

- Against this backdrop, this research aims at assessing the current status of crypto-asset anonymization technologies in order to lay down solid foundations for future policymaking.

1.1 Current status of AML/CFT concerning crypto-assets

The risk of crypto-crime is increasing with the expansion of crypto-asset markets. However, the rapid development of privacy protection technologies is making it difficult to identify and trace crypto-asset transactions so it is becoming more difficult for regulators to prevent money laundering and financing of terrorism using crypto-assets.
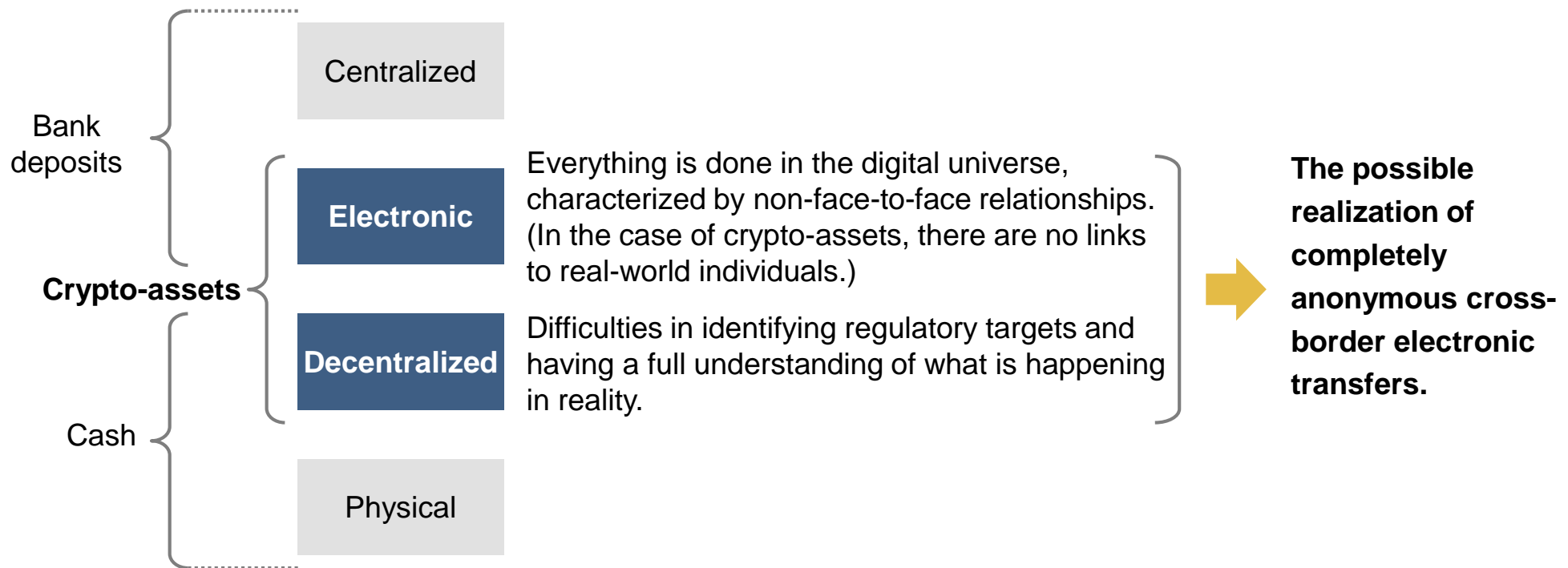
Major stakeholders surrounding the current status of AML/CFT concerning crypto-assets

Lack of mutual understanding

Unintended use of anonymization technology

Difficulty identifying the reality of criminal activity

Crypto-asset technology community

Crypto-Hackers

Regulators

Crypto-asset technology has been proactively developed seeking to enhance privacy and usability; anonymous crypto-assets; DEX that offers a service without centralized entity; and anonymizing networks.

Crypto-crime is growing and the types of attacks are diversifying including ransomware, crypto-jack and cyber attacks on exchanges.
Crypto-laundering is then carried out by using anonymization technology.

Regulatory measures that ensure identity verification and anti-money laundering countermeasures in exchanges are taken, in a reflection of the fact that the issue of AML/CFT concerning crypto-assets has been a growing controversy in the FATF and other international bodies.

1.1 Current status of AML/CFT concerning crypto-assets – Characteristics of crypto-assets

Crypto-assets are processed electronically and in a decentralized manner, which partially combines the nature of (1) electronically processed and centralized bank deposits and (2) cash that is processed physically and in a decentralized manner. Based on these characteristics, there is a risk that crypto-assets will not allow links to individuals in the real world and identifying the reality of criminal activity.

Characteristics of crypto-assets compared to fiat currencies

Bank deposits

Centralized

Crypto-assets

Electronic — Everything is done in the digital universe, characterized by non-face-to-face relationships. (In the case of crypto-assets, there are no links to real-world individuals.)

Decentralized — Difficulties in identifying regulatory targets and having a full understanding of what is happening in reality.

Cash

Physical

The possible realization of completely anonymous cross-border electronic transfers.

1.1 Current status of AML/CFT concerning crypto-assets－Development trends

In addition to the characteristics of crypto-assets, various anonymization technologies are being actively developed and are being linked to ideas on securing fungibility (the property of goods or assets whose individual units are interchangeable regardless of the contents of the transaction and transfer route) or protecting privacy.

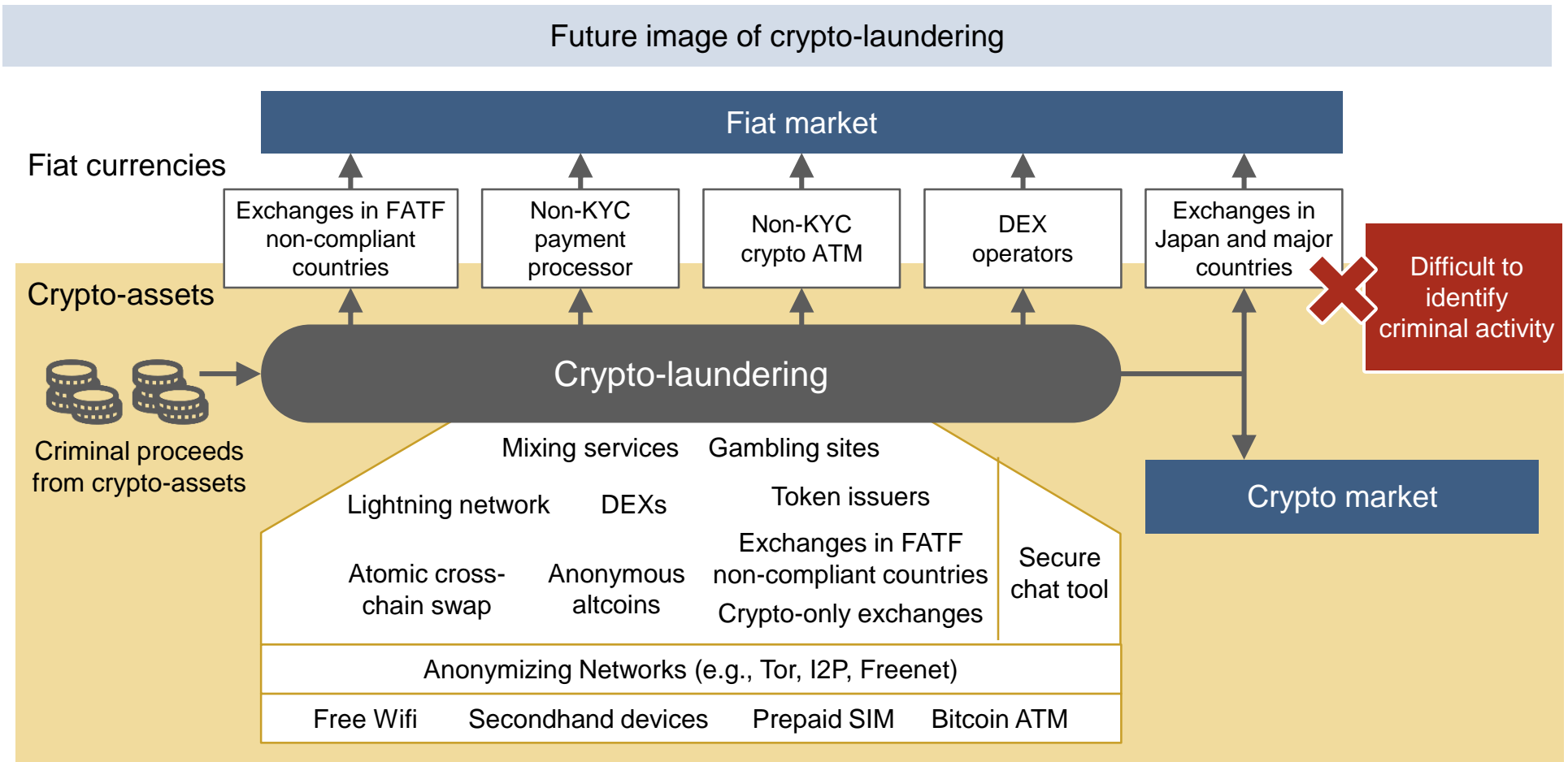## Relationship between fungibility of crypto-assets and crypto-laundering

Privacy

Security

Censorship resistance

Fungibility (interchangeability)

Liberalism

Technology

Anonymization technology

Anonymity

Untraceability Unlinkability Confidentiality
Pseudonymity Undetectability Unobservability

Blockchain technology

Autonomous Decentralization

Openness Borderless Trustless
Tamper-resistance High availability Technical-oriented

Crypto-laundering

Fungibility is an important asset as a currency, and there is a lot of effort being put into ensure that it exists in crypto-assets.

Since transfer routes could be made irrelevant by making transactions private, fungibility is being discussed within the crypto-asset technology community which in turn relates to other ideas such as privacy and security, as well as liberalism and censorship resistance.

On the other hand, there is a risk that a combination of anonymization technology and blockchain technology which will bring about fungibility could be used for crypto-crime and crypto-laundering.

1.1 Current status of AML/CFT concerning crypto-assets－Future trends

The expansion of crypto-asset trading and the progress of crypto-asset technology will increase the risks of crypto-laundering.

Future image of crypto-laundering

Fiat market

Fiat currencies

| Exchanges in FATF non-compliant countries | Non-KYC payment processor | Non-KYC crypto ATM | DEX operators | Exchanges in Japan and major countries |

Crypto-assets

Crypto-laundering

Difficult to identify criminal activity

Criminal proceeds from crypto-assets

Mixing services   Gambling sites

Lightning network   DEXs   Token issuers

Atomic cross-chain swap   Anonymous altcoins   Exchanges in FATF non-compliant countries   Secure chat tool

Crypto-only exchanges

Crypto market

Anonymizing Networks (e.g., Tor, I2P, Freenet)

Free Wifi   Secondhand devices   Prepaid SIM   Bitcoin ATM

1.2 Research Objectives

The number of players in the crypto-asset ecosystem is growing and the types of players are also diversifying. Under these circumstances, the ability to enforce the law will be weakened due to the difficulty of identifying and monitoring targets when anonymization technologies become widely available as autonomous distributed services. Such concerns have grown in recent years as these technologies become available.

Developments in anonymization technologies in the crypto-asset market are likely to prevent the realization of a safe, fair and reliable crypto-asset ecosystem with customer protection and the moderation of crypto-asset trading etc.

Against this backdrop, this research aims at assessing

the current status of crypto-asset anonymization technologies

in order to lay down solid foundations for future policymaking

2. Current situation of crypto-assets

2.1 Expansion of the crypto-asset economy

2.2 Expansion of crypto-crime

2.3 Crypto-laundering

Summary of this chapter

- Although the crypto-asset ecosystem has not grown very much as of yet, the transaction of crypto-assets is rapidly expanding among individuals in particular.

- The variety of uses for crypto-assets are expanding in the areas of e-commerce, crypto-fiat trading, capital flight, crypto-crypto trading and crypto-related services.

- On the other hand, the risk of criminal activity using crypto-assets is also increasing. Bitcoin has been widely used in dark markets, and the use of altcoin is now expanding. Furthermore, crypto-crime is growing and the types of attacks are diversifying. As a result, the total amount of financial damage is increasing.

- Criminal proceeds from crypto-assets are laundered through (1) exchanges, payment service providers, and DEXs that are not compliant with regulations, (2) mixing services, and (3) gambling sites.

- Among these, exchanges are reported to be the most widely used as a laundering tool. Although reports indicate that AML/CFT regulations are having an impact, there are still quite a few exchanges located in FATF non-compliant countries or non-KYC exchanges. Therefore, the closing of all the laundering routes that lead to criminal proceeds from crypto-assets poses as a real challenge.

2.1 Expansion of the crypto-asset economy－Increase in accounts

The use of crypto-assets, which initially attracted attention as a tool used to facilitate capital flight in a financial crisis or in high inflation countries and as a settlement tool used in the dark market, has expanded rapidly in recent years. It is estimated that the number of crypto-asset accounts totals about 1.4 billion globally, and many of them are held by individuals.

Growth of crypto-asset accounts

A survey of 47 countries showed that the number of crypto-asset accounts increased by 63% in 2018 (1.4 billion), including about 25% of ID-verified users.

Lower-bound Estimate of Total cryptoasset Users

Million

Legend: ■ Total Accounts ■ Total ID-verified users

- 2016: 190%, 398%
- 2017: 163%, 194%
- 2018Q1-Q3
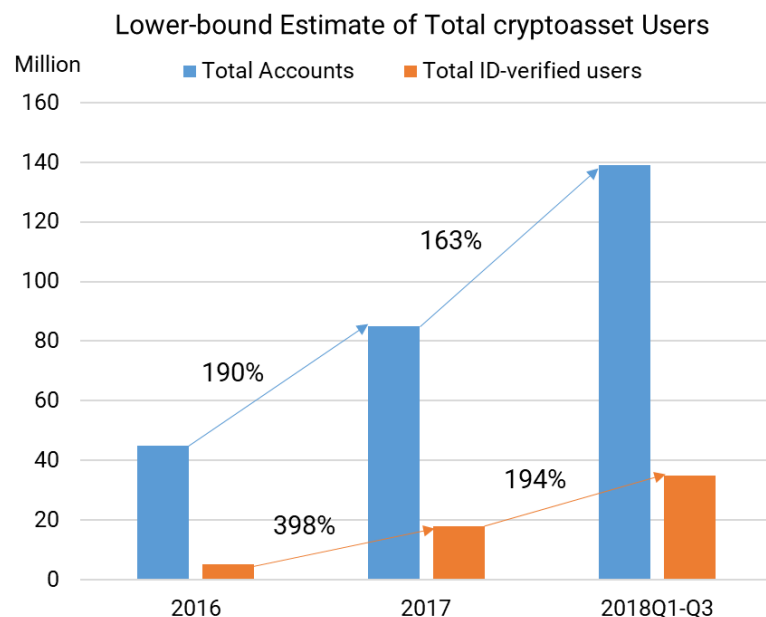
Share of crypto-asset account holders

The majority of users are individuals from all types of service providers.

Legend: ■ Individuals ■ Business clients ■ N/A

- Multi-segment: Individuals 58%, Business clients 26%, N/A 16%
- Exchange: Individuals 46%, Business clients 32%, N/A 22%
- Wallet Providers: Individuals 70%, Business clients 19%, N/A 11%
- Payment Gateways: Individuals 78%, Business clients 16%, N/A 6%
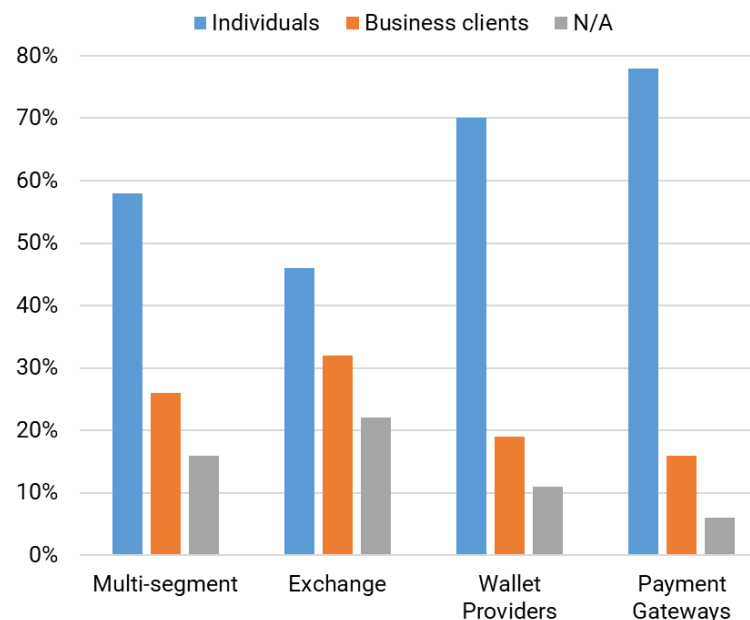
(Left, Right) Created by MRI based on Rauchs, M., et al., University of Cambridge Judge Business School, "2nd Global Cryptoasset Benchmarking Study", https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-12-ccaf-2nd-global-cryptoasset-benchmarking.pdf, Jan 9, 2019
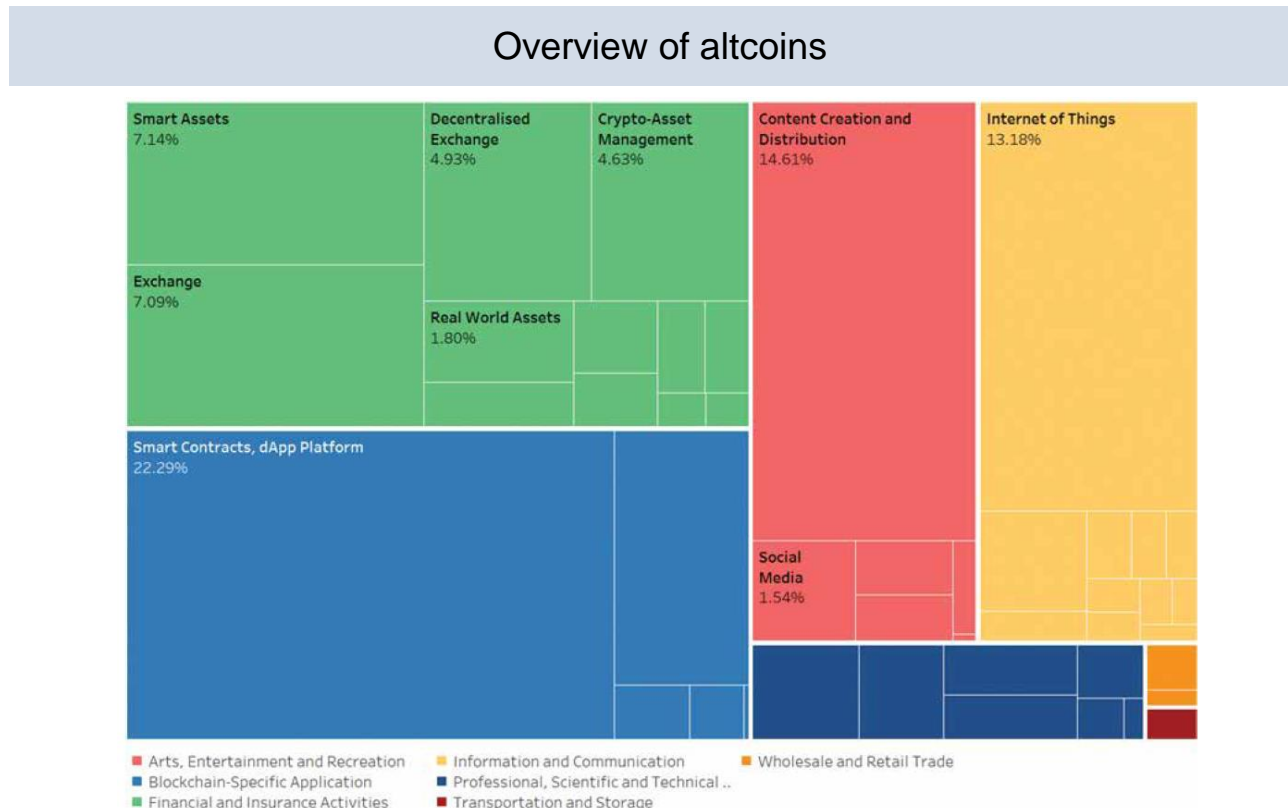
2.1 Expansion of the crypto-asset economy－Increase in countries

The crypto-asset industry is expanding globally. It is estimated that between 2-9% of the population of developed countries such as Japan, U.S., Europe, and Canada have crypto-assets obtained via crypto-asset service providers.

Geographic distribution of the crypto-asset industry

Number of entities
- 1-2
- 3-5
- 6-10
- 11-20
- 21-50
- >50
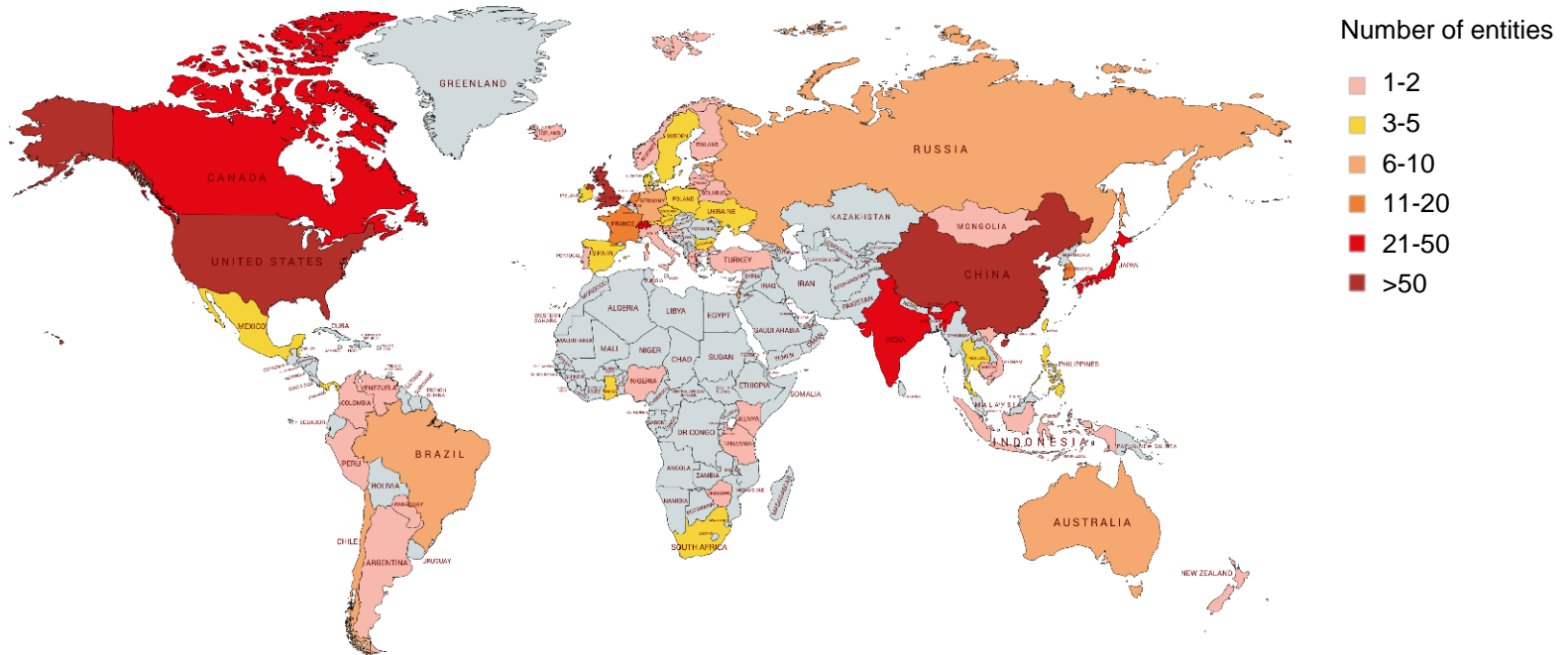
Created by MRI using; Minas, "mapchart.net", https://mapchart.net/world.html, Feb 23, 2019
based on; Rauchs, M., et al., University of Cambridge Judge Business School, "2nd Global Cryptoasset Benchmarking Study", https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-12-ccaf-2nd-global-cryptoasset-benchmarking.pdf, Feb 23, 2019

2.1 Expansion of the crypto-asset economy – Legality

It is reported that Bitcoin is either legal or neutral in 110 countries: however it is treated differently, either as "currency", "property" or a "commodity", from country to country where regulations also differ.

Bitcoin legality by country

Legend:
- legal
- neutral
- restricted
- illegal
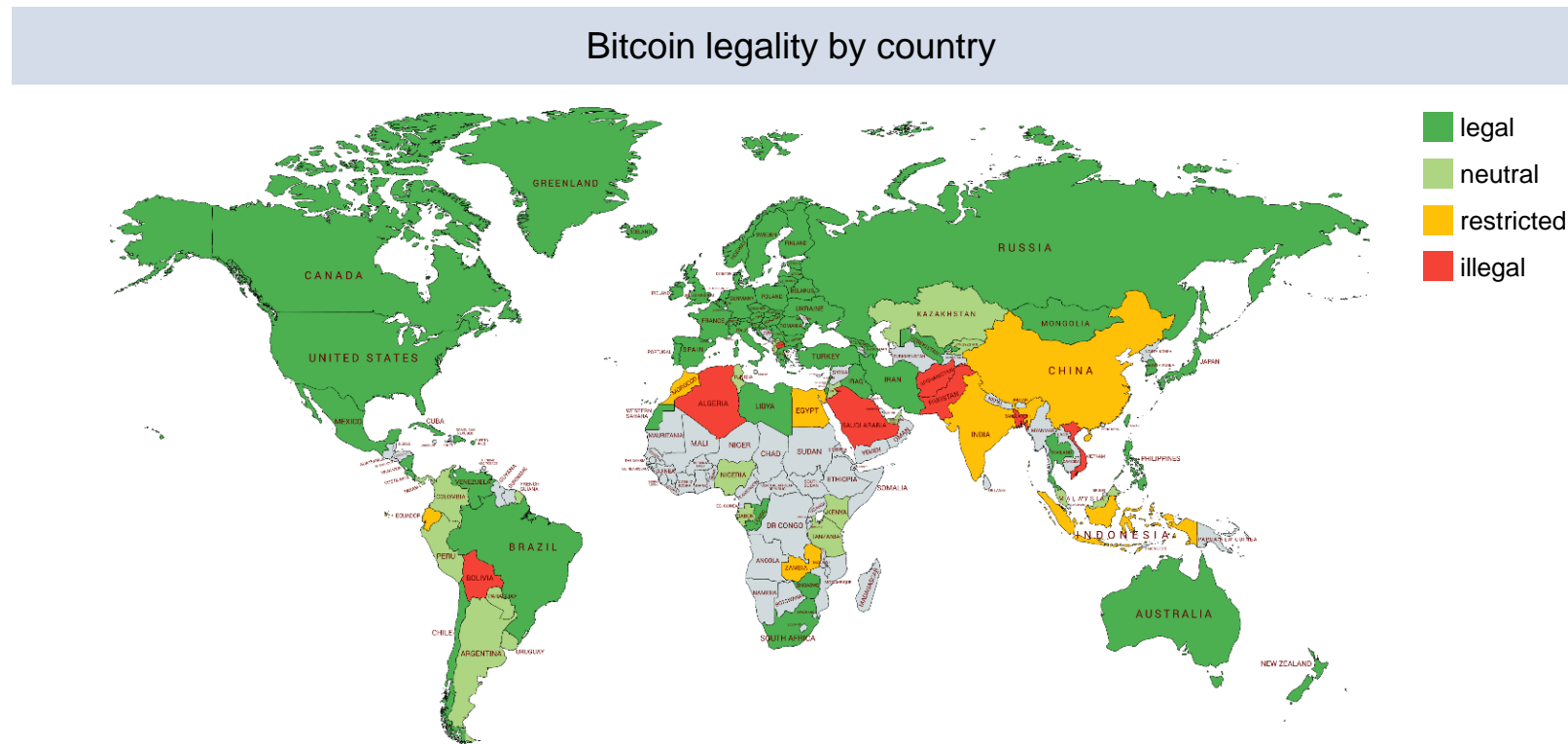
Created by MRI using; Minas, "mapchart.net", https://mapchart.net/world.html, Feb 23, 2019
based on; Coin Dance, coin.dance, "Bitcoin Legality by Country", https://coin.dance/poli/legality, Feb 23, 2019

2.1 Expansion of the crypto-asset economy – Emerging uses

Uses of crypto-assets are often sorted into three categories: a means of exchange ("Exchange Token"), an investment/capital raising tool ("Security Token"), and a means of accessing applications or services ("Utility Token"). In addition to having a strong association with digital goods as exchange tokens, crypto-assets are increasingly used as utility tokens; SNS, online games, and contents delivering.

Overview of altcoins

Smart Assets 7.14%

Decentralised Exchange 4.93%

Crypto-Asset Management 4.63%

Content Creation and Distribution 14.61%

Internet of Things 13.18%

Exchange 7.09%

Real World Assets 1.80%

Smart Contracts, dApp Platform 22.29%

Social Media 1.54%

Legend:
- Arts, Entertainment and Recreation
- Information and Communication
- Wholesale and Retail Trade
- Blockchain-Specific Application
- Professional, Scientific and Technical ..
- Financial and Insurance Activities
- Transportation and Storage

2.1 Expansion of the crypto-asset economy – Crypto-to-crypto transactions

More than 1,900 different types of crypto-assets currently exist (another survey including other subspecies reported more than 160 thousand), and crypto-to-crypto transactions are actively taking place.

Fiat-to-crypto and crypto-to-crypto volumes (October to November, 2018)

A survey collecting data from more than 70 exchanges showed that about two-thirds of the total volume are crypto-to-crypto transactions (40% of exchanges covered only crypto-to-crypto transactions).

CryptoCompare, Crypt Coin Comparison LTD, "CCCAGG Exchange Review, November 2018", https://www.cryptocompare.com/media/35308846/cryptocompare_exchange_review_2018_11.pdf, Jan 14, 2019
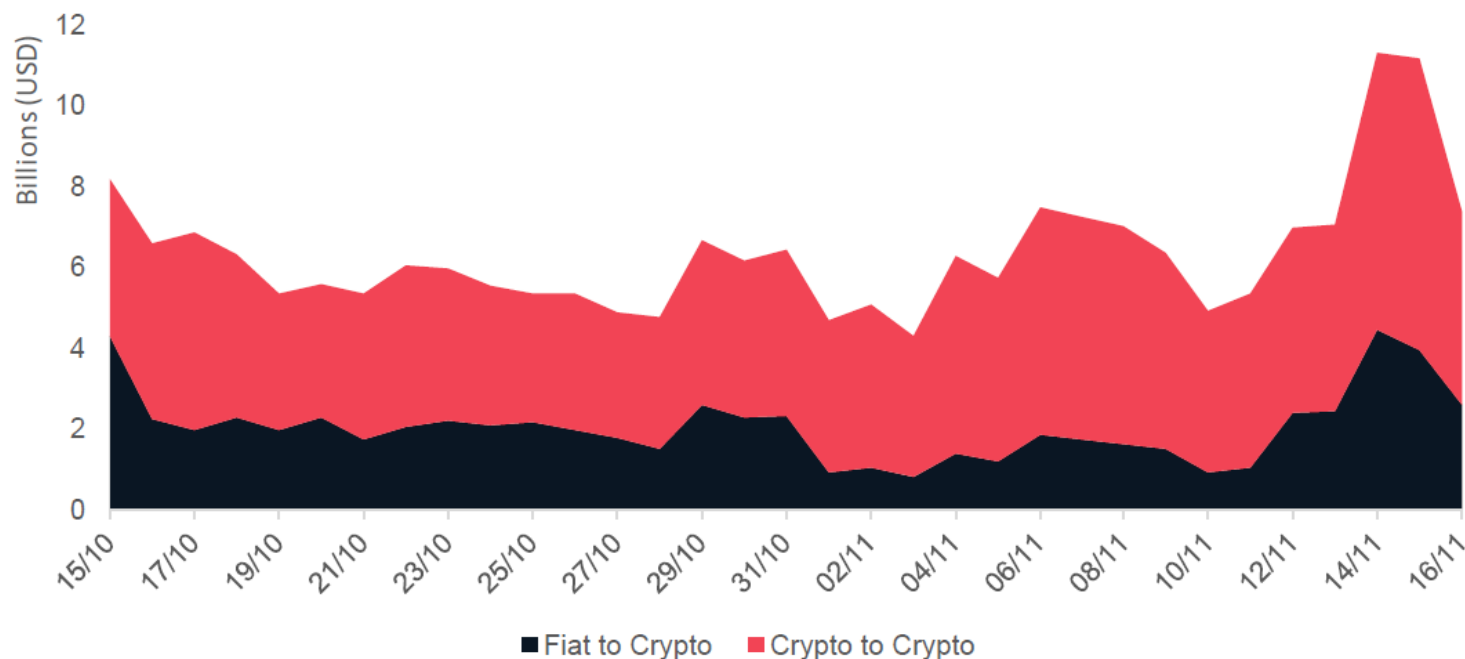
2.1 Expansion of the crypto-asset economy – Potential of blockchain technology

It has been pointed out that blockchain technologies could change traditional business models as the market capitalization of shared protocols that provide shared data and tokens grows faster than applications. More possibilities are expected with DApps (Distributed Applications) due to their unique characteristics; no central entity is required, they are always available, their program logic is published publicly and highly transparent, and there is the possibility of programmable payment.

Comparison between the Internet and blockchain technology

In blockchain technology, a shared protocol provides shared data and tokens that can be used by a variety of applications. Therefore, it is said that the capitalization of shared protocols will grow faster because the success of individual applications calls for demand and speculation concerning tokens/data. This demand increases the market capitalization of the shared protocol (Opinions concerning this prominent point of view are divided).
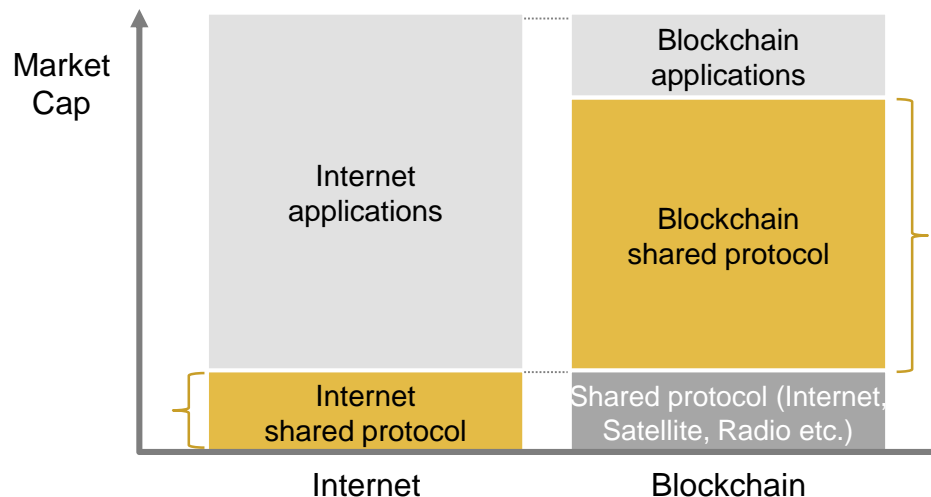
Comparison between centralized and decentralized system

Distributed applications used on a blockchain are characterized by several unique features: the program logic is published, the logic cannot be changed in secret by any one party, and any changes that do occur are made public. Such transparency and verifiability are considered to be important features of DApps.

(Left) Created by MRI based on Monegro, J., UNION SQUARE VENTURES, "Fat Protocols", http://www.usv.com/blog/fat-protocols, Jan 11, 2019
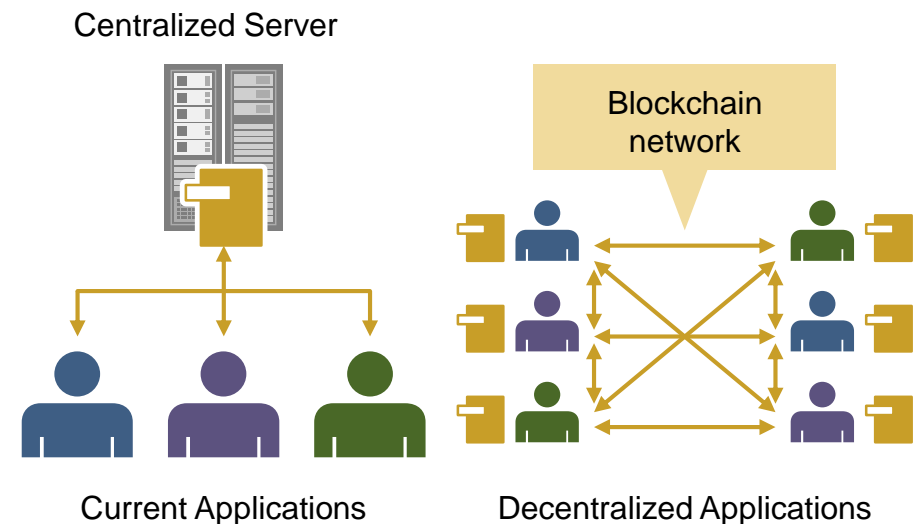
2.2 Expansion of crypto-crime – Trends in dark markets

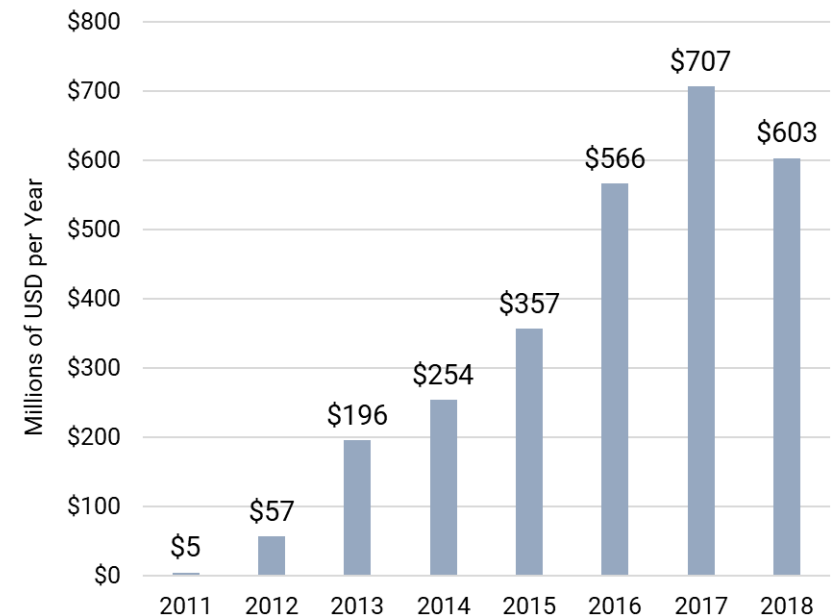Bitcoin has been widely used in dark markets, and the use of altcoin is now growing.

| Crypto-assets used in the dark web (2018) | Bitcoin flowing into dark markets (2011 - 2018) |

A survey investigating 150 sites, including the marketplace and bulletin board, on the dark web reported that BTC (Bitcoin) was available on all sites and Litecoin came in second. The survey also reported geographical variations: for example, Monero was used mainly in English-speaking countries, and Dash in Eastern Europe.

The amount of Bitcoin that flowed into dark markets exceeded $700 million in 2017. From mid-2017, it is estimated that the use of altcoins has been increasing due to Bitcoin's larger transaction fees and longer processing delays.

Bitcoin 100%
Litecoin 30%
Dash 20%
BitcoinCash 13%
Ether 9%
Monero 6%

Millions of USD per Year

2011 $5
2012 $57
2013 $196
2014 $254
2015 $357
2016 $566
2017 $707
2018 $603

(Left) Created by MRI based on Barysevich, A., et al, Record Future, "Litecoin Emerges as the Next Dominant Dark Web Currency", https://www.recordedfuture.com/dark-web-currency/, Feb 23, 2019
(Right) Created by MRI based on Chainalysis Team, Chainalysis, "Crypto Crime Report - Decoding increasingly sophisticated hacks, darknet markets, and scams January 2019", https://blog.chainalysis.com/2019-cryptocrime-review, Feb 23, 2019

2.2 Expansion of crypto-crime – Trends in dark markets

The number of dark markets is on the rise, and they are diversifying into multiple markets. It is believed that crypto-assets used in dark markets are then sent to crypto-laundering services.

Number of illicit entities dealing with criminal proceeds from crypto-assets, by type (2013-2016)

Dark markets account for the majority of illicit entities using criminal proceeds acquired from crypto-assets. The number of entities including ransomware increased five-fold from 2013 to 2016 (total 60 entities).
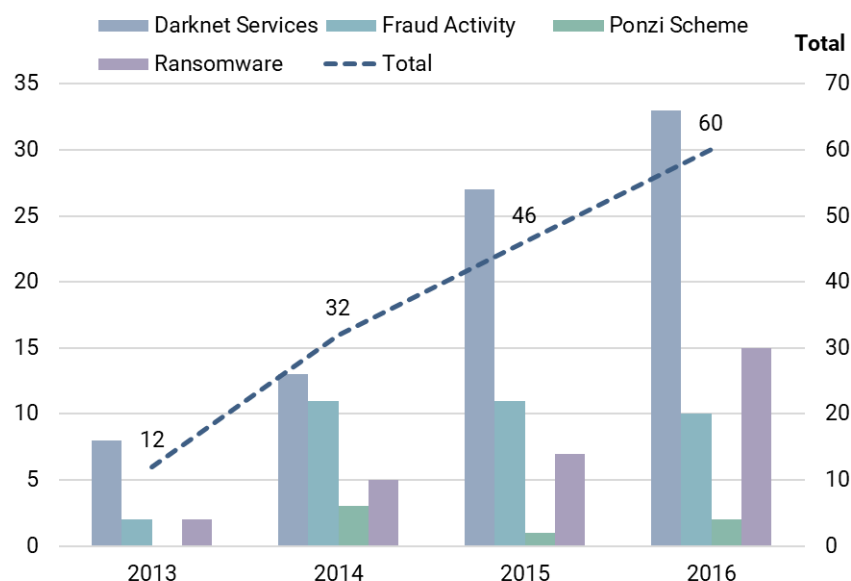
Major dark markets (Origin of illicit bitcoin entering laundering services, 2013-2016)

The dominating dark market shifted from SilkRoad (shut down in 2013) to Agora (shut down in 2015) and then to AlphaBay (shutdown in 2017). The overall market is becoming less dominated by just a few key players.
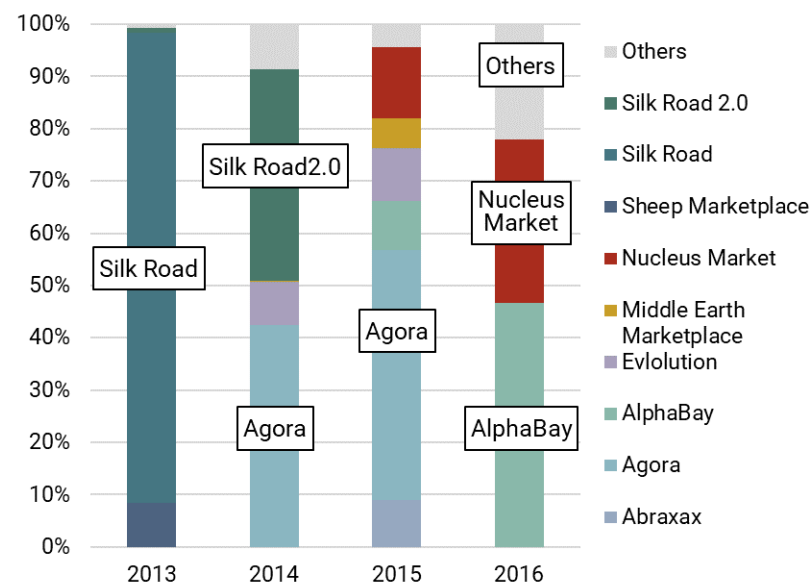
(Left, Right) Created by MRI based on Fanusie, Y., et al, Foundation for Defense of Democracies (the Center on Sanctions and Illicit Finance), "Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services", https://www.fdd.org/wp-content/uploads/2018/01/MEMO_Bitcoin_Laundering.pdf, Jan 18, 2019

2.2 Expansion of crypto-crime － Cyber-security incidents

Exchange hacks that targeted MtGox, Coincheck, and Zaif in particular attracted the attention of the general public due to the exposure of security risks concerning exchanges and crypto-launderings.

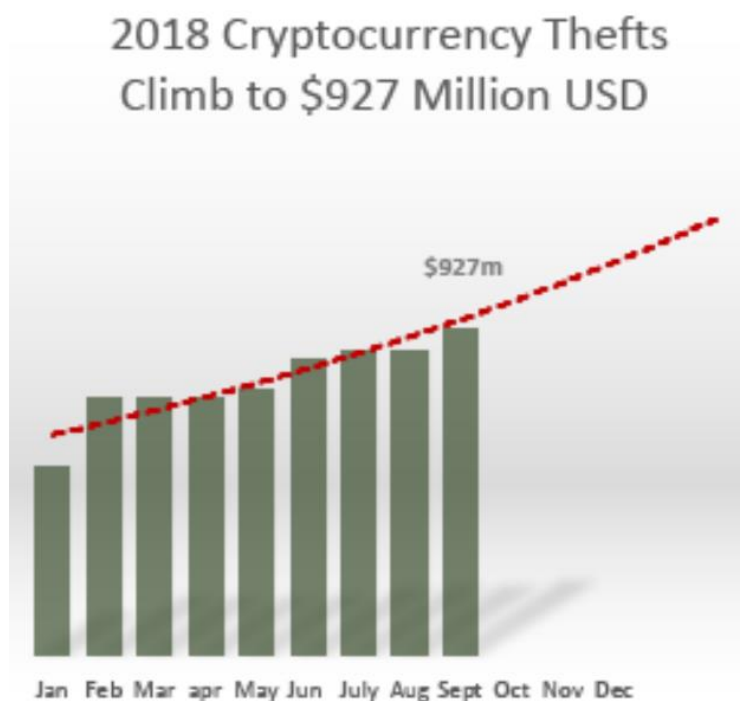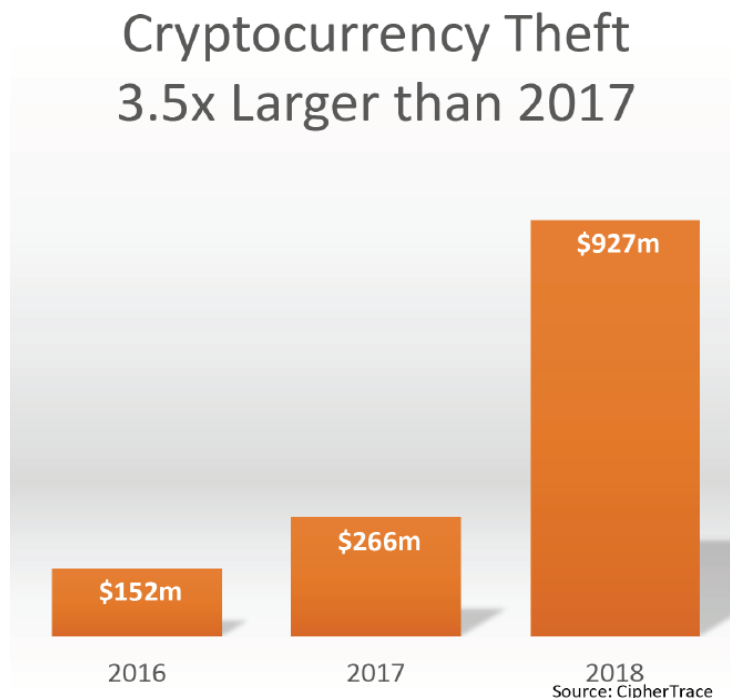| Major cyber-security incidents concerning crypto-assets		
Date	**Exchange/name of incident**	**Amount lost**
Feb. 2014	MtGox (Japan)	47 billion yen
Jun. 2016	The DAO	6.5 billion yen
Aug. 2016	Bitfinex (Hong-Kong)	6.5 billion yen
Jun. 2017	Wanacry	16 million yen (amount of ransom)
Oct. 2017	Thether (U.S.)	5 billion yen
Dec. 2017	NiceHash (Slovenia)	6.8 billion yen
Jan. 2018	Coincheck (Japan)	58 billion yen
Feb. 2018	BitGrail (Italy)	18.1 billion yen
Jun. 2018	Coinrail (South Korea)	4 billion yen
Jun. 2018	Bithumb (South Korea)	3.3 billion yen
Jul. 2018	Bancor (Switzerland)	2.6 billion yen
Sep. 2018	Zaif (Japan)	7 billion yen

2.2 Expansion of crypto-crime – Amount of losses

The amount of crypto-asset theft from exchanges during the first three quarters of 2018 was already 3.5 times larger ($927 million) than the entire year of 2017. At the time, it was estimated that the total amount will be well over $1 billion by the end of the year. It is thought that the stolen crypto-assets were then sent to crypto-laundering services.

Stolen crypto-asset amounts (Left: by year, Right: by month in 2018)

Cryptocurrency Theft 3.5x Larger than 2017

$927m
$266m
$152m

2016   2017   2018
Source: CipherTrace

2018 Cryptocurrency Thefts Climb to $927 Million USD

$927m

Jan Feb Mar apr May Jun July Aug Sept Oct Nov Dec

(Left, Right) CipherTrace, CipherTrace, Inc., "Cryptocurrency Anti-Money Laundering Report - Q3 2018", https://ciphertrace.com/wp-content/uploads/2018/10/crypto_aml_report_2018q3.pdf, Jan 11, 2019

2.2 Expansion of crypto-crime－Types of cyber attacks

In addition to cyber-crime that targeting exchanges, crypto-crime is not only growing but the types of attacks have also increased in recent years including crime that exploits blockchain reorganization, ransomware aimed at members of the general public, phishing fraud and crypto-jacking.

Number of detected ransomwares (top) and crypto jacking malwares (bottom)

There was a shift in the major type of cyber attacks after the end of 2017 when the value of crypto-assets rose dramatically.
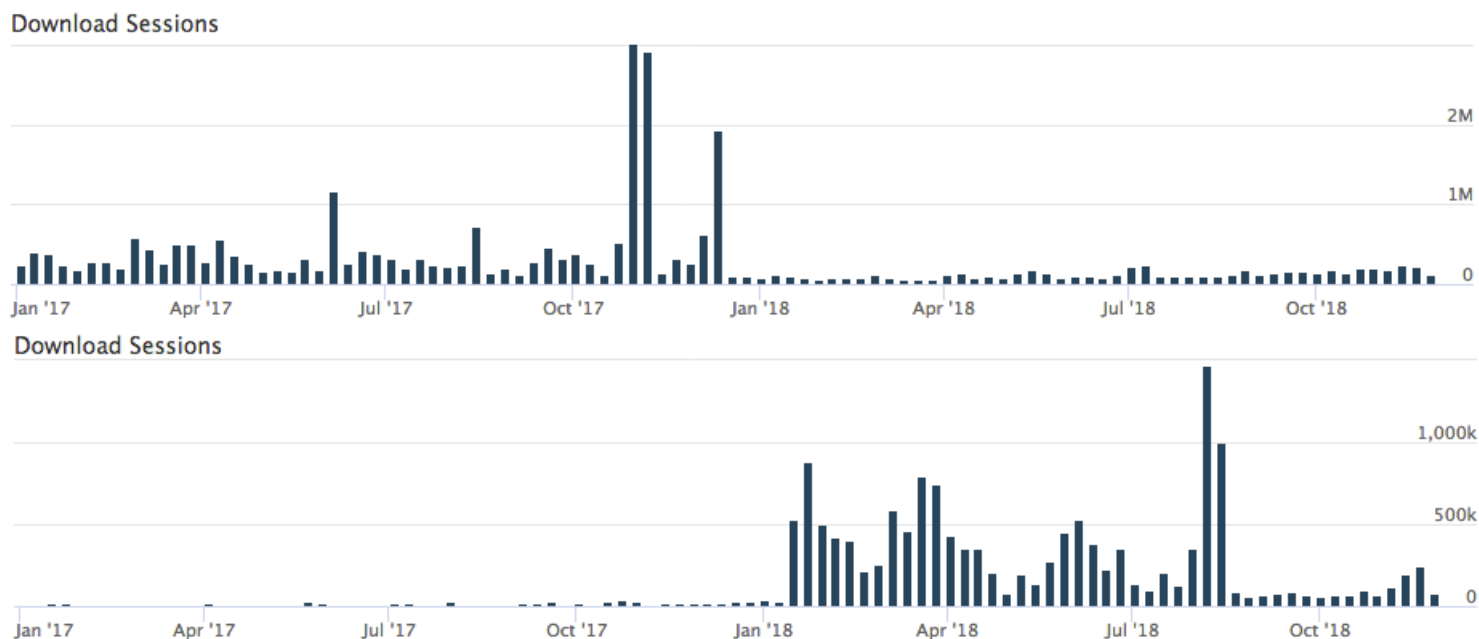
(Top) 林 薫, Palo Alto Networks, Inc., "2018年のサイバー脅威の振り返りと2019年の予測", https://www.paloaltonetworks.jp/content/dam/pan/ja_JP/Images/blog/2018/126525/picture-02.png, Jan 30, 2019
(Bottom) 林 薫, Palo Alto Networks, Inc., "2018年のサイバー脅威の振り返りと2019年の予測", https://www.paloaltonetworks.jp/content/dam/pan/ja_JP/Images/blog/2018/126525/picture-03.png, Jan 30, 2019

2.3 Crypto-laundering

The criminal proceeds on crypto-assets are thought to be laundered through (1) exchanges, payment service providers and DEXs that are not compliant with regulations, (2) mixing services, and (3) gambling sites.

Illustration representing the flow of crypto-laundering

Exchanges and DEXs not compliant with regulations

Mixing services

Crypto-assets gained through criminal activities

Exchanges

Fiat

Gambling sites

2.3 Crypto-laundering – Utilized services

The following services are thought to be used for crypto-laundering: exchanges, mixing services, online gambling sites and DEXs.

Between 20-30 percent of bitcoins received via mixing services came from illicit sources (this ratio decreased in 2016 due to a dramatic increase of the total volume).
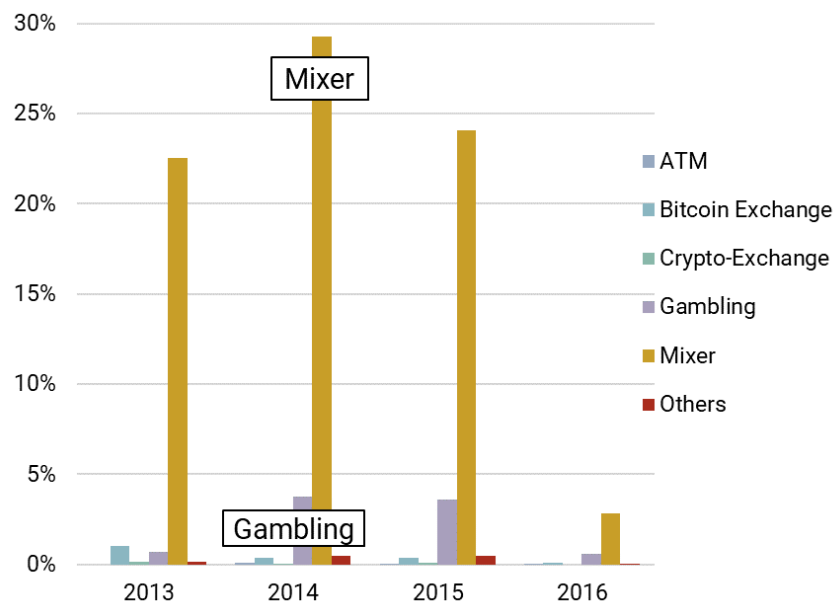
Exchanges, mixing services, online gambling sites and DEXs are services originating from dark markets that are used for the laundering of crypto-assets from illicit entities.
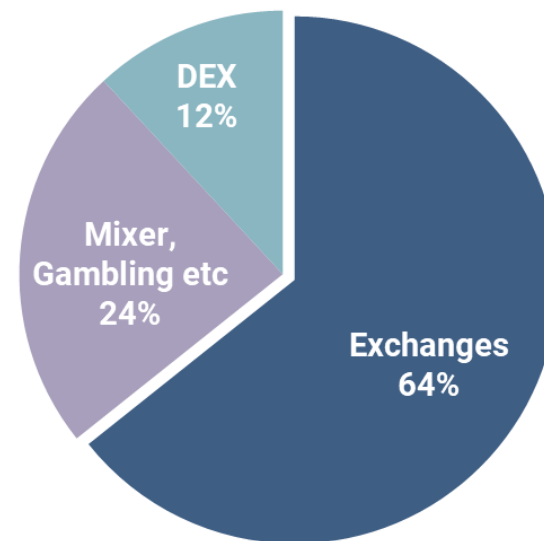
Note that both the left and right figures do not cover all crypto-crime nor all dark market transactions.

(Left) Created by MRI based on Fanusie, Y., et al, Foundation for Defense of Democracies (the Center on Sanctions and Illicit Finance), "Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services", https://www.fdd.org/wp-content/uploads/2018/01/MEMO_Bitcoin_Laundering.pdf, Jan 18, 2019
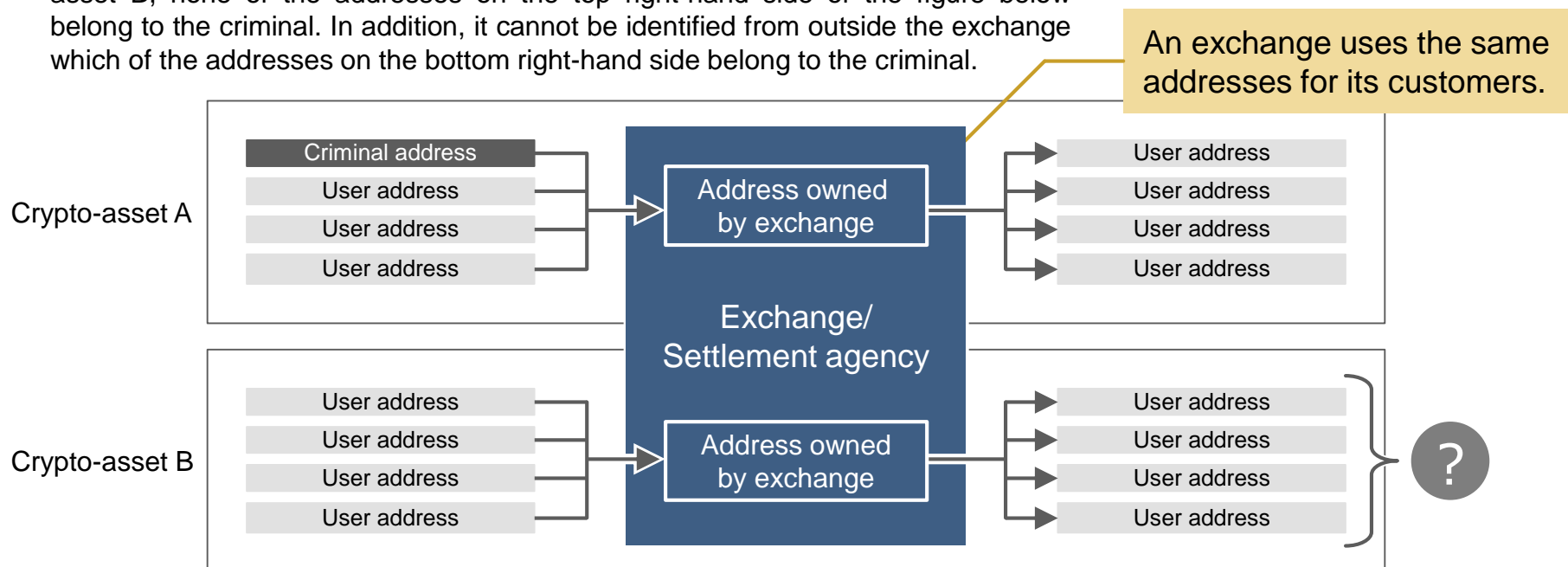(Right) Created by MRI based on Chainalysis Team, Chainalysis, "Crypto Crime Report - Decoding increasingly sophisticated hacks, darknet markets, and scams January 2019", https://blog.chainalysis.com/2019-cryptocrime-review, Jan 18, 2019

2.3 Crypto-laundering – Exchanges

Exchanges are often used for crypto-laundering, since one can convert assets to fiat currencies or other crypto-assets and transfer routes within exchanges are not visible externally. Crypto-laundering though major exchanges is estimated to be around $2.5 billion from January 2009 to September 2018.

Illustration of an exchange used for crypto-laundering

When a criminal sends crypto-asset A to the exchange and withdraws it as crypto-asset B, none of the addresses on the top right-hand side of the figure below belong to the criminal. In addition, it cannot be identified from outside the exchange which of the addresses on the bottom right-hand side belong to the criminal.

An exchange uses the same addresses for its customers.

Crypto-asset A

| Criminal address |
| User address |
| User address |
| User address |

Address owned by exchange

| User address |
| User address |
| User address |
| User address |

Exchange/ Settlement agency

Crypto-asset B

| User address |
| User address |
| User address |
| User address |

Address owned by exchange

| User address |
| User address |
| User address |
| User address |

?

Reference: CipherTrace, CipherTrace, Inc., "Cryptocurrency Anti-Money Laundering Report - Q3 2018", https://ciphertrace.com/wp-content/uploads/2018/10/crypto_aml_report_2018q3.pdf, Jan 11, 2019

2.3 Crypto-laundering – Effect of regulation on exchanges

Indications show that there has been a larger influx of illicit crypto-assets into exchanges in unregulated or weakly regulated countries. On the other hand, results show the quantitative effects of AML/CFT regulations imposed on exchanges.
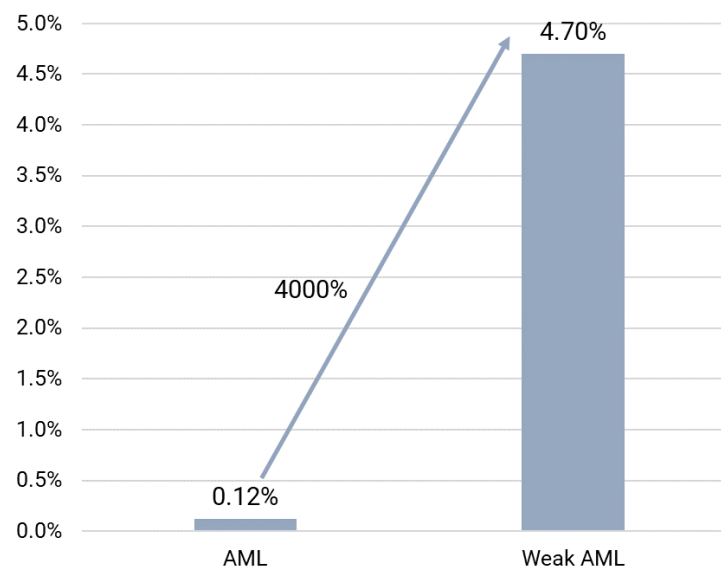
AML regulations and illicit bitcoins on exchanges (January 2009–September 2018)

It is estimated that, compared to exchanges in strongly regulated countries, those in weak AML countries received 36 times more bitcoins from criminal sources and sent 18 times more bitcoins to criminal entities.
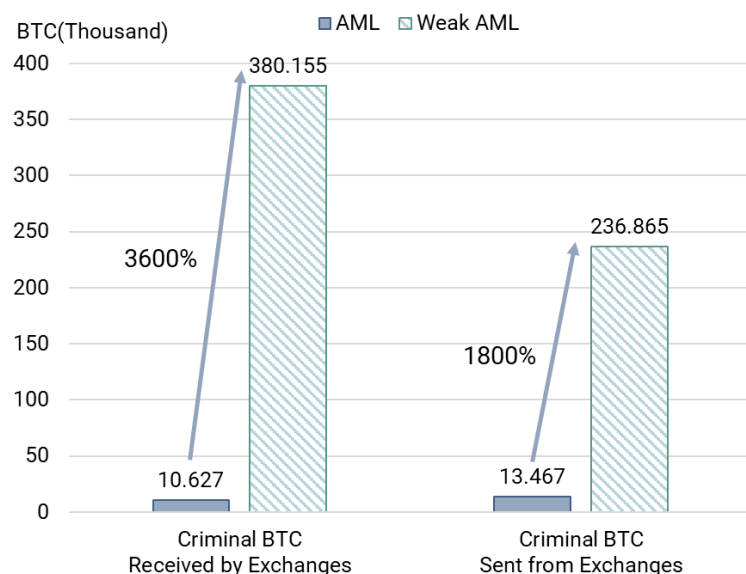
AML regulations and the percentage of suspicious transactions in exchanges (January 2009-September 2018)

Approximately 4.7% of all incoming bitcoins to exchanges in unregulated or weak countries are estimated to be related to criminal revenue compared to 0.12% for those exchanges in strongly regulated countries.

(Left, Right) Created by MRI based on CipherTrace, CipherTrace, Inc., "Cryptocurrency Anti-Money Laundering Report - Q3 2018", https://ciphertrace.com/wp-content/uploads/2018/10/crypto_aml_report_2018q3.pdf, Jan 11, 2019
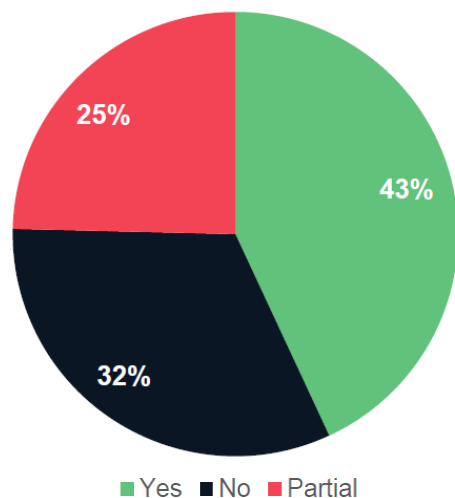
2.3 Crypto-laundering – Current status of Exchanges

There are quite a few exchanges that are non-compliant with AML/CFT regulations. It was reported that among 25 exchanges in Europe and the U.S., about 70% do not fully require KYC and about one third of the top 130 exchanges do not require KYC.

In addition, since there are many exchanges that have legal jurisdictions that are not fully compliant with FATF recommendations, indications show that it is difficult for regulators to make them fully comply with regulations.

KYC requirements among the top 130 exchanges	Top 10 exchange legal jurisdictions (Average exchange volumes between 15th October and 15th November 2018)

About one third (32%) of exchanges do not require KYC.

Top exchanges are located in Korea, Malta, Hong Kong, Samoa, Seychelles, USA, Singapore, Virginia Islands, Vanuatu, Estonia.
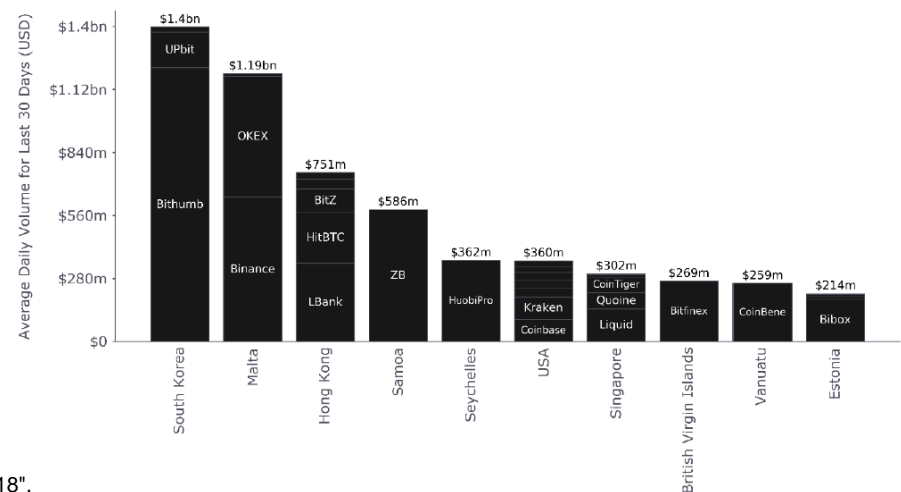
2.3 Crypto-laundering – Gambling sites

Entities that offer deposit and withdrawal services such as gambling sites can be used for crypto-laundering, since crypto-assets are accumulated together and transfer routes within the service are not visible externally.

Distribution of DApps by category	Illustration of crypto-laundering using gambling sites
About 50% of DApps are categorized as gambling.	Similar to exchanges, transfer routes within services that offer deposit and withdrawal services are not visible externally (Transfer routes will become even more complicated if users can send crypto-assets to each other within the particular service).

	Ethereum	EOS
Others (e.g, DEX)	25%	24%
Games	28%	10%
Gambling	47%	66%

Criminal address, User address → Deposit address → User address
Gambling site
User address → Withdrawal address → User address → ?
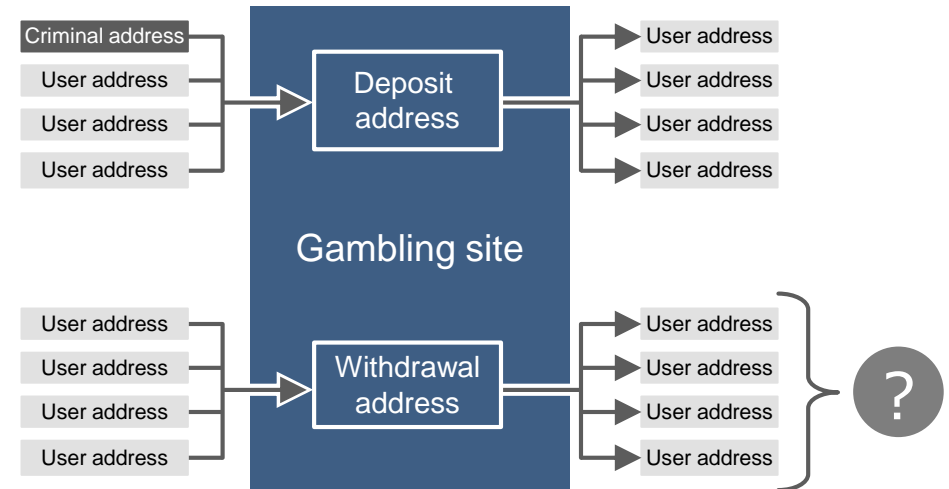
(Left) Created by MRI based on diar, Diar Ltd, "EOS, Tron Lure Betting Crowd to Decentralized Applications", https://diar.co/volume-3-issue-3/, 2019/2/8
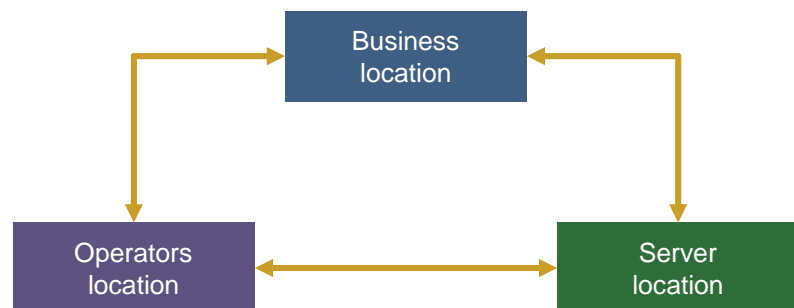(Right) Created by MRI based on Fiedler, I., ResearchGate, "Online Gambling as a Game Changer to Money Laundering?", https://www.researchgate.net/publication/254969899_Online_Gambling_as_a_Game_Changer_to_Money_Laundering, Feb 8, 2019

2.3 Crypto-laundering – Location of services used for crypto-laundering

The actual location of service providers used for crypto-laundering is often unknown and closing them proves to be rather difficult. Even if a service is can be accessed on the surface web rather than the dark web, it is still considered to be difficult to identify its location.
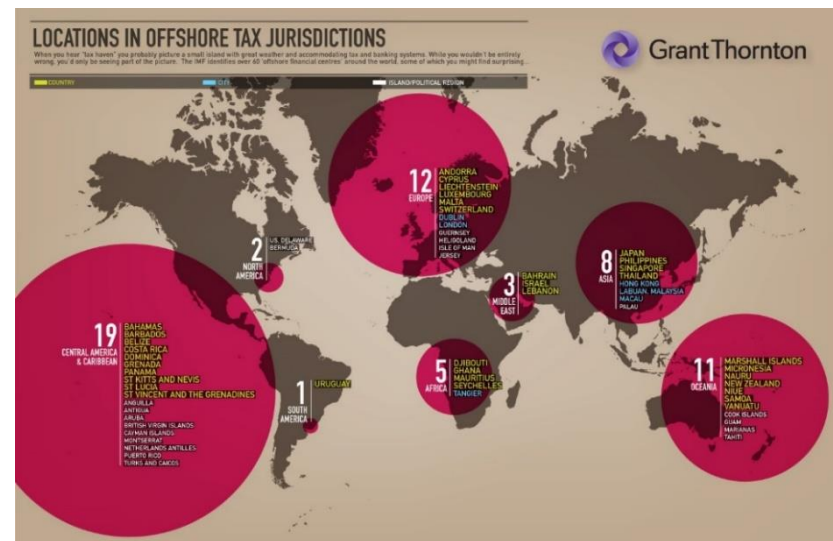
Location of illicit service providers	Examples of offshore company locations

Illegal sites such as phishing fraud sites can be cited as an example when talking about the location of services used for crypto-laundering. Research suggests that such an illegal business operator establishes an offshore company at a low price, provides a service using a special kind of hosting service that permits illegal content called "Bulletproof hosting", periodically closes the site and creates another one. In this case, it is difficult to enforce regulations because the registered company location, server location, and operator location are separated.

Reports show that offshore companies are often placed in offshore financial centers such as Belize, the Cayman Islands, Curacao and so on.

3. Investigation on anonymization technology for crypto-asset transactions

3.1 Overview of assessed technologies

3.2 Application layer (Blockchain)

3.3 P2P layer/Internet layer

3.4 Physical layer

Summary of this chapter

- We have classified anonymization/de-anonymization technologies into three layers: the "Application Layer", "P2P Layer/Internet Layer", and "Physical Layer".

- Concerning blockchain technology within the "Application Layer", in addition to already established techniques such as mixing and ring signatures, new approaches such as lightning networks, atomic cross-chain swaps, zero knowledge proofs and Mimblewimble are being proactively developed. These techniques enhance the anonymity of Bitcoin as well as other anonymous and privacy-focused altcoins.

  - The way mixing techniques that are already being widely used are anonymized has shifted from delegating to trusted intermediaries to the anonymization of transfer routes to intermediaries, transaction amounts, and the existence of transactions themselves.

  - These techniques are developed with scalability, reduction of custody risk and reduction of blockchain data in mind, in addition to ensuring fungibility and protecting privacy. They are evolving according to the prerequisites specific to the public blockchain.

- As for DEX in the "Application Layer", it remains in its early stages. Although it is designed to eliminate any custody risk when it comes to centralized exchanges, the transaction volume through DEX is still low and the technology behind DEX is still searching for the balance between safety and efficiency. It is predicted that there will be development of new uses only available for DEX as well as appropriate technical solutions.

Summary of this chapter

- Anonymizing networks int the "P2P Layer/Internet Layer" are easily and readily available. Protecting the overall anonymity of these networks as well as other applications such as Bitcoin and secure chat tools will be important in the near future.

- As for the "Physical Layer", internet access without KYC has already been possible through the use of free Wifi, prepaid SIM, and secondhand devices.

- Under these circumstances, de-anonymization is conducted with the combination of two approaches: (1) estimation based on protocols of each layer and (2) re-identification based on external data. However, this highly depends on errors made by criminals and is not effective in all cases. External data such as information concerning KYC, EC purchase history, logs and registries play an important role in performing de-anonymization. Nonetheless, there are cases in which such data cannot be used: for example, the information is discarded after a certain period of time, the quality of the information is low, or the information is not collected due to the privacy policy. These cases underline the technical difficulties with de-anonymization.

3.1 Overview of assessed technologies
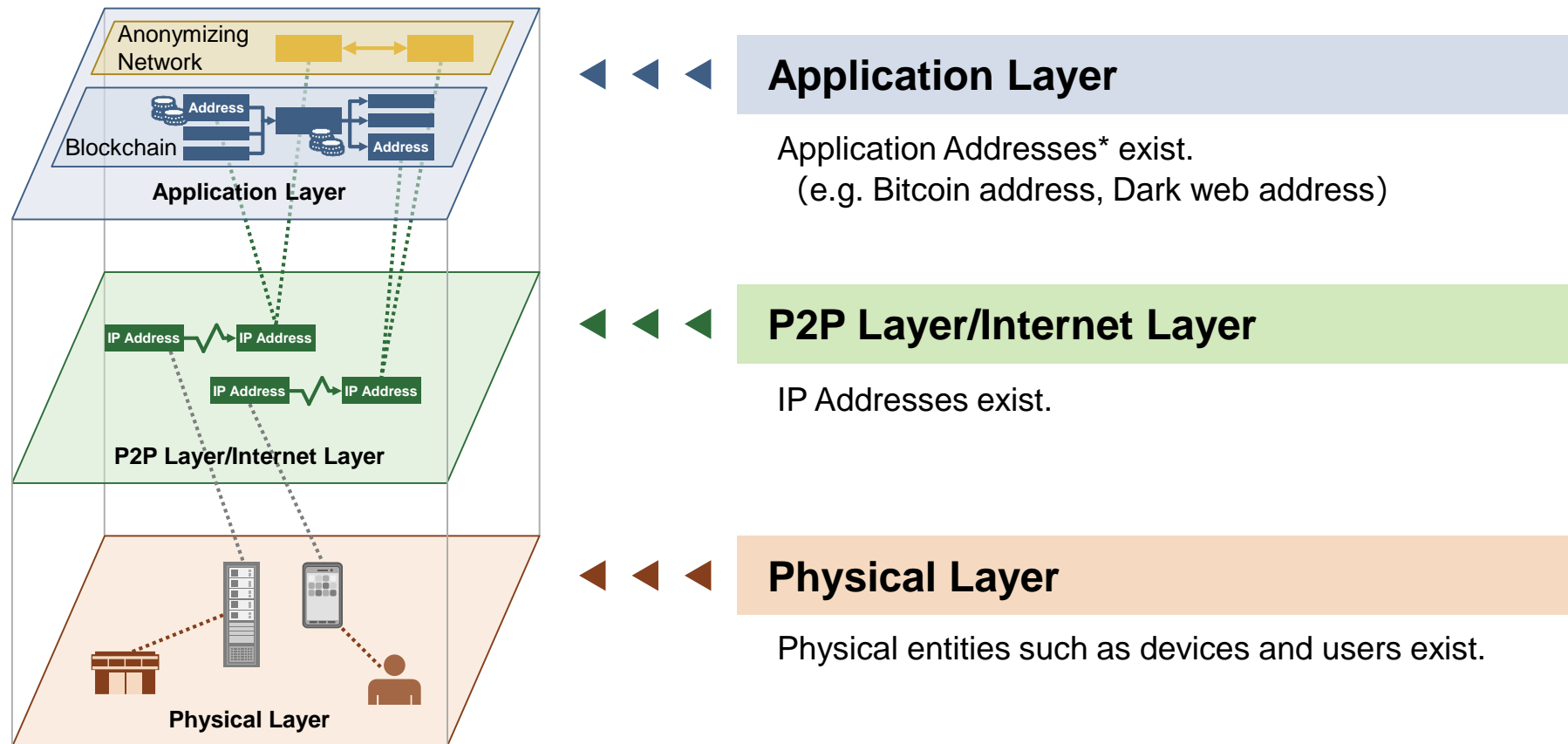
3.1.1 Overview of technologies

3.1.2 Examples of anonymization technology

3.1.3 Examples of de-anonymization technology

3.1.4 Examples of issues resolved through this research

3.1.1 Overview of technologies

We have classified anonymization/de-anonymization technologies into three layers: the "Application Layer", "P2P Layer/Internet Layer", and "Physical Layer".

Application Layer

Application Addresses* exist.
  (e.g. Bitcoin address, Dark web address)

P2P Layer/Internet Layer

IP Addresses exist.

Physical Layer

Physical entities such as devices and users exist.

* "Address" is an identifier relating to a user's location on a network or an application. (e.g., e-mail address)

3.1.1 Overview of technologies – Comparison with Internet Protocol Suite

Internet protocol suite

Anonymizing network

Address

Blockchain

Address

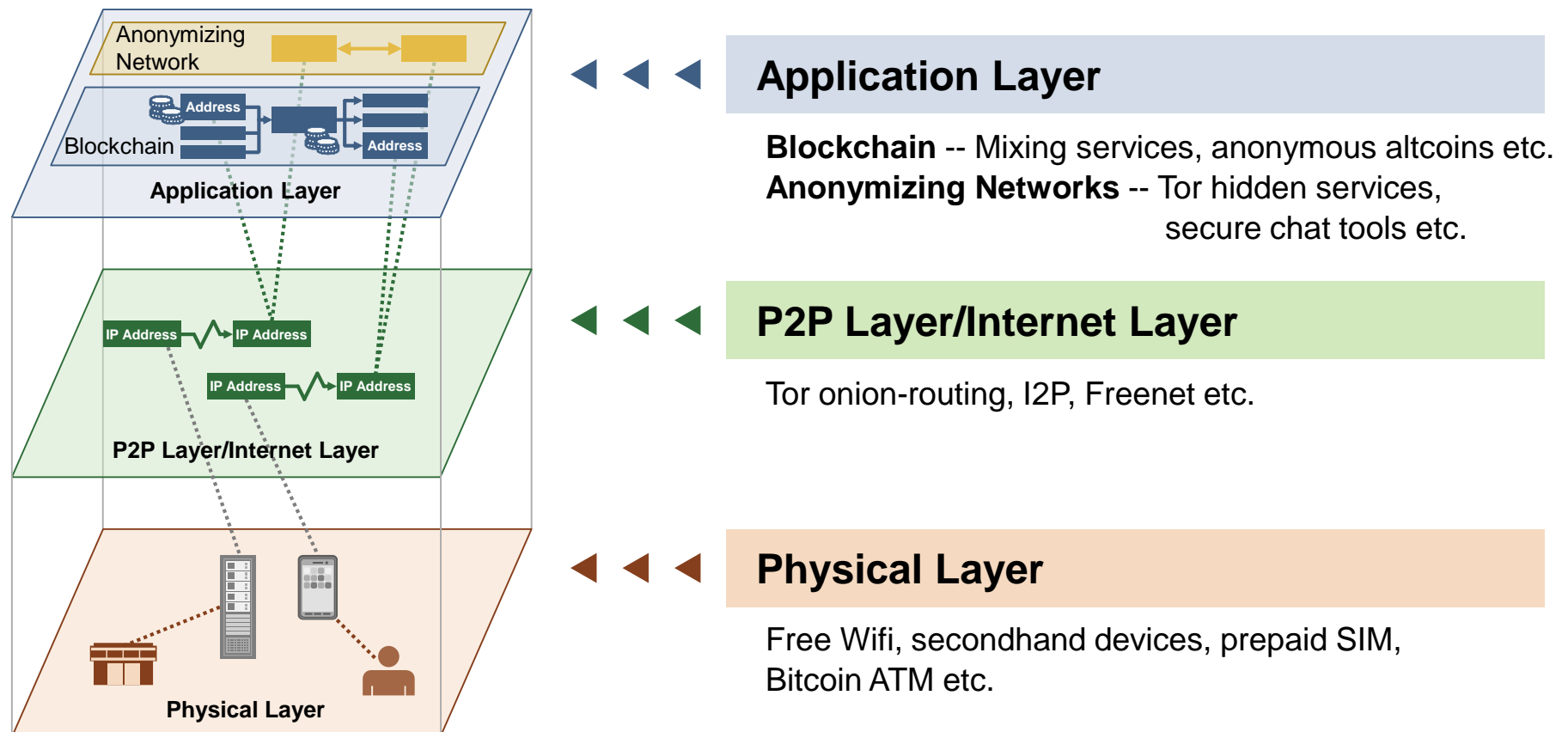**Application Layer**

The Application Layer corresponds to the

Application Layer

This layer has Blockchain and anonymizing network etc.

Application Layer

IP Address — IP Address

IP Address — IP Address

P2P Layer/Internet Layer

The Transport and Internet Layers correspond to the

Internet Layer

The Transport Layer specifies each application.
The Transport and Internet Layers can be classified as the same single layer from a tracing viewpoint.
On the other hand, since the association between IP addresses and MAC addresses can be changed arbitrarily, the Link Layer should be separate from the layers mentioned above.

Transport Layer
（Port number）

Internet Layer
（IP address）

Physical Layer

The Link Layer, devices and entities correspond to the

Physical Layer

Since the Link layer is generally able to be associated with devices on a one-to-one basis from a tracing viewpoint, they can be classified together as the same one layer (Physical Layer).

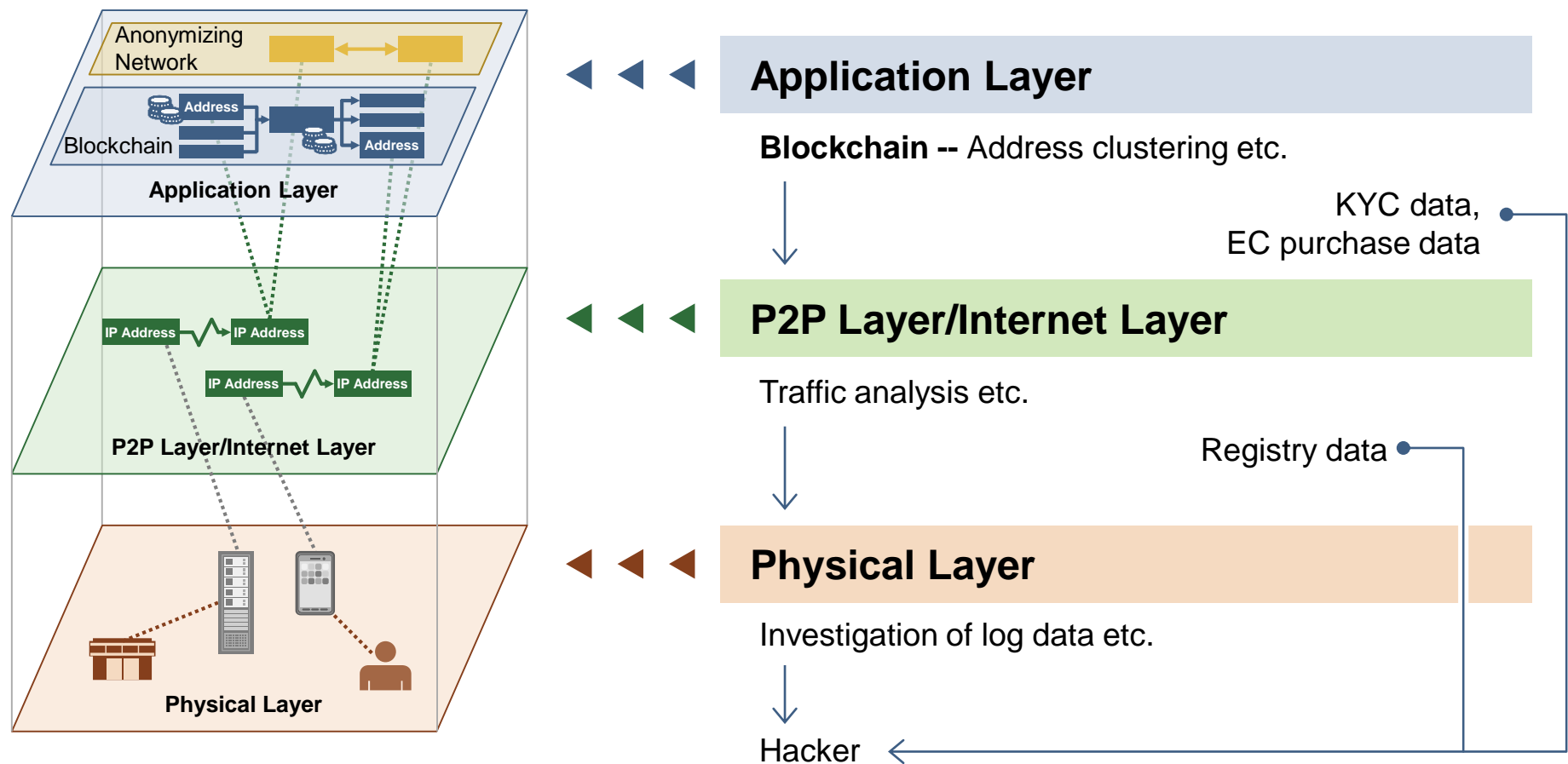**Link Layer**
（MAC address）

Entity ➡ Device

3.1.2 Examples of anonymization technology

Anonymization technologies are available for each layer, and it is not particularly difficult technologically or mentally to use them.

Application Layer

Blockchain -- Mixing services, anonymous altcoins etc.
Anonymizing Networks -- Tor hidden services,
secure chat tools etc.

P2P Layer/Internet Layer

Tor onion-routing, I2P, Freenet etc.

Physical Layer

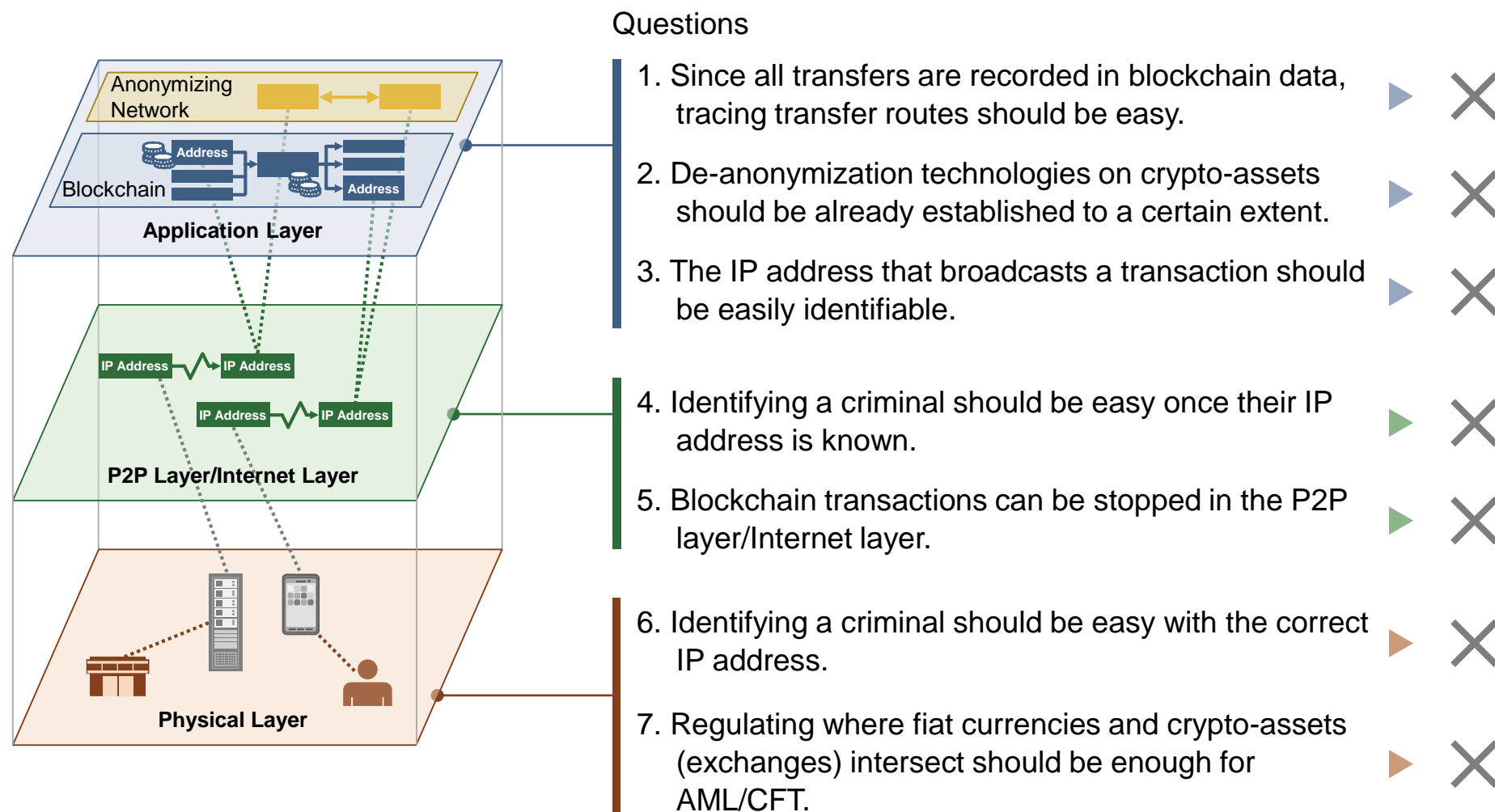Free Wifi, secondhand devices, prepaid SIM, Bitcoin ATM etc.

3.1.3 Examples of de-anonymization technology

De-anonymization technologies combine two approaches when used: (1) estimation based on protocols of each layer and (2) re-identification based on external data. However, these technologies highly depend on errors made by criminals meaning they are not always effective in all cases.

Application Layer

◀ ◀ ◀

Blockchain -- Address clustering etc.

KYC data, EC purchase data

P2P Layer/Internet Layer

◀ ◀ ◀

Traffic analysis etc.

Registry data

Physical Layer
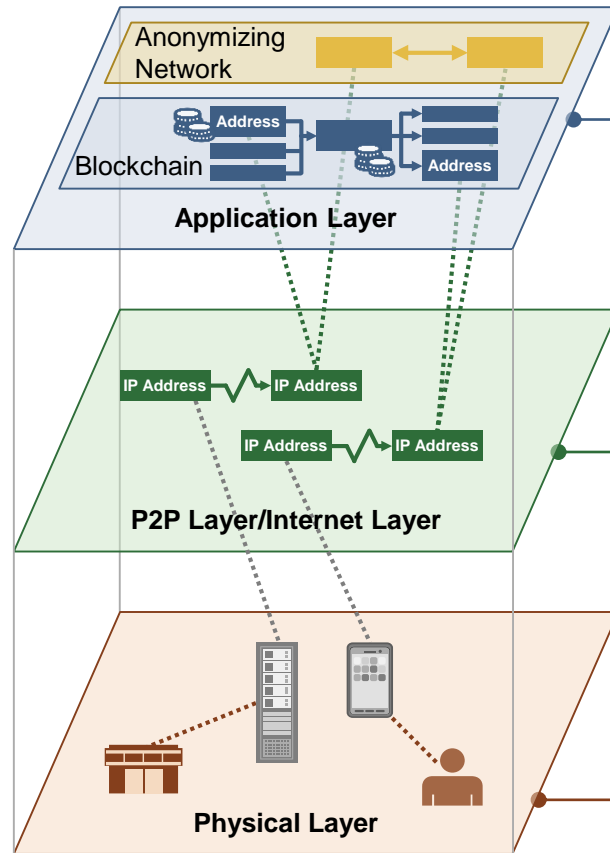
◀ ◀ ◀

Investigation of log data etc.

Hacker

3.1.4 Examples of issues resolved through this research

Having a firm understanding of the technological possibilities of de-anonymization is essential for discussions on crypto-asset regulations.

Questions

1. Since all transfers are recorded in blockchain data, tracing transfer routes should be easy. ▶ ✕

2. De-anonymization technologies on crypto-assets should be already established to a certain extent. ▶ ✕

3. The IP address that broadcasts a transaction should be easily identifiable. ▶ ✕

4. Identifying a criminal should be easy once their IP address is known. ▶ ✕

5. Blockchain transactions can be stopped in the P2P layer/Internet layer. ▶ ✕

6. Identifying a criminal should be easy with the correct IP address. ▶ ✕

7. Regulating where fiat currencies and crypto-assets (exchanges) intersect should be enough for AML/CFT. ▶ ✕

Anonymizing Network

Blockchain
Address
Address
Application Layer

IP Address — IP Address
IP Address — IP Address
P2P Layer/Internet Layer

Physical Layer

3.1.4 Examples of issues resolved through this research

Answers

1. It is difficult to link the source and the destination of a remittance, as well as trace transfer routes when mixing is used because candidate combinations grow exponentially.

2. There are no academic evaluations concerning the effectiveness of de-anonymization, and they are stochastic estimations as well as not always being effective.

3. It may be possible to prevent a sender from being identified by putting random delays in transfers between nodes or preparing dummy senders.

4. It is possible to withhold a source IP address from third parties by using anonymizing networks such as Tor.

5. It is difficult to distinguish blockchain transactions from one another through packet encryption or protocol spoofing and blocking IP addresses cannot cover all the possible target IP addresses.

6. It is not easy to identify criminals since internet access without KYC is now possible by using free Wifi and secondhand devices.

7. It is insufficient to only regulate exchanges due to the fact that highly anonymous crypto-laundering is already possible.

3.2 Application layer (Blockchain)

3.2.1 Blockchain anonymization technologies

3.2.2 Blockchain de-anonymization technologies

3.2.1 Blockchain anonymization technologies

3.2.1.1 Elemental blockchain anonymization technologies

3.2.1.2 DEX

Appendix. Secure chat tools

3.2.1.1 Elemental blockchain anonymization technologies

3.2.1.1.1 List of technologies surveyed

3.2.1.1.2 Mixing

3.2.1.1.3 Stealth Address

3.2.1.1.4 Ring Signature

3.2.1.1.5 Zero-Knowledge Proof (zk-SNARKs)

3.2.1.1.6 Lightning Network

3.2.1.1.7 Atomic Cross-Chain Swap

3.2.1.1.8 Mimblewimble

3.2.1.1.9 Schnorr Signature

3.2.1.1.10 Dandelion

3.2.1.1.11 Anonymous altcoins

3.2.1.1.1 List of technologies surveyed – Anonymizing principles

Anonymization in crypto-asset transfers targets (1) transaction contents and (2) originating nodes.

- Since transactions are published, the contents of the transaction– actual transfer routes, actual transfer information (sender, receiver, amount etc.), and the existence of the transaction itself – need be anonymized.
- The originating node refers to the owner of the required private key and can be supposed from the path through which the transaction propagates in the P2P network. In order to anonymize an originating node, propagation routes need to be complicated, and dummy nodes need to be prepared etc.

Example of anonymizing transaction contents (actual transfer routes)	Example of anonymizing originating nodes

Actual transfer routes can be obscured by accumulating coins together and then distributing them ("mixing").

An originating node can be obscured by having a random delay on each node for each transaction relay and making it difficult to estimate the propagation path.
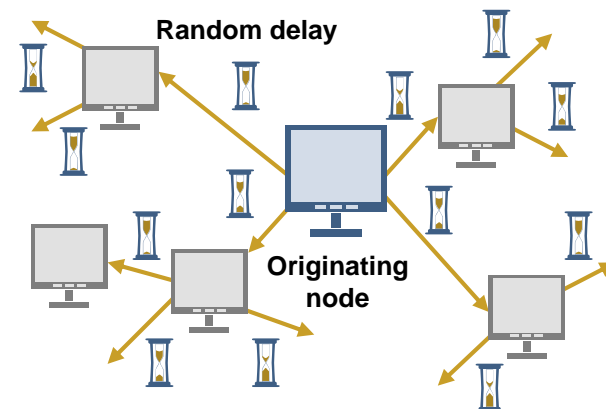
3.2.1.1.1 List of technologies surveyed

The following anonymization technologies were selected to be assessed based on advice from experts.

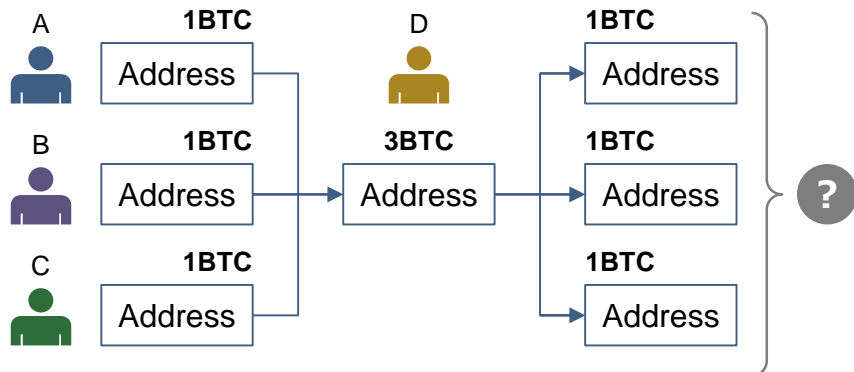| List of technologies assessed in this research				
No	Anonymiza tion	Technology	Example	Brief explanation
1	Transaction contents	Mixing	Bitcoin (CoinJoin, Tumblebit etc.), Dash (PrivateSend)	The relationship between a sender's address and a receiver's address is obscured from third parties by accumulating coins.
2		Stealth Address	Monero	The receiver is anonymized by using one-time addresses instead of the receiver's actual address.
3		Ring Signature	Monero (RingCT)	The sender is anonymized by introducing dummy senders.
4		Zero-Knowledge Proof (zk-SNARKs)	Zcash, Ethereum	Transaction contents are anonymized by not recording transaction details (sender, receiver, amount etc.) in blockchain data.
5		Lightning Network	Bitcoin (Lightning Network), Ethereum (Raiden Network)	The relationship between a sender's and a receiver's address is anonymized by making transactions off-chain (outside the blockchain) and have other nodes relay transactions.
6		Atomic Cross-Chain Swap	Bitcoin, Litecoin, Decred, Ethereum etc.	The relationship between transfers of different crypto-assets is anonymized by ensuring that deliveries of crypto-assets are made across different blockchain networks without any intermediaries.
7		Mimblewimble	Grin, Beam	The transaction amount is anonymized by using encryption and the existence of the transaction is also anonymized by not recording unnecessary transactions on blockchain data.
8		Schnorr Signature	Grin, Beam	By using signature aggregation, the amount of blockchain data is reduced, and the number of involved parties and transaction contents are anonymized.
9	Originating node	Dandelion	Grin, Zcoin	The originating node is anonymized by relaying transactions to randomly selected nodes a random number of times and letting other nodes broadcast.

3.2.1.1.2 Mixing

Mixing anonymizes actual transfer routes (a connection between a sender's address and a receiver's address) from third parties, and can be used for Bitcoin, Ethereum etc. Crypto-assets from multiple senders are accumulated and then redistributed.

Centralized mixing	Decentralized mixing（CoinJoin）

Multiple users send crypto-assets to a mixing service provider and receive the accumulated assets. However, as is often the case with exchanges, there are problems such as mixing service provider-related asset loss (e.g. loss due to stolen assets, hacking, and server failures) and privacy leakage to other mixing service providers.
*In practice, mixing service providers refund crypto-assets from a totally different fund pool.

Multiple users bring the same amount of crypto-assets, and then a transaction is carried out where each user withdraws the same amount, and gives their signature in order. As this transaction will not be valid unless all the signatures are available, there are no cases of stolen assets. However, in practice, it is difficult to bring users who send the same amount together at the right time. When amounts are uneven, the transfer routes may be able to be guessed to some extent by a third party.


Input	Output		Signature
A（1BTC）			$\mathcal{A}$
B（1BTC）	D	3BTC	$\mathcal{B}$
C（1BTC）			$\mathcal{C}$

Input	Output		Signature
	E	1BTC	
D	F	1BTC	$\mathcal{D}$
	G	1BTC	
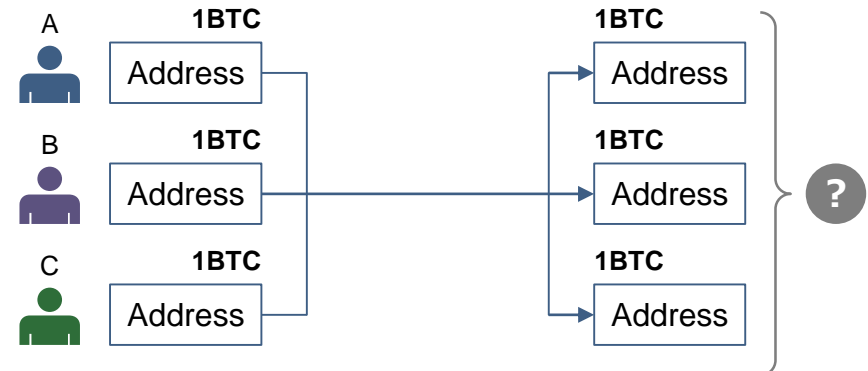
Input	Output		Signature
A（1BTC）	D	1BTC	$\mathcal{A}$
B（1BTC）	E	1BTC	$\mathcal{B}$
C（1BTC）	F	1BTC	$\mathcal{C}$

3.2.1.1.2 Mixing – Chaumian CoinJoin

Anonymization methods have evolved from delegating to trusted intermediaries to the anonymization of transfer routes to intermediaries (CoinShuffle, Tumblebit, Chaumian CoinJoin), transaction amount (ValueShuffle) and the existence of transactions themselves (CoinJoinXT).

Chaumian CoinJoin flowchart
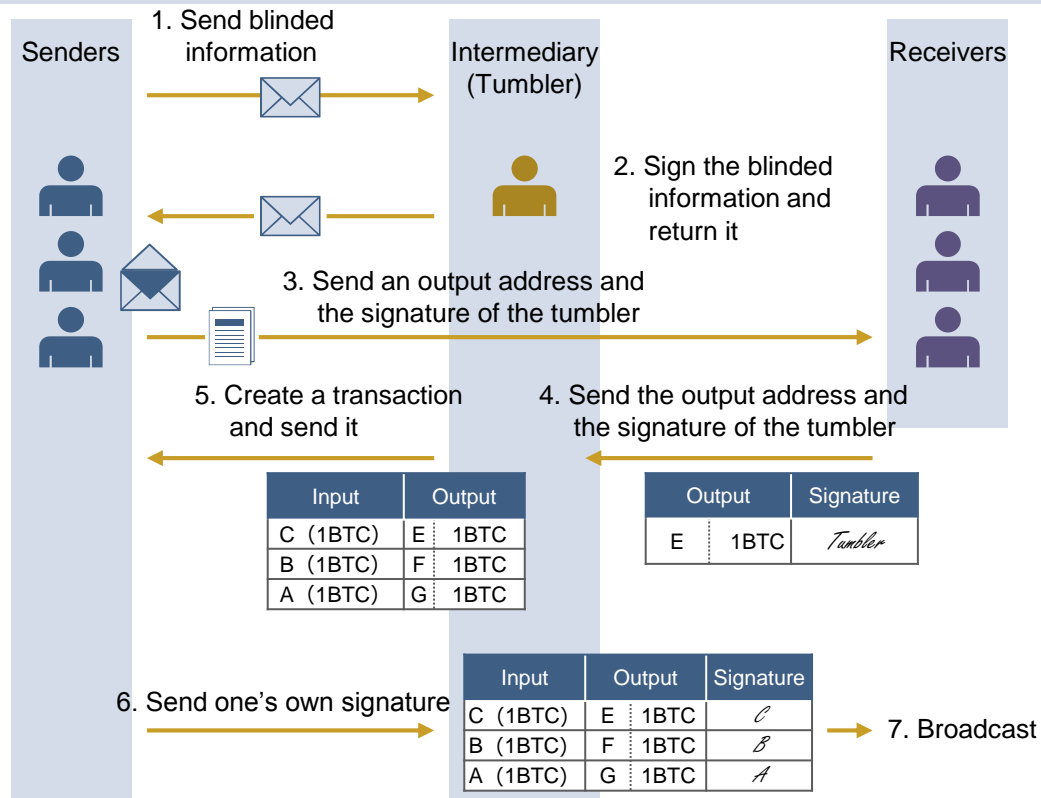
Chaumian CoinJoin obscures the actual transfer route from third parties and intermediaries, called tumblers. It uses a signature method called a blind signature that does not require contents to be revealed. It is supported by some wallets such as the Hidden Wallet, Wasabi Wallet, and the Samourai Wallet.

1. The sender sends transfer information to an intermediary (tumbler). As the output address is blinded, the tumbler can not see it.

2. The tumbler confirms that the input address is an unused one, and signs the blinded output address before returning it to the sender.

3. The sender then unblinds the output address and the signature of the tumbler, and sends them to the receiver.

4. The receiver sends the output address and the signature of the tumbler back to the tumbler.

5. The tumbler confirms that his/her signature is present. He/she creates a transaction using the input address obtained at Step 1 and output address obtained at Step 4, and sends it to the sender.

6. The sender confirms the content of the transaction and sends his/her signature to the tumbler.

7. The tumbler adds the received signature to the transaction and broadcasts it to the blockchain network.

# 3.2.1.1.2 Mixing – Challenges and new initiatives

Since the approach of mixing crypto-assets requires tradeoffs concerning anonymity and convenience, there is a possibility that this mixing process may anonymize transaction contents and the existence of the transactions themselves.

Challenge	Content	New initiative
Tradeoff between anonymity and convenience	• It is important to accumulate a sufficient number of users to increase anonymity. (Reports indicate that mixing is vulnerable against active attacks where coins are sent and then tracked). • On the other hand, increasing the number of users reduces usability because users need to wait for other users to join every time mixing happens.	• Monero circumvents this tradeoff by using dummy senders (Ring Signature) instead of mixing.
Tradeoff between anonymity and risk of being identified	• Increasing the number of users in order to increase anonymity also increases the possibility that the use of mixing will be found out by a third party.	• CoinJoinXT may be able to resolve this tradeoff by dealing in transactions that carry out mixing outside of the blockchain (off-chain). • Tumblebit circumvents this tradeoff by separating the coins for deposit and withdrawal instead of mixing them.
Tradeoff between anonymity and transaction size	• Increasing the number of users in order to increase anonymity also increases the transaction size. Due to transaction size limits, the maximum number of anonymity set in a single Bitcoin transaction is around 350-470.	Partially resolved • Schnorr signatures (introduced to several crypto-assets such as Grin and Beam) have alleviated this tradeoff to some extent by combining multiple signatures as well as public keys, but this problem has not been completely resolved.
Tradeoff between anonymity and convenience	• The transfer amount needs to be as uniform as possible to increase anonymity.	Resolved • ValueShuffle (introduced to the crypto-asset Stegos) resolved this tradeoff by encrypting transfer amounts.
Custody risk	• Custody risk exists when it comes to centralized mixing because intermediaries (mixers) hold the private keys of users.	Resolved • This problem has been resolved by using decentralized mixing such as CoinJoin.
Single point of failure	• Intermediaries are single points of failure in mixing that relies on such intermediaries.	Not important in practice • Except for with centralized mixing, since intermediaries do not hold the private keys of users, users can switch to other intermediaries if problems arise in one particular intermediary.

51

3.2.1.1.3 Stealth Address

Stealth addresses anonymize a receiver's actual address from third parties even if the receiver needs to publish his/her address for donation purposes etc. This anonymization method has been adopted by Monero. Although the representative address is published, the actual receiver's address is a randomly generated one-time address every time.

Remittance process using a stealth address
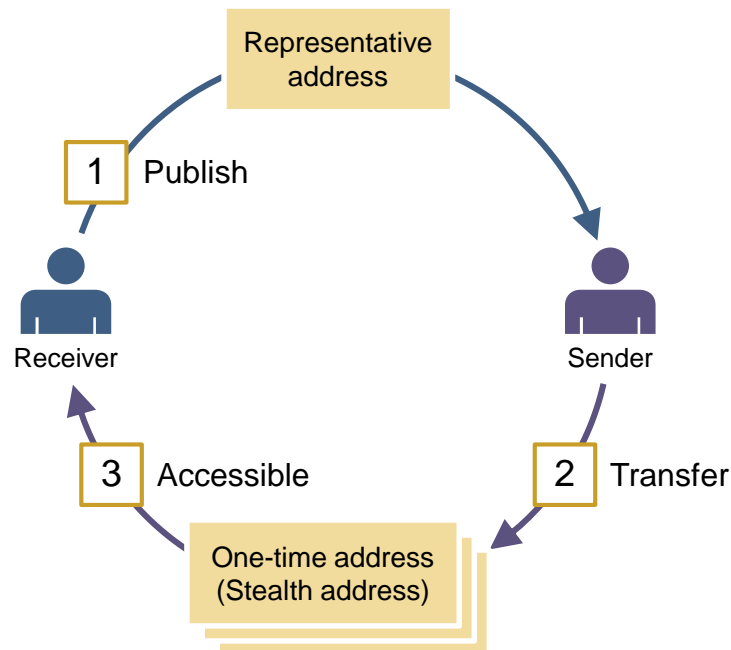
1. The receiver publishes two public keys **A** and **B.**

2. The sender creates a one-time address by using (i) two public keys, **A** and **B**, and (ii) his/her own private key **r**. He/she then sends coins to the address including the public key **R** that corresponds to his/her private key **r** in the transaction.

3. The receiver creates a private key that corresponds to this one-time address using (i) his/her private keys **a** and **b**, that corresponds the public keys **A** and **B**, and (ii) the sender's public key **R**. The coins sent to the one-time address will be able to be accessed when the created private key is used.

Using a one-time address that is only available for the receiver also requires the cooperation of the sender. Stealth addresses use the Diffie-Hellman key exchange that creates a common key shared by both the sender and the receiver.

3.2.1.1.3 Stealth Address – Challenges and new initiatives

The overall problems related to stealth addresses have already been resolved. Although they have been not adopted by Bitcoin, they are supported by some other wallets such as Samourai Wallet and BillionApp because they can be immediately introduced without any major protocol modifications.

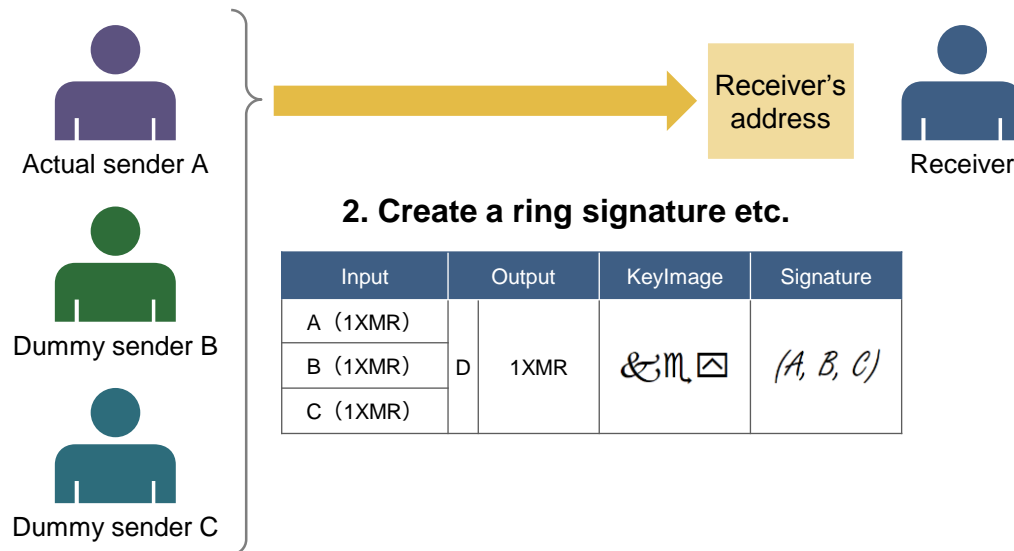| Challenge	Content	New initiative
Necessity of use	• A receiver can gain the same benefits every time he/she creates a stealth address to receive coins.	• Mimblewimble circumvents the use of stealth addresses since every transfer requires the cooperation of both the sender and receiver, making identifiers such as addresses unnecessary.
Necessity of confirming payments	• The receiver is not notified of the generated address. To confirm payments, he/she must (1) get a message from the sender, or (2) investigate every transaction on blockchain data by him/herself or a trusted third party.	–
Reuse of private keys	• The original proposal used a single public key for the representative address raising security concerns as the private key should be used to confirm payments.	Resolved • An method using two public keys, one for confirmation of payments and another to use sent coins, has been introduced. With this method, the receiver can entrust the confirmation of payments to a third party by depositing a private key that cannot be used to directly access the coins.

3.2.1.1.4 Ring Signature

Ring signatures make a sender anonymous to third parties and have been adopted by Monero. They anonymize the actual sender by including dummy senders.

A unique value generated from the private key of the actual sender (called a Key Image) is included in each transaction to prevent double spending attacks.

Remittance flow using a ring signature

1. Select no. of dummy senders

Actual sender A

Dummy sender B

Dummy sender C

2. Create a ring signature etc.

Input		Output	KeyImage	Signature
A（1XMR）				
B（1XMR）	D	1XMR	&ℳ☒	(A, B, C)
C（1XMR）				

3. Accessible

Receiver's address

Receiver

1. The sender selects a number of dummy input transactions that have the same transaction amount and creates transaction **X** that includes both the dummy and the actual input transactions.

2. The sender creates a key image from the private key of the actual input transaction and puts it in transaction **X**. He then creates a ring signature from transaction **X**, the private key, and the public keys from the dummy input transactions and broadcasts transaction **X**.

3. The receiver can use the coins sent to his address but no one else can distinguish the actual input from the other input transactions.

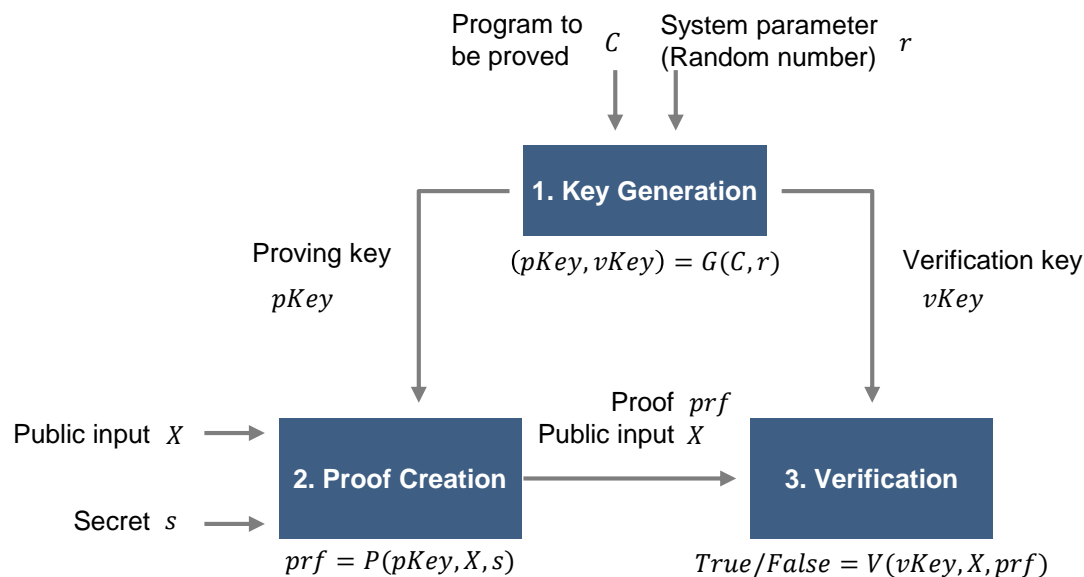# 3.2.1.1.4 Ring Signature – Challenges and new initiatives

Selecting the right dummy senders is quite important when using a ring signature, and it is necessary to choose dummies that have attributes that are as similar to those of the actual sender as possible.

Challenge	Content	New initiative
Attributes of dummy senders	• The actual sender could be discovered due to the following dummy sender biases: ✓ Chronological bias 　Since dummy senders that have been used in the past are likely to be used many times afterwards, the actual sender is likely to be the most recent one. ✓ Transaction bias 　Since it is rare for dummy senders to be selected from a single transaction, those that are are likely to be the actual ones.	Partially resolved • It has been reported that chronological biases can be resolved by changing the sampling distribution that choose dummies. However, this proposal has not been adopted by Monero at the time of writing.
Tradeoff between anonymity and transaction size	• Monero has increased the minimum number of dummy senders several times in order to increase anonymity. However, increasing the number of users also increases the transaction size.	Partially resolved • Schnorr signatures (introduced to several crypto-assets such as Grin and Beam) have alleviated this tradeoff to some extent by combining multiple signatures as well as public keys, but this problem has not been completely resolved.
Number of dummy senders	• In the initial release of Monero, most of the transactions did not include dummy senders so 95% of actual senders were able to be identified.	Resolved • Monero has increased the minimum number of dummy senders several times. The minimum number is 10 at the time of writing (v0.13.0.4).

3.2.1.1.5 Zero-Knowledge Proof (zk-SNARKs)

Zero-knowledge proofs are methods where a prover assures a verifier that the prover knows a secret without revealing said secret to the verifier. zk-SNARKs, or Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, are variants of zero-knowledge proofs and are adopted by Zcash and Ethereum. Based on a homomorphic encryption that allows the computation of encrypted data, zk-SNARKs anonymize actual transaction content from third parties by recording proofs instead of the actual transaction contents (senders, receivers, amounts etc.) on blockchain data.

Remittance flow using zk-SNARKs

Program to be proved C System parameter (Random number) r

1. Key Generation

$$(pKey, vKey) = G(C, r)$$

Proving key $pKey$

Verification key $vKey$

Public input X

Secret s

2. Proof Creation

$$prf = P(pKey, X, s)$$

Proof prf
Public input X

3. Verification

$$True/False = V(vKey, X, prf)$$

1. A trusted third party creates a proving key (*pKey)* and a verification key (*vKey)* by using the program to be proved (a Boolean-valued function) and the system parameter *r.* The created *pKey* and *vKey* are then published publicly.

2. The prover creates a proof *prf* by using the proving key *pKey*, the public input *X*, and the secret input *s*.

3. The verifier verifies the proof *prf* by using the verification key *vKey* and the public input *X*.

The prover refers to both the sender and the receiver of the remittance, and the verifier refers to miners and relay nodes. In Ethereum, the smart contract that is available only supports verification at Step 3. Therefore, Step 3 is processed on-chain while Steps 1 and 2 are processed off-chain.

3.2.1.1.5 Zero-Knowledge Proof (zk-SNARKs) – Challenges and new initiatives

A lot of work has been put into overcoming well-known limitations where system parameters created at the time of key generation cannot to be leaked and improvements have mainly focused on reducing the amount of calculations necessary. In Ethereum, zk-SNARKs are also expected to improve scalability.
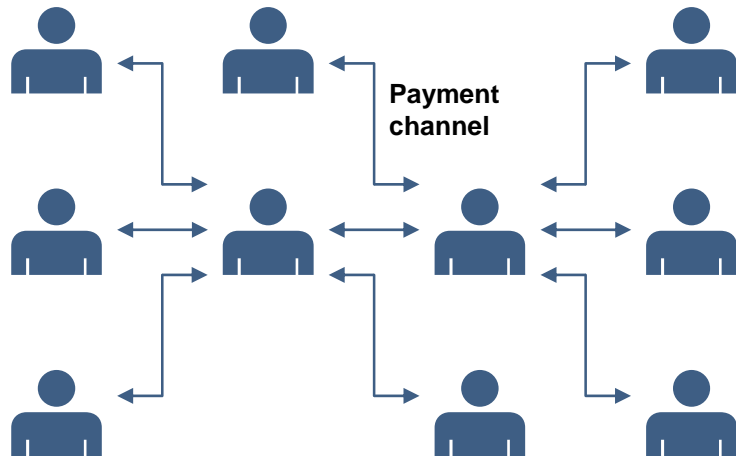
Challenge	Content	New initiative
Necessity of use	• Off-chain processing gives one the same benefits as zk-SNARKs. ✓ zk-SNARKs have been developed based on blockchain-specific constraints; for example, both a sender and a receiver cannot communicate with miners (non-interactivity is needed) and the cost of recording a transaction on blockchain data is expensive (succinctness is needed). Therefore, the optimal solutions could change as the constraints change.	• Quorum developed by JP Morgan has worked around the use of zk-SNARKs by using another approach – only a hashed value of encrypted transaction content is recorded as blockchain data and each node sends the actual transaction off-chain.
Necessity of key generation by trusted third parties	• Key generation must be conducted by trusted third parties. A fake proof could be generated without knowing the secret input s if the parameter r mentioned in the previous slide is leaked. This process of key generation is often called a "trusted setup". • A trusted setup should be conducted every time the content to be anonymized (the program C in the previous slide) changes. This constraint causes problems in practice when zk-SNARKs are applied to various problems.	Partially resolved • zk-STARKs, or Zero-Knowledge Scalable Transparent ARguments of Knowledge", resolved the following problems, but have raised other problems such as increases in size of the proof data (in some cases increases of over 200 times the original amount).
Amount of calculation and the size of the proof data	• The more complicated the problem (the program C from the previous slide), the more time is needed to calculate the proof data.	✓ Leaked parameters cause no problems. ✓ The complexity of the problem has less effect on calculation times.
Quantum-resistance	• Elliptic curve cryptography that makes use of the difficulty of the discrete logarithm problem is not quantum-resistant.	✓ zk-STARKs are quantum-resistant using collision-resistant hash functions.

3.2.1.1.6 Lightning Network

Lightning network mechanisms bring about improved scalability to blockchain networks, immediate settlements, and the reduction of transaction fees etc. They are used for Bitcoin and Litecoin. In particular, they minimize transactions that are recorded as blockchain data, and most of the actual transactions are exchanged off-chain.

Lightning network flowchart	Illustration of a "trustless" situation

Only the first and last transactions are recorded as blockchain data: the transaction history in between is not recorded. However, transactions exchanged off-chain have a limit on the amount of coins that can be initially deposited. Also, users have to wait until the first transaction is included in a block.

As there are no intermediaries to prevent acts of fraud between mutual parties, the party who committed the fraud is penalized: the entire initial deposit amount is forfeited to the other party.

3.2.1.1.6 Lightning Network

Lightning networks make it possible to make a transaction between any parties that do not have a directly open payment channel, and is a mechanism that enables off-chain transactions between any two parties by combining multiple payment channels.
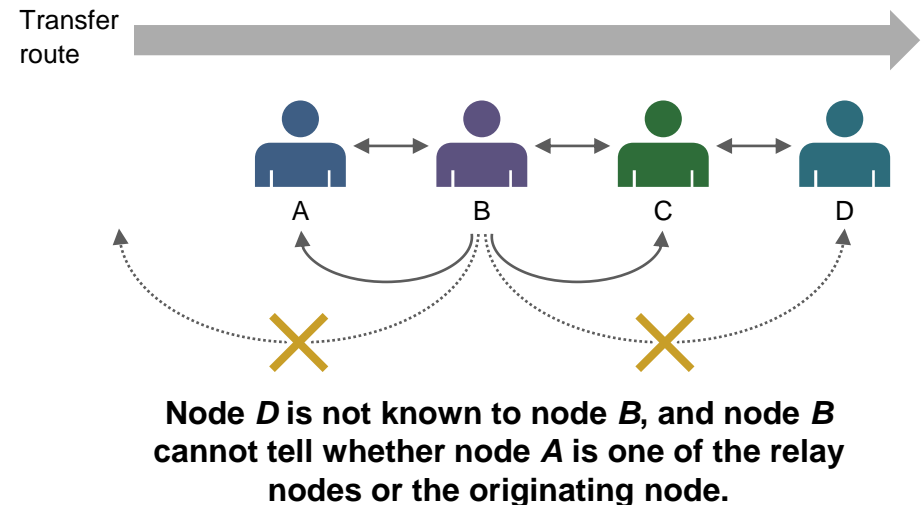
Illustration of lightning network relay transfers	Relay transfers and privacy

It is possible for trade to occur between any two parties by combining multiple payment channels. However, since transaction fees depend on the number of relays, a node with many payment channels attracts further payment channels, resulting in those nodes becoming hubs.

According to the current specifications, a mechanism similar to that of onion routing "Tor" (see Section 3.3.1.3) is outlined concerning the relay transfer of lightning networks. That is, only the nodes before and after the remittance are known to each node. Therefore, the more the number of relay nodes increases, the more the anonymity increases. (the transfer route is determined by the sender.)

Payment channel

Transfer route

A   B   C   D

Node *D* is not known to node *B*, and node *B* cannot tell whether node *A* is one of the relay nodes or the originating node.

3.2.1.1.6 Lightning Network – Challenges and new initiatives

The so-called second layer technology that uses off-chain techniques is characterized by a faster progress rate than that of on-chain technology corresponding to the base layer of blockchain. New proposals are being actively developed and were included in the specifications from a rather early stage.

Challenge	Content	New initiative
Presence of hub nodes	• When a specific node holding a large amount of coins becomes a hub and dominates the payment channels, the failure of and any attack on that hub node will damage the stability of the entire network.	–
Routing	• It is challenging for a sender to choose the optimum transfer route when there is a large number of payment channels although there are no specific entities that manage all the routes.	–
Economic incentives of relay nodes	• There is a concern that relay nodes earn little or no profits as they have to pay an initial deposit that cannot be used for any other purpose while only receiving a small amount of the transaction fee.	–
Efficiency in the use of liquidity	• Deposited coins can only be used for settlement within payment channels and cannot be used for ordinary settlements in the base layer of the blockchain, so users' liquidity will be divided between on-chain and off-chain.	Partially resolved • A method, called Splicing, that retrospectively updates the capacity of the payment channel has been proposed.
Capacity (limit of transaction amount)	• A trade amount cannot exceed that of the first deposit (capacity). In particular, in the case of relay transfers, trading cannot exceed the lowest maximum capacity of the combined payment channels.	Partially resolved • Atomic Multi-Path Payments, a method that uses multiple routes to transfer coins that total a full trade amount, have been proposed. They are scheduled to be introduced in the upcoming specifications at the time of writing.

3.2.1.1.6 Lightning Network – Challenges and new initiatives

Challenge	Content	New initiative
Necessity of monitoring and backup/recovery	• Each party must always monitor the blockchain network to prepare for any kind of fraud from the other party. Furthermore, every party needs to be able to properly backup and then recover the payment channels in case there is a failure.	Partially resolved • Many methods to resolve this have been proposed: for example, "Watchtower" that allows the monitoring of the network to be delegated to others, "Data Loss Protection" that allows backup/recovery, and "eltoo" that relaxes punishments of any fraud committed. Some wallets support Watchtower and these other methods.
Griefing attacks during relay transfers	• There is a possibility that the final recipient or a relay node will carry out a harassment attack that delays the processing of nodes within the transfer route by not disclosing secrets (a value to be hashed) and not receiving relayed assets. Victim nodes cannot use liquidity until it is refunded.	Resolved • This problem has been resolved by the Ripple Interledger Protocol, by repeating transfers of small amounts many times. When any node receives a griefing attack, it is able to immediately close the payment channel.
Privacy concern related to relay transfers	• In the case of relay transfers, the same hash value and secret for each payment channel on the transfer route need to be used. This means that a malicious third party can make estimations about the transfer route by using these hash values and secret.	Not important in practice or resolved • This problem has been resolved by encrypting the packet data as Tor Onion Routing does. • Furthermore, other solutions have been proposed: "Multi-Hop Locks" that use different hash values and secrets for each payment channel in a transfer route, and "Scriptless Script" that embed hash values and secrets into signatures.

3.2.1.1.7 Atomic Cross-Chain Swap

Atomic cross-chain swaps are mechanisms for exchanging crypto-assets across two different blockchain networks on a peer-to-peer basis without any intermediaries nor any physical connection between them. They are used by Bitcoin and Litecoin. Atomic cross-chain swaps are carried out by delivering mutual crypto-assets using a technique called a "Hashed Timelock Contract".

Illustration of an Atomic Cross-Chain Swap	Illustration of a Hashed Timelock Contract

By using this atomic cross-chain swap for both Bitcoin and Litecoin, the risk of the Litecoin (or Bitcoin) payment failing to be delivered despite the delivery of the Bitcoin (or Litecoin) one is eliminated.
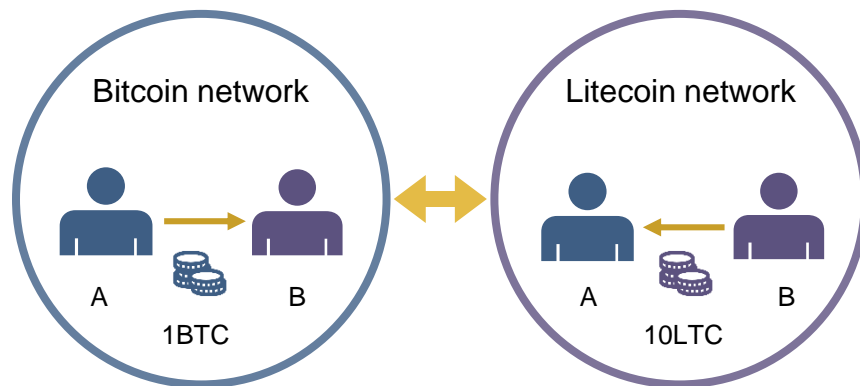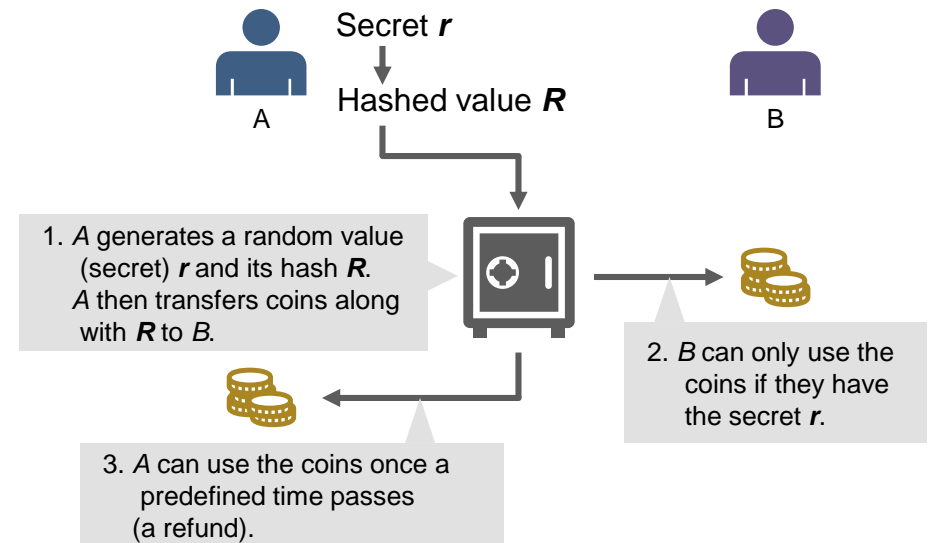
A Hashed Timelock Contract enables there to be conditional payments by combining a hash function and a time lock function. A similar concept is also used in Lightning networks, the Ripple Interledger Protocol etc.

Bitcoin network

Litecoin network

A   B

A   B

1BTC

10LTC

Secret *r*

Hashed value *R*

A   B

1. *A* generates a random value (secret) *r* and its hash *R*. *A* then transfers coins along with *R* to *B*.

2. *B* can only use the coins if they have the secret *r*.

3. *A* can use the coins once a predefined time passes (a refund).

3.2.1.1.7 Atomic Cross-Chain Swap

Both parties can cancel a transaction at any time.

Atomic Cross-Chain Swap flowchart

■ Bitcoin network

■ Litecoin network

A	B

B	A

Generates a random value *r*, and its hash *R*

TX 1

Input	Output		Signature
A	B if *r* is provided	1BTC	*A*
	A if 2 hours pass		

→ Verification →

TX 2

Input	Output		Signature
B	A if *r* is provided	10LTC	*B*
	B if 1 hour passes		

→ Verification

TX 4

Input	Output		Secret	Signature
TX 1	B	1BTC	*r*	*B*

1BTC is available to *B*

← *r* is obtained from TX3 ←

TX 3

Input	Output		Secret	Signature
TX2	A	10LTC	*r*	*A*

10LTC is available to *A*

*The locking time can be any amount of time but in these examples, we have used two hours and one hour.

3.2.1.1.7 Atomic Cross-Chain Swap – Challenges and new initiatives

Many parts of the development of atomic cross-chain swaps and lightning networks overlap since they both use the same "Hashed Timelock Contract". Although current efforts mainly focus on improving privacy, ensuring atomicity and shortening processing times are also seen to be important in practice.

Challenge	Content	New initiative
Ensuring atomicity	• Only in the case of the last transaction not being sent (in the previous slide, the last transaction of *B* is not sent), will atomicity not be ensured. Atomicity refers to indivisibility. Atomic operations either have both deliveries carried out fully or not at all.	• A method has been proposed where the sending of the last transaction is delegated to a trusted third party.
Necessity of monitoring	• Both parties need to monitor the blockchain network at all times to make sure that the other party is following predetermined procedures.	–
Efficiency of processing times and the use of liquidity	• In order to confirm that transactions are not canceled, both parties need to wait a significantly long time for each transaction. If transactions are canceled, both parties also need to wait for a certain amount of time before receiving a refund. • As coins cannot be used for other transactions during a trade, the efficiency of liquidity decreases.	Partially resolved • It has been proposed that atomic cross-chain swaps be used on lightning networks. The time needed to confirm the cancelation of a transaction become shorter but it still takes time to open new payment channels and to complete a refund.

3.2.1.1.7 Atomic Cross-Chain Swap – Challenges and new initiatives

Challenge	Content	New initiative
Available blockchain	• Both blockchains need to have a "Hashed Timelock Contract". Also, blockchain data needs to be disclosed to all participants.	Partially resolved • BarterDEX uses Multisignatures instead of "Hashed Timelock Contracts". However, at least one of the blockchains needs to have a "Hashed Timelock Contract".
Privacy concerns	• Since the same secret (a value to be hashed) and hash value for each blockchain network needs to be used, a malicious third party may be able to connect the transactions from both blockchain networks.	Resolved • This problem is resolved by embedding hash values and secrets into signatures: a process called "Scriptless Script". "Scriptless Script" uses Schnorr signatures (in 2017) or ECDSA (in 2018), but it has not been adopted by any crypto-assets as of yet.
Option contract	• As both parties can cancel or continue a transaction at any time, meaning that a trade can be carried out at any time before the deadline at the market price, atomic cross-chain swaps are considered to have an American call option. If this characteristic is not reflected in the trade rate, the transaction becomes disadvantageous for the seller.	Not important in practice or resolved • It has been proposed that a buyer of an option will be penalized if he/she cancels the transaction by making them put up something as collateral.

3.2.1.1.8 Mimblewimble

Mimblewimble is a piece of technology designed to make blockchain data compactable and quickly verifiable. It also anonymizes transaction content and hides the existence of transactions themselves by not recording unnecessary transactions within blockchain data. It is adopted by the crypto-assets Grin and Beam. The mechanism behind Mimblewimble is quite different from that of traditional crypto-assets such as Bitcoin. Remittances with Mimblewimble do not require addresses but the cooperation of the senders and receivers.

Mimblewimble transactions	Discarding unnecessary transactions

Transaction amounts are put into a locked "safe", called a "Pedersen commitment", and are not visible externally. A transaction can be conducted without revealing the secret in the "safe". A value transfer is achieved using cryptographic techniques and without using any addresses.

Unnecessary transactions are discarded and signatures are aggregated by a mechanism, called "Transaction Cut-Through". In the figure below, transactions containing c2 and c3 are not recorded on blockchain data.

Bitcoin transactions

Input	Output		Signature
A's UTXO	B's address	3BTC	*B*

Actual transactions

Mimblewimble transactions

Input	Output	Signature
🔒 c1	🔒 c2	s1 = signature signed by a private key corresponding to (c2 – c1)
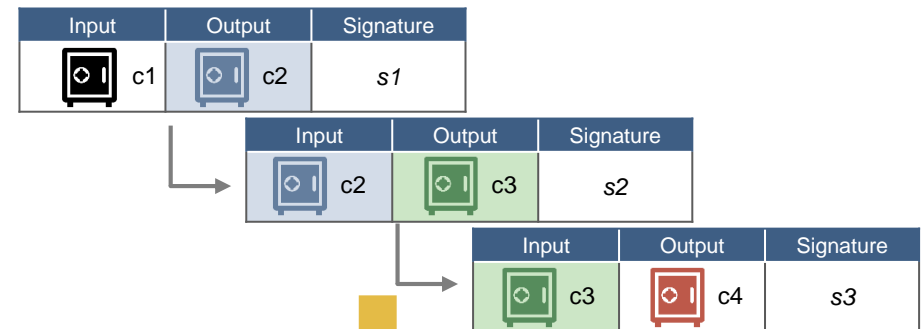
Transactions recorded as blockchain data

Input	Output	Signature
🔒 c1	🔒 c4	s1 + s2 + s3

* In current implementations such as in Grin, signatures are created with the cooperation of senders and receivers, and they are not aggregated.

3.2.1.1.8 Mimblewimble – Challenges and new initiatives

Grin and Beam were launched in January 2019. A variety of new problems are expected to arise as the number of users increases.

Challenge	Content	New initiative
Script function	• Mimblewimble does not have script functions, or smart contracts, that are adopted by Bitcoin.	Partially resolved • Several functions are realized by embedding hash values and secrets into signatures ("Scriptless Script"). • Grin's timelock function of "Hashed Timelock Contract" uses transaction functions instead of script functions.
Usability	• Every remittance with Mimblewimble requires the cooperation of senders and receivers. Since the remittance process is quite different from usual payments, it is difficult to predict whether the processes required will be accepted by many users.	–
Quantum-resistance	• Since the Pedersen commitments are not quantum-resistant, a malicious user can generate any amount of coins arbitrarily and see the transaction contents.	Partially resolved • Grin and Beam prevent the arbitrary generation of coins by using Switch commitments that enable both quantum-resistant Elgamal commitments and the current Pedersen commitments. However, the problem of the transaction amounts being visible has still not been resolved.
Side effect of anonymizing transaction amount	• If Lightning networks are combined with Mimblewimble, calculating optimal routes may be problematic as the transaction amounts are made anonymous to any third party.	–

3.2.1.1.9 Schnorr Signature

Schnorr signatures are a form of digital signature that, like ECDSA, are based on the difficulty of the discrete logarithm problem and they have been adopted by Grin and Beam. Since multiple signatures and public keys can be aggregated, Schnorr signatures are expected to (1) reduce the size of blockchain data and (2) anonymize the transaction content and the number of involved parties. Schnorr signatures can be introduced to Bitcoin as backward-compatible "soft-forks".

Illustration of the reduction of blockchain data	Illustration of the anonymization of transaction contents

As Schnorr signatures can aggregate multiple public keys and signatures, (1) multisignatures can be represented as a single normal address, and (2) coins sent to the multisignature address can be made available by using a single signature. The amount of blockchain data can be reduced through the aggregation of public keys/signatures.

Input	Output		Signature	Script
UTXO sent to the multisignature address of *A* and *B*	D	1BTC	$\mathcal{A}$ $\mathcal{B}$	Script itself including two public keys of A and B

Input	Output		Signature
P	D	1BTC	$\mathcal{A} + \mathcal{B}$

P is the address generated from the public key that was aggregated using two public keys from both *A* and *B*.

A method called Taproot has been proposed that replaces multiple payment conditions with a single public key by using Schnorr signatures. Taproot improves privacy by minimizing payment conditions as no payment conditions are recorded as blockchain data when coins are sent, and only one fulfilled condition is recorded.

Input	Output		Signature	Public key
A	Multisignature address of A and B	1BTC	$\mathcal{A}$	A
	A if 1 hour passes			

Input	Output		Signature	Public key
A	P	1BTC	$\mathcal{A}$	A

P is the address generated from the public key that is aggregated from multiple payment conditions.

3.2.1.1.10 Dandelion

Dandelion is a protocol that anonymizes the originating node of a transaction on a P2P network and has been adopted by Grin and Zcoin. A transaction is broadcast after being relayed a random amount of times by randomly selected nodes.

The process of Dandelion

Originating node

→ Relay phase (Stem phase)

→ Broadcast phase (Fluff phase)
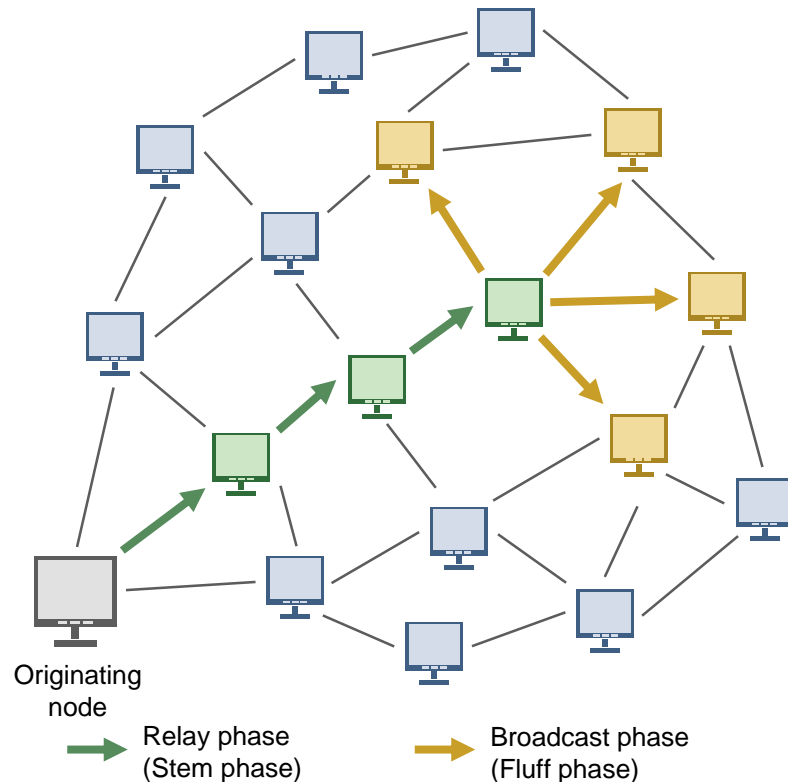
Dandelion anonymizes the actual originating node by having another node broadcast a transaction. Three steps are predominantly used: the creation of transfer routes, relay of the transaction and its broadcast.

1. Each node randomly selects a subset of outbound nodes. The subset is updated every 10 minutes.

2. The originating node randomly selects a relay node and sends a transaction to it. Each relay node chooses whether to relay or broadcast the transaction with a 90/10 probability. This step is called the "Stem" phase.

3. When the relay node selects a broadcast, or when the expiration date set randomly for each node has passed, the node broadcasts a transaction. This step is called the "Fluff" phase and the transaction is propagated to the entire network.

Grin combines both Mimblewimble and Dandelion. When each node relays a transaction, multiple sent transactions are aggregated into a single transaction using "transaction cut-through" techniques. Because of this, some transactions are completely discarded during relays of each node.

3.2.1.1.11 Anonymous altcoins

Crypto-assets that adopt anonymization technologies with every remittance are often called anonymous altcoins and examples include Dash, Monero and Zcash.
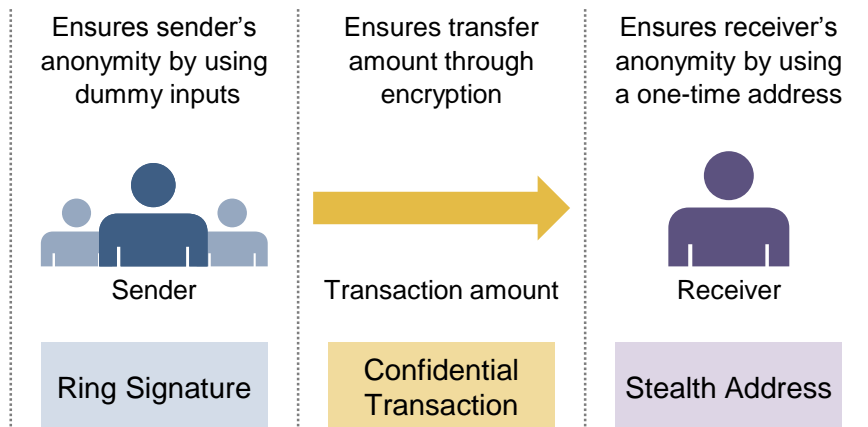
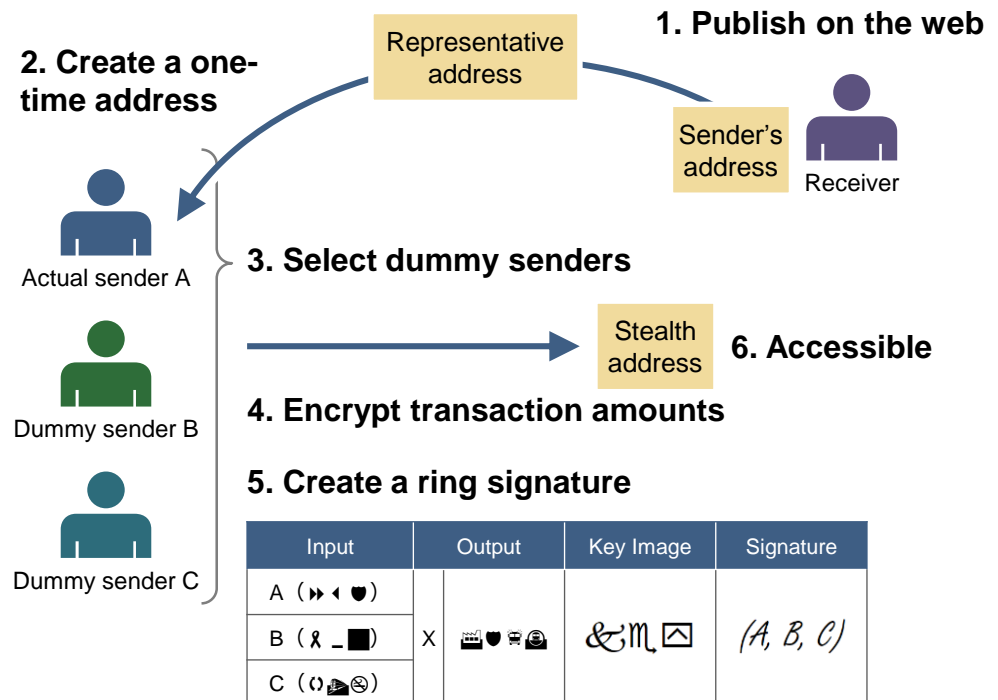| Altcoin	Launch date	Technology	Characteristics
Dash	Jan 2014	Mixing ("PrivateSend")	• Mixing is performed only when specified by the user(s). 　➢ The user(s) activate(s) a function called "PrivateSend". 　➢ When three users who have activated "PrivateSend" come together, mixing is done several times based on four different types of amounts (0.01/0.1/1/10 DASH). • However, it must be noted that transaction content (senders, receivers, and amounts) is not anonymized.
Monero	Apr 2014	Stealth Address, Ring Signature ("RingCT")	• Ring signatures that anonymize senders, Stealth addresses that anonymize receivers, and Confidential transactions (CT) that anonymize transaction amounts are used without being specified by the user(s). 　➢ Stealth addresses use one-time addresses as a remittance destination. 　➢ Ring signatures use dummy senders of the same amount for every remittance, anonymizing the actual sender(s). 　➢ Confidential Transactions use encryption to anonymize transaction amounts.
Zcash	Oct 2016	Zero-Knowledge Proof ("zk-SNARKs")	• zk-SNARKs are used to anonymize all transaction content (e.g. senders, receivers, amount) only when specified by users. It is pointed out that zk-SNARKs are more confidential than mixing, ring signatures etc. 　➢ Addresses of Zcash consist of invisible and visible addresses. 　➢ It is possible to designate what transaction content (senders, receivers, amount) is made anonymous using a combination of an invisible address and a visible one (there are four types of combination in total). • By using a viewing key, transaction content can be confirmed by third parties but they cannot use this key to get the crypto-assets.

3.2.1.1.11 Anonymous altcoins – Monero

There are cases where anonymization technologies are used in combination with each other. For example, Monero uses different technologies to anonymize senders, receivers and transaction amounts. Monero has actively adopted anonymization technologies that have been proposed for Bitcoin and is widely known as a major anonymous altcoin along with Zcash.

Illustration of combining anonymization technologies	Monero process flowchart

Monero uses Ring signatures to anonymize senders, Stealth addresses to anonymize receivers, and Confidential transactions to anonymize transaction amounts. The combination of Ring signatures and Confidential transactions is called "RingCT" and was activated in January 2017.

Ensures sender's anonymity by using dummy inputs	Ensures transfer amount through encryption	Ensures receiver's anonymity by using a one-time address
Sender	Transaction amount	Receiver
Ring Signature	Confidential Transaction	Stealth Address

1. Publish on the web

Representative address → Sender's address / Receiver

2. Create a one-time address

Actual sender A

3. Select dummy senders

Dummy sender B

Stealth address **6. Accessible**

4. Encrypt transaction amounts

Dummy sender C

5. Create a ring signature

Input	Output	Key Image	Signature
A (⤻◂❤)			
B (⚋_■) X	📠❤🚂☕	&m.⊠	(A, B, C)
C (◖◗📨☺)			

71

3.2.1.2 DEX

3.2.1.2.1 Overview of DEXs

3.2.1.2.2 Classification of DEXs
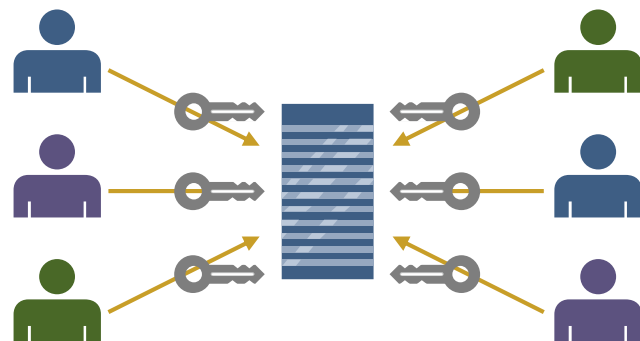
3.2.1.2.3 Major examples of DEXs

3.2.1.2.4 Challenges and new DEX initiatives

3.2.1.2.1 Overview of DEXs

Decentralized Exchanges, or DEX, are exchanges where no centralized management entities exist. They have a series of functions necessary for exchanges using peer to peer technologies; matching between sellers ("makers") and buyers ("takers"), price formation, and settling.

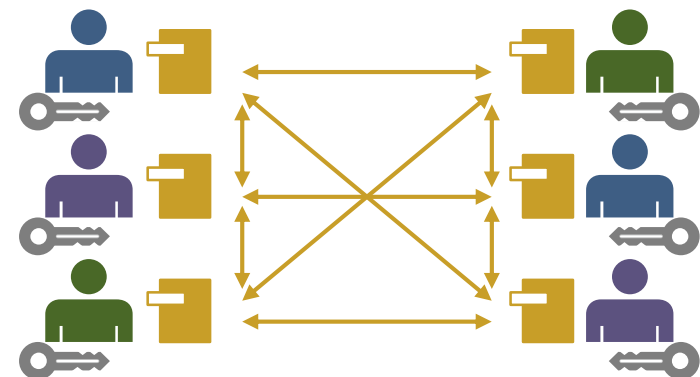| Current exchanges (centralized exchanges)	DEX (Distributed exchanges)
Users deposit their secret keys at exchanges. Users need to trust exchanges' operations such as the management of secret keys and/or servers.	Users manage the private keys by themselves. Transactions are processed via the smart contract within the blockchain data.

Elimination of custody risks

Risks are concentrated around exchanges (single point of failure, single point of trust)

Risks spread to users; there is increased transparency and availability

3.2.1.2.1 Overview of DEXs－Benefits compared to centralized exchanges

The primary benefit of DEX is that users do not suffer any losses related to centralized exchanges: for example, losses from being hacked, caused by price fixing or wash sales or due to server failure etc. Other main benefits include the following:

- Transactions are processed all the time (high availability).
- Transactions can be carried out without KYC (convenience of conducting trades, high anonymity)
- Crypto-assets not handled by a centralized exchange are tradable.

|	Centralized Exchange	DEX
Point of Failure, Point of Trust	Exchange service providers	DEX service providers or smart contracts, in many cases
Exchange of fiat currencies	Possible	Not possible, in many cases
Exchange of crypto-assets	Possible	Possible
Custody function	Provided (Exchange service providers manage users' private keys)	Not provided (Users manage their own private keys)
Liquidity management function (order book management function)	Provided	Provided, in many cases (There are some DEXs that do not provide order books and that only trade crypto-assets to users)
Usability	Good (Margin trading, stop loss orders or limit orders are available. The number of tradable crypto-assets is large.)	Not good (In many cases, margin trading, stop loss orders, and limit orders are not available. The number of tradable crypto-assets is small.)
Amount of liquidity	High	Low
Customer Identity Verification	Required	Not required, in many cases

3.2.1.2.1 Overview of DEXs – Transaction Volume

It is estimated that the transaction volume going through DEX constitutes 0.1% of the total exchange volume (as of 13th November, 2018).

Trading Volume through DEX (Nov. 13, 2018)

	Transaction volume of the previous 24 hours (excluding transactions with no fees)	Transactions of the previous seven days (including transactions with no fees)
USD	$7,413,898	$39,736,254
JPY	¥843,701,592	¥4,521,985,705

Ratio of DEX transactions of the previous 7 days (including transactions with no fees, Nov. 13, 2018)
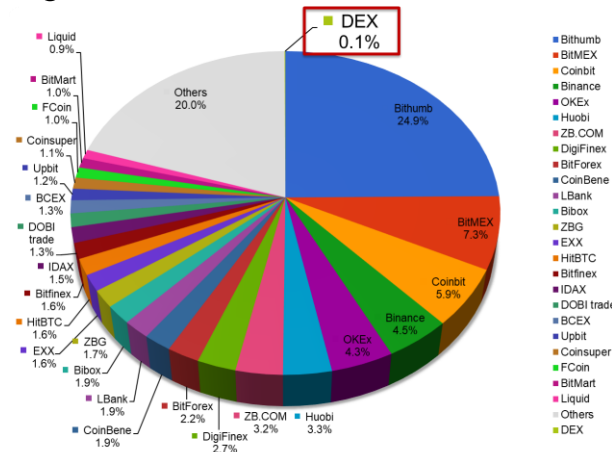
Transaction volume through DEX (Jun 2017 – Feb 2019)
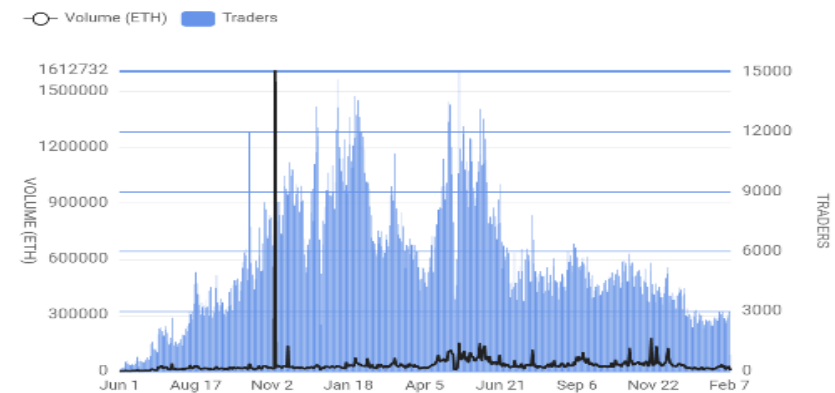
Market capitalization comparison (as of Sep. 17, 2018)

	USD	JPY	Percentage compared to Bitcoin market capitalization	Percentage compared to Ethereum market capitalization
Bitcoin	108.5 billion	12 trillion	100.00%	–
Ethereum	20.2 billion	2.3 trillion	18.61%	100.00%
0x	290 million	32.4 billion	0.27%	1.43%
IDEX(Aurora)	10 million	1.1 billion	0.01%	0.05%

(Top left, Bottom left) Created by MRI based on CoinMarketCap, coinmarketcap.com, "Top Cryptocurrency Exchanges by Trade Volume", https://coinmarketcap.com/rankings/exchanges/, Nov 13, 2018
(Top right) DEXWatch and Alethio, DEX Watch, "DEX Volume and Traders on Ethereum", https://dex.watch/, Feb 8, 2019
(Bottom right) Created by MRI based on CoinMarketCap, coinmarketcap.com, "Historical data", https://coinmarketcap.com/ Nov 13, 2018
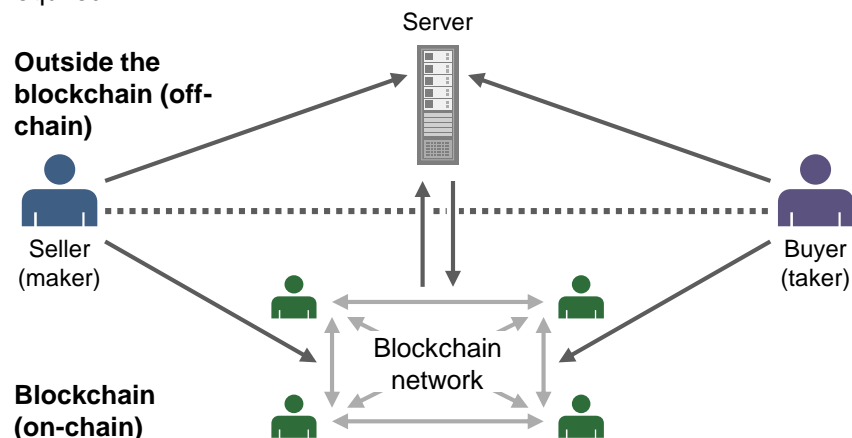
3.2.1.2.2 Classification of DEXs – Main points of classification

From a technical point of view and the viewpoint of the authorities, we have classified DEX based on two main points: the presence of off-chain processing and availability of different kinds of crypto-assets.

- The presence of off-chain processing relates to the efficiency (technologically-speaking) and identification of regulatory targets (system-related).

- Availability of different kinds of crypto-assets relates to interoperability (technologically-speaking), richness of the tradable assets (convenience) and importance of AML/CFT regulations (system-related).

Presence of off-chain processing	Availability of different kinds of crypto-assets
A specific node or entity efficiently carries out a series of processes during off-chain processing . On the other hand, off-chain processing increases security risks and the risk that a failure will occur. It also means that regulatory targets exist since specific management entities are required.	The availability of different kinds of crypto-assets including fiat currencies is important in terms of interoperability and user convenience. It also places importance on AML/CFT regulations.
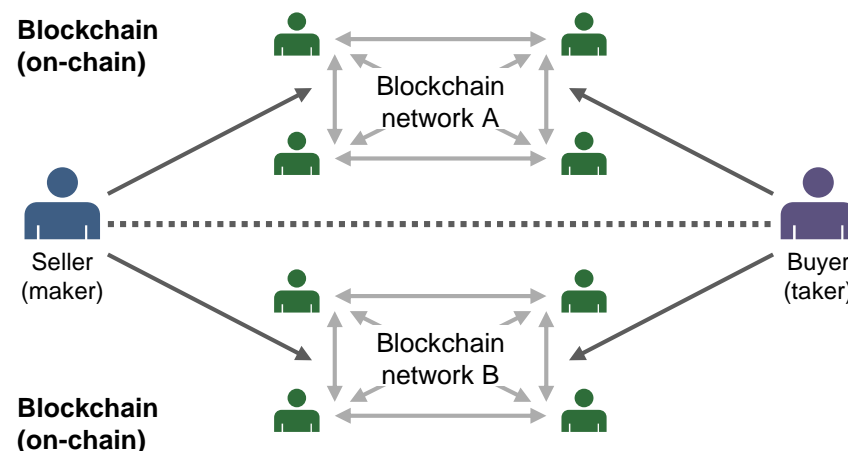
3.2.1.2.2 Classification of DEXs – List of DEXs

Each type of DEX is described in the subsequent slides.

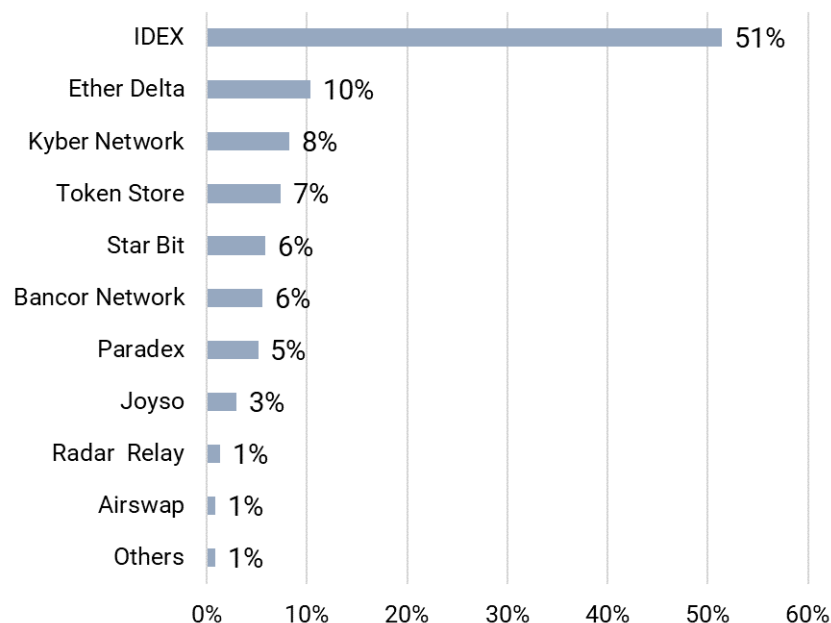| List of DEXs				
Specific management entities	Exist (The name of the management entity is shown in parentheses)		Not exist	
Kinds of available crypto-assets	Same	Different (Fiat currencies are included)	Same	Different (Fiat currencies are included)
Type of DEX	(1)	(2)	(3)	(4)
Off-chain processing content (Points of failure and points of trust)	Matching and price formation (Order book, balance information, etc.)	Settlement (Management of different crypto-assets and fiat currencies)	No	No
Examples	IDEX (IDEX Server)	OpenLedger* (OpenLedger ApS)	EtherDelta	BarterDEX
	EtherDelta (Orderbook)	CryptoBridge* (Crypto Bridge)	Bancor	BitSquare*
	0x (Relayer)	Waves DEX* (Waves Platform)	Kyber Network	Altcoin.io
	AirSwap (Indexer)			

* As far as the research was concerned, fiat currencies were tradable in theses DEXs.

3.2.1.2.2 Classification of DEXs – Major DEXs

There is a strong network affect on exchanges and liquidity is thought to attract further liquidity. These ideas can be applied to DEX as well, with a handful of DEXs handling most of the transactions.
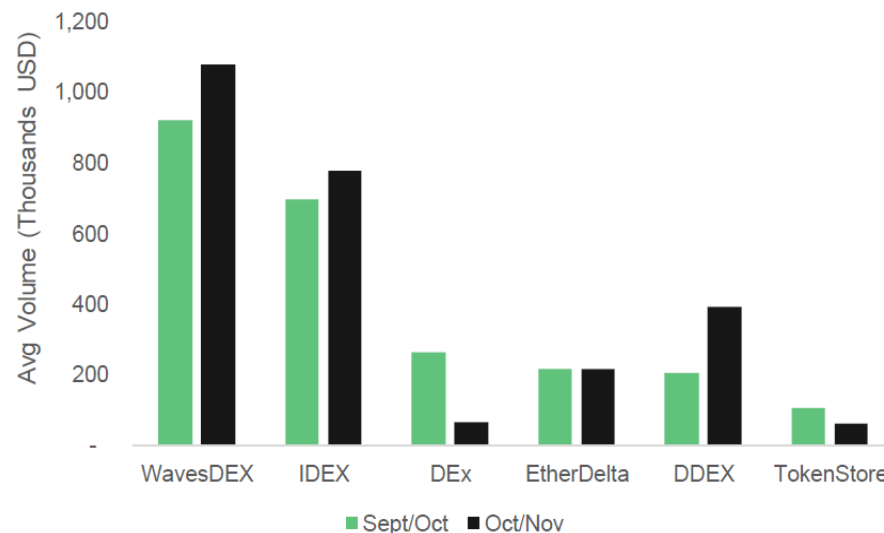
Major DEXs for ERC20 tokens (same type of crypto-assets)	Major DEXs for different crypto-assets

IDEX accounts for the majority of transactions (data from the 30 days prior to Feb. 1, 2019).

WavesDEX and IDEX account for the majority of transactions (average transaction volume every 24 hours throughout Oct 2018 – Nov 2018). The transaction volume through DEXs shown below accounted for about 0.4% of the total exchange volume.

3.2.1.2.3 Major examples of DEXs – (Type 1) management entities exist, same kind of crypto-assets only

Specific entities manage order books and balance information off-chain, and settlements are performed on-chain. The same kind of crypto-assets are available (mostly ERC20 tokens).

In general, "matching" between makers and takers and "price formations" are done through the order book managed off-chain.

IDEX flowchart

Outside the blockchain (off-chain)

INDEX Server 2b. Update of the order book
3b. Update of the order book

2a. Creation of a trade order

3a. Purchase of the trade order

Maker

Taker

1b. Update of the amount of deposited tokens

4. Order execution (settlement)

1a. Deposit

1. Deposit

IDEX smart contract

Blockchain network (Ethereum)

Blockchain (on-chain)
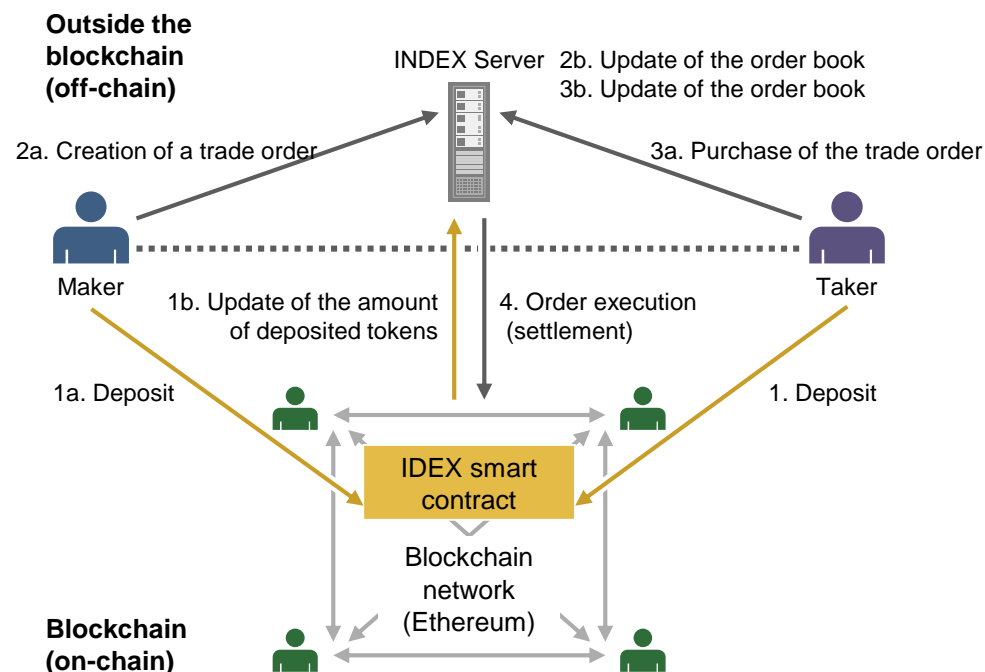
1. Both the maker and taker deposit their tokens into the smart contract.

2. The maker registers the type and amount of tokens to be exchanged within the amount of deposited tokens in the order book.

3. The taker selects an order from the order book within the amount of deposited tokens.

4. The transaction is broadcasted on the blockchain network and the settlement is processed.

Because order books and balance information are managed off-chain, IDEX has fast transaction processing, and does not charge fees for the correction or cancellation of an order.

3.2.1.2.3 Major examples of DEXs－(Type 2) management entities exist, different kinds of crypto-assets available

Specific entities manage the settlement of tokens including fiat currencies. Generally, these management entities issue tokens pegged with crypto-assets or fiat currencies and the issued tokens are then traded on a blockchain network.

"Matching" between makers and takers and "price formations" are done on-chain, while "settlements" are done both on and off-chain.

OpenLedger flowchart
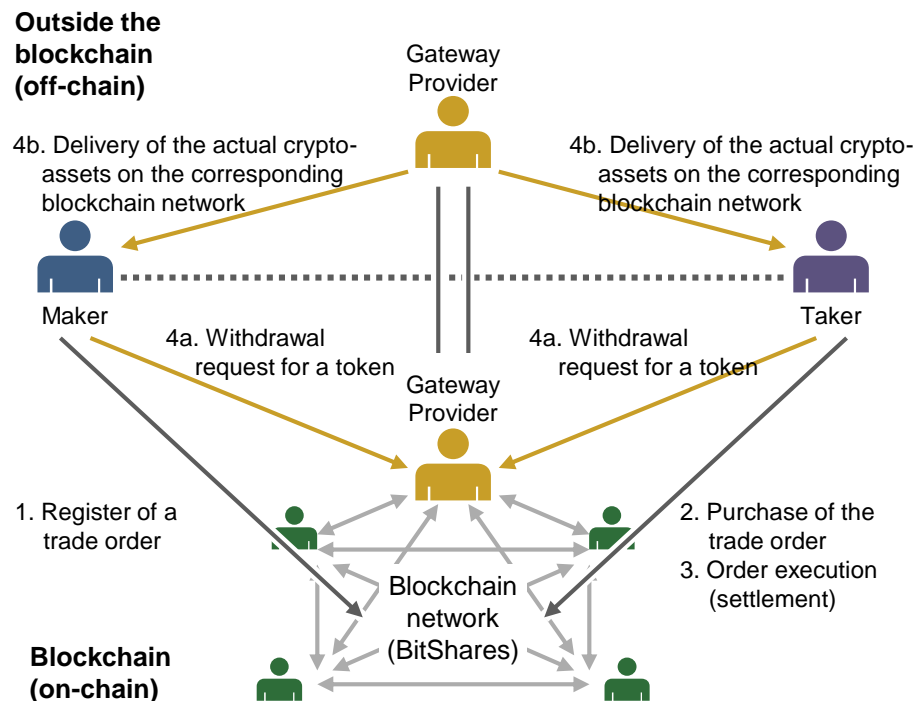
1. The maker broadcasts the sell order on the Bitshares network (The blockchain data in the Bitshares network is the order book).

2. The taker selects the desired sell order and broadcasts the response sell order. When the maker confirms the response sell order, he broadcasts the response buy order.

3. The settlement is done on the Bitshares network when both the response orders of the maker and the taker are complete.

4. Actual exchanges with different crypto-assets or fiat currencies are carried out by the gateway provider (a specific administrator) in return for the tokens on the BitShares network.
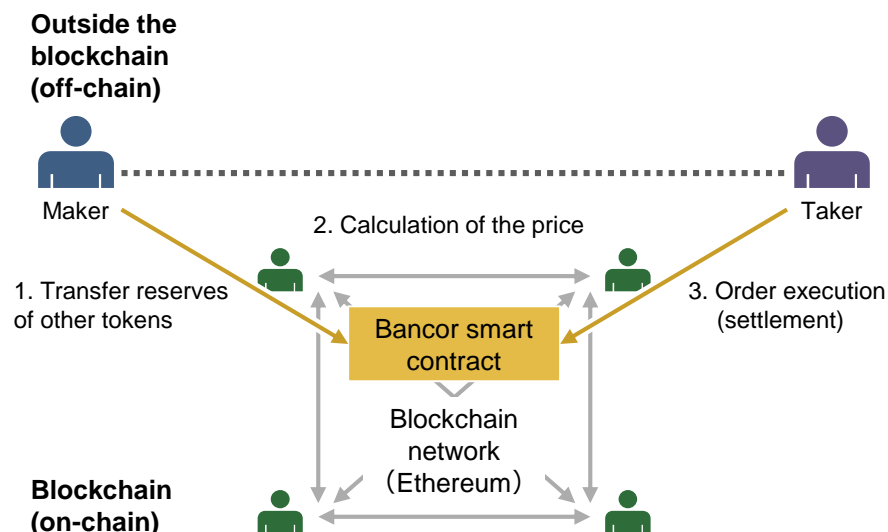
It is thought that a settlement risk exists (credit and liquidity risk) since specific entities are involved in the actual settlements.

3.2.1.2.3 Major examples of DEXs – (Type 3) management entities do not exist, same kind of crypto-assets only

There are no specific administrative entities, and "matching", "price formations" and "settlements" by the maker and the taker are all done on-chain. The crypto-assets handled are limited to the same kind of tokens (mostly ERC20 tokens).

In general, only the sales office transactions are carried by the smart contract, and are done without the interposition of a particular management subject.

Bancor flowchart

Outside the blockchain (off-chain)

Maker

1. Transfer reserves of other tokens

2. Calculation of the price

Taker

3. Order execution (settlement)

Bancor smart contract

Blockchain network (Ethereum)

Blockchain (on-chain)

1. The issuer of a particular token becomes a maker. the maker transfers reserves of other tokens to Bancor.

2. Bancor calculates the theoretical price of the token using the total amount of the tokens and reserves etc. The taker purchases or sells the token at that price.

3. The theoretical price is revised each time a taker purchases or sells tokens.

Bancor is aiming to eliminate fraud by removing people and addressing the liquidity risk of crypto-assets that are not traded actively.

3.2.1.2.3 Major examples of DEXs – (Type 4) management entities do not exist, different kinds of crypto-assets available

There are no specific administrative entities, and "matching", "price formations", and "settlements" with foreign tokens are all done on-chain by the maker and the taker.

In order to carry out a transaction across different blockchain networks without a specific administrative entity, the user must do so through a complex procedure.
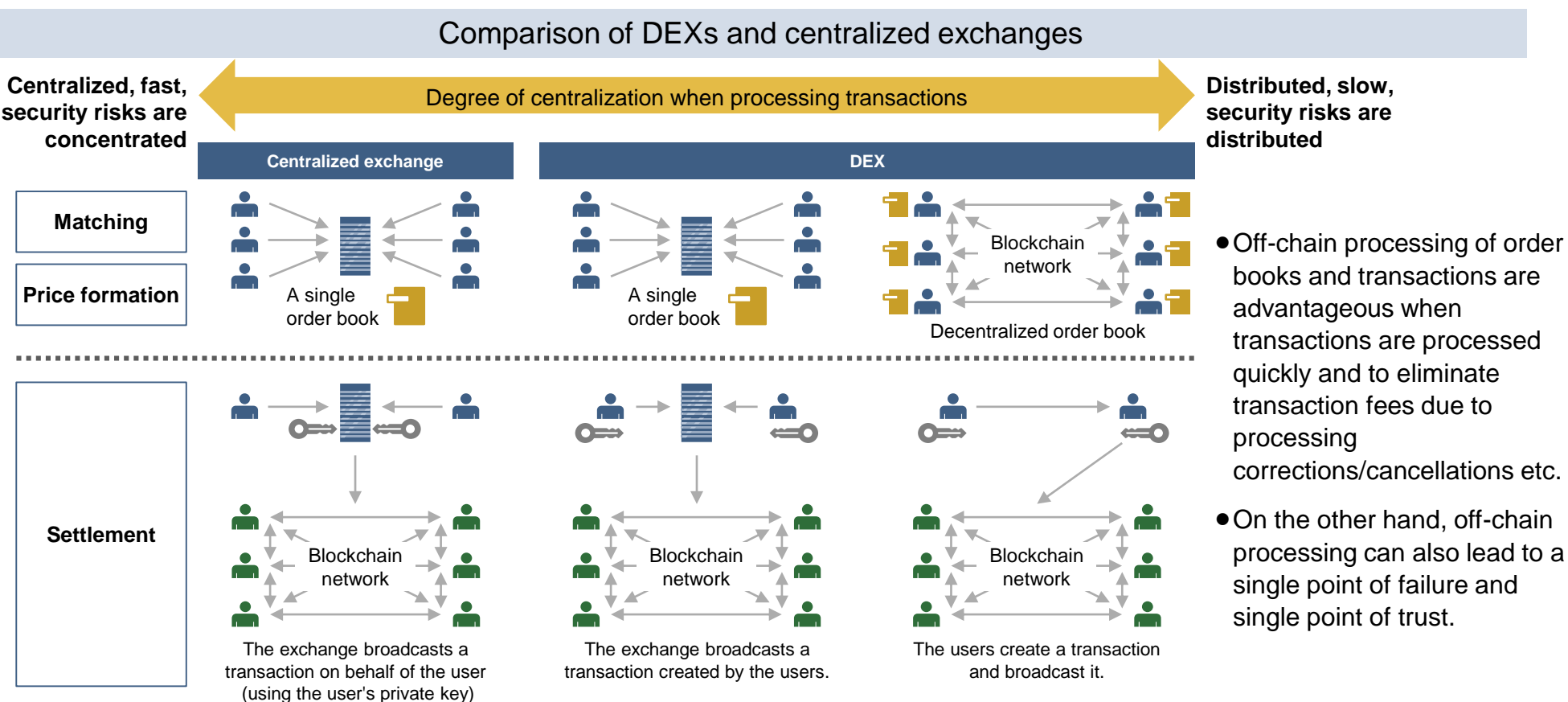
BarterDEX flowchart
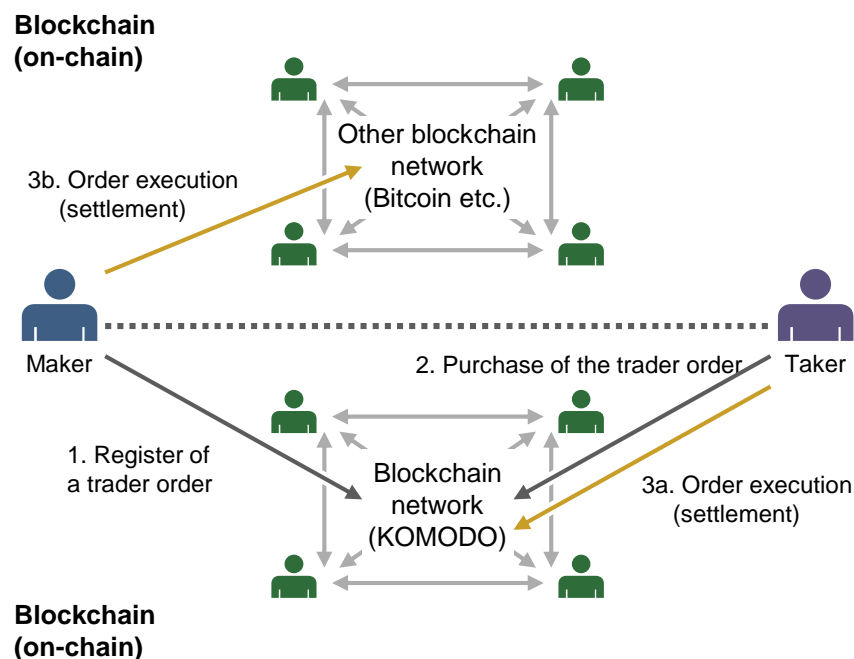
1. The maker registers a trade order in a distributed order book.

2. The taker selects the desired sell order.

3. After confirming the balance of the maker and the taker on different blockchain networks, matching is carried out.

4. Both the maker and the taker exchange crypto-assets between the two different blockchain networks in accordance with the atomic cross-chain swap protocol.

There are big burdens on the user compared with other DEXs: for example, the users need to manage their private keys on each blockchain network, they need to use the complicated procedure that is the atomic cross-chain swap, and they need to wait for a sufficiently long time for each transaction in order to confirm that transactions are not cancelled.

3.2.1.2.4 Challenges and new DEX initiatives – technical aspects

Since DEX originally intends to eliminate the custody risk, it is desirable that all operations be decentralized. However, in recent years many DEXs have adopted centralized processing, are focusing on efficiency rather than safety, and they resemble the way in which centralized exchanges act. Appropriate technical solutions for DEXs that have the right balance between safety and efficiency need to be considered moving forward.

Comparison of DEXs and centralized exchanges

Centralized, fast, security risks are concentrated — Degree of centralization when processing transactions — **Distributed, slow, security risks are distributed**

- Off-chain processing of order books and transactions are advantageous when transactions are processed quickly and to eliminate transaction fees due to processing corrections/cancellations etc.

- On the other hand, off-chain processing can also lead to a single point of failure and single point of trust.

83

3.2.1.2.4 Challenges and new DEX initiatives – Usability

Regarding crypto-asset transactions, existing centralized exchanges and payment service providers are better than DEXs in terms of usability. It is anticipated that there will be new uses only available for DEXs such as trading platforms for a large number of tokens or ones combined with other decentralized financial services.

Challenge	Content
Wide array of user responsibilities	• Private keys of crypto-assets need to be properly managed. • Users need to strictly follow complicated procedures in some DEXs. • Users need to take risks such as having bugs in smart contracts and other unintended failures.
Attacks by miners and malicious users	• DEX needs to be designed to prevent "front running" attacks (attacks that causes the attacker's transactions to be processed before those of the attack victim) and/or griefing attacks (attacks that cause unnecessary transaction fees by making the processing of a transaction fail due to insufficient balances etc.). However, attacks by miners cannot be prevented. • These countermeasures will inconvenience users as liquidity will be locked ahead of trades etc.
Inconveniences compared with existing centralized exchanges	• Processing speeds are slow compared to centralized exchanges that process transactions off-chain. • There are restrictions on the kinds of available crypto-assets. The number of DEXs that offer exchanges with fiat currencies is small. • Stop loss or limit orders are not available in many DEXs. • Leveraged trade and margin trading are not available in many DEXs. • Transaction fees are no cheaper than centralized exchanges. (Transaction fees of DEXs, in which higher transaction fees bring about a higher possibility of the successful completion of a transaction, are highly likely to increase.) In the case of "DEXs of which management entities do not exist and different kinds of crypto-assets are available": • There is a risk that transactions will be canceled partway through due to price fluctuations. • Users need to constantly monitor the blockchain network in case of fraud by counterparties. • The efficiency in the use of liquidity deteriorates when atomic cross-chain swaps are carried out.
Low liquidity	• The transaction volume through DEXs constitutes 0.1% of the total exchange volume. • Low liquidity will further lower liquidity due to network externality.

Appendix. Secure chat tools

Secure chat tools

Secure chat tools in the "Application Layer" are often used to anonymize communication concerning blockchain-related developments and dark market transactions. It is possible to encrypt communicated contents and obscure whole transmission paths by combining secure chat tools with anonymizing networks.
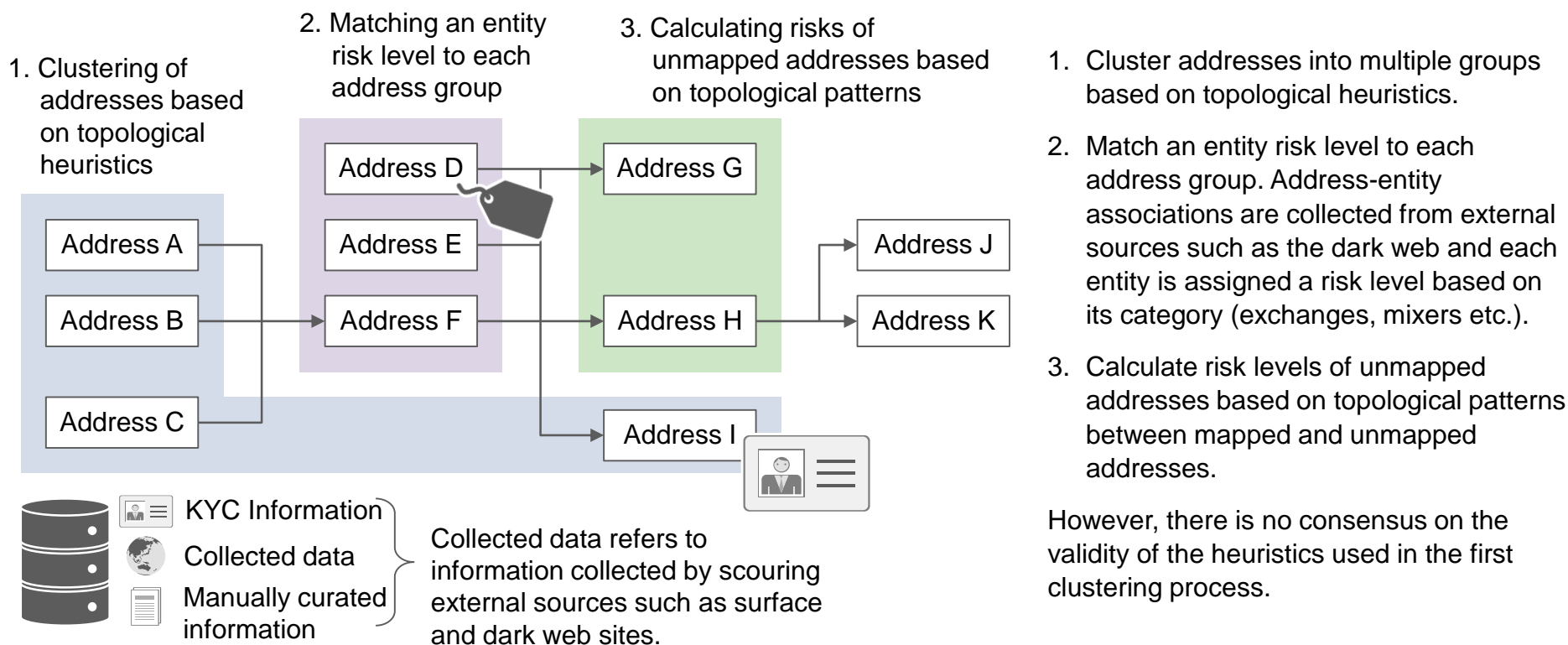
Major secure chat tools		
Name of Tool	Telegram	Signal
Brief explanation	There are over 200 million active users per month (as of March 22, 2018). The client software is open sourced, but the server software is a proprietary code.	Signal was approved as a communication tool for use by US senators. Part of the Signal Protocol is also used by other software such as WhatsApp. Both the client and server software are open sourced.
History	Launched in 2013 by brothers Nikolai and Pavel Durov, who previously founded the Russian social network, Vkontakte.	Previously separate apps TextSecure and Redphone that were launched around 2010 were combined into one app called Signal in 2014.
Mechanism and degree of anonymization	Telegram uses a proprietary protocol called MTProto, although concerns about its security have been raised. Only one-to-one secret chats are end-to-end encrypted	Signal uses a proprietary protocol called Signal Protocol, and as well as the extended Triple Diffie-Hellman key agreement protocol. All communications are end-to-end encrypted.
Incidents related to governments	Telegram has refused a disclosure request from a Russian federal agency. It has been banned in Russia. It has also been reported that it is banned in Iran as well.	Signal is designed to never collect or store any sensitive information. The U.S. government demanded data concerning suspicious communications in 2016, but they could not find any useful data.

3.2.2 Blockchain de-anonymization technologies

3.2.2 Blockchain de-anonymization technologies

Risk assessment on blockchain data addresses requires the following three steps: (1) clustering addresses into multiple groups based on topological heuristics, (2) linking each address group to information that is collected from external sources, and assigning each group a risk level, (3) calculating risk levels of unmapped addresses based on topological patterns between mapped and unmapped addresses. However, it should be noted that the assessed risks are estimations and depend heavily on the quality and quantity of external databases. (The effectiveness of anonymization and de-anonymization technology has not been academically evaluated as of yet.)

Illustration of blockchain data de-anonymization

1. Clustering of addresses based on topological heuristics

2. Matching an entity risk level to each address group

3. Calculating risks of unmapped addresses based on topological patterns

Address A
Address B
Address C
Address D
Address E
Address F
Address G
Address H
Address I
Address J
Address K

KYC Information
Collected data
Manually curated information

Collected data refers to information collected by scouring external sources such as surface and dark web sites.

1. Cluster addresses into multiple groups based on topological heuristics.

2. Match an entity risk level to each address group. Address-entity associations are collected from external sources such as the dark web and each entity is assigned a risk level based on its category (exchanges, mixers etc.).

3. Calculate risk levels of unmapped addresses based on topological patterns between mapped and unmapped addresses.

However, there is no consensus on the validity of the heuristics used in the first clustering process.
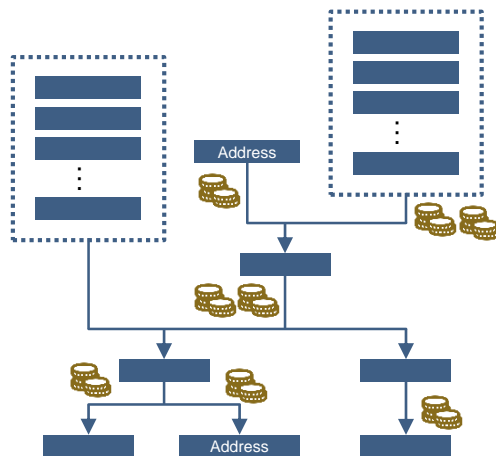
3.2.2 Blockchain de-anonymization technologies

De-anonymization methods are being developed by detecting distinctive patterns of advanced anonymization techniques such as mixing. Methods that use browser cookies and SNS information as external sources have also been proposed.

De-anonymization based on the distinctive patterns of mixing services

It is quite difficult to link a remittance source and destination when mixing is being used. Since addresses can be infinitely generated, identifying mixing services addresses is also difficult.

Therefore, de-anonymization based on the distinctive patterns of mixing services are being developed.

Pattern	Content
Reuse of the same address	• Transfer to the same address (central address) many times • The same address exists in multiple transfer routes
Distinctive topological patterns	• Repeatedly divided into two addresses that include a remittance destination and a change (Peeling chain) • The number of relays or the time interval between relays is constant • A single remittance source and multiple remittance destinations

De-anonymization that uses new external sources

A method that uses browser cookies as external sources has been proposed. Cookies are collected through banner advertisements and such that are posted on Bitcoin EC sites. Other proposed methods include mapping Bitcoin addresses to account information of SNS and dark web sites.
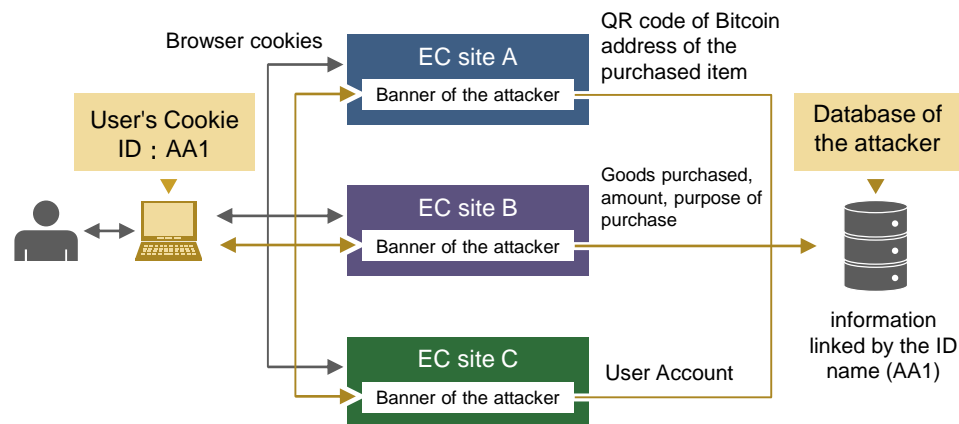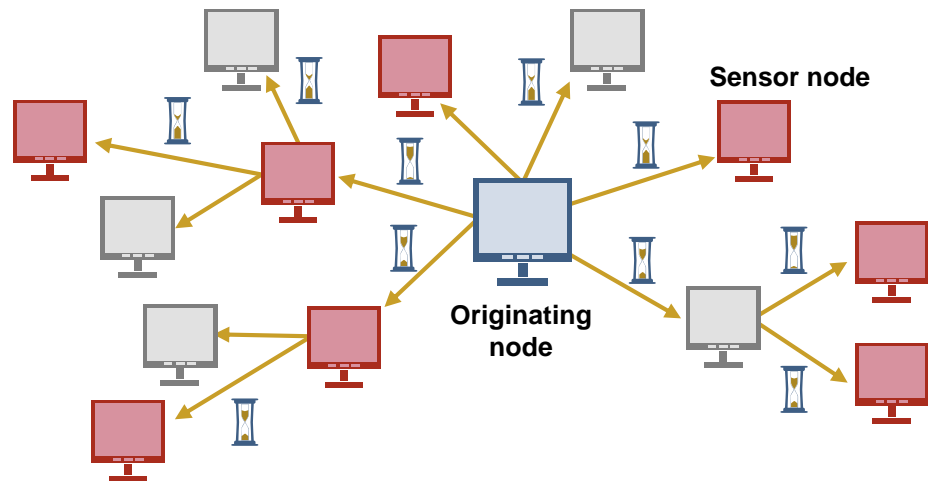

In the figure above, an attacker posts banner advertisements on multiple EC sites, and can link purchased information, such as account information and the remittance source address, on each site using the same cookie ID.

3.2.2 Blockchain de-anonymization technologies

Another method that identifies the originating node by collecting the logs from a sufficient number of sensor nodes on the P2P network has also been proposed. There have been instances where the method was actually carried out on Monacoin networks using more than 200 sensor nodes.

Illustration of source node de-anonymization

Estimations concerning the originating node are based on logs collected from many sensor nodes, much like sensors around a seismic epicenter. When making these estimations, a sufficient number of sensor nodes (the red nodes in the figure below) is necessary to increase the probability of being directly connected to the originating node. However, even if the originating node of a transaction can be specified, there is a possibility that this is not the original source IP address and the real one has been obscured using anonymizing networks.

Sensor node

Originating node

For details on an actual example, refer to the following: Japan Digital Design, "仮想通貨取引所Zaifから流出した仮想通貨の追跡について", https://www.japan-d2.com/news-detail/2018/11/5, Dec 12, 2018

3.3 P2P layer/Internet layer

3.3.1 P2P layer/Internet layer anonymization technologies

3.3.2 P2P layer/Internet layer de-anonymization technologies

3.3.1 P2P layer/Internet layer anonymization technologies

3.3.1.1 Overview of anonymizing networks

3.3.1.2 Classification of anonymizing networks

3.3.1.3 Major examples of anonymizing networks

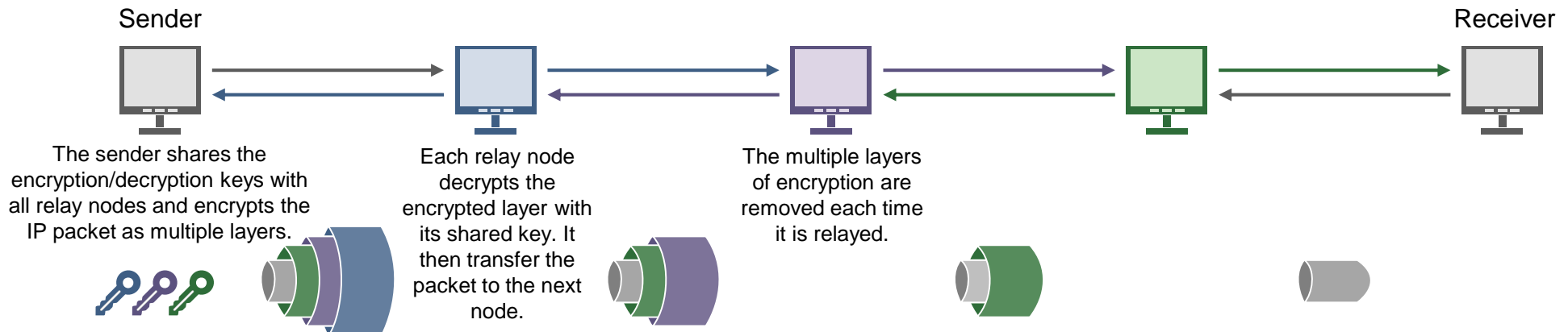3.3.1.4 Challenges and new anonymizing network initiatives

3.3.1.1 Overview of anonymizing networks – Anonymizing principles

The targets of Internet communication-related anonymization are (1) communication content and (2) transmission paths of IP packets.

➢ Since communication content is disclosed to only senders and receivers, encryptions are used to anonymize it similar to those of the popular SSL.

➢ Regarding the transmission paths, the source and destination IP addresses are recorded in IP packets, and the packets are relayed via each node based on the recorded IP addresses. Therefore, the whole transmission path should be anonymous to each of the relay nodes.

Example of anonymizing communication content and transmission paths

The IP packet is encrypted as multiple layers and only the information related to the next node is disclosed to each relay node on that transmission path. Therefore, the IP addresses of the senders and the contents of the communication can be kept secret from any third parties including the relay nodes ("Onion routing").

Sender

Receiver

The sender shares the encryption/decryption keys with all relay nodes and encrypts the IP packet as multiple layers.

Each relay node decrypts the encrypted layer with its shared key. It then transfer the packet to the next node.

The multiple layers of encryption are removed each time it is relayed.

3.3.1.1 Overview of anonymizing networks – Examples of illegal incidents

While anonymizing networks were developed for privacy protection and to share information when freedom of speech is being censored and/or controlled, it is also often used for illegal bargaining or criminal activity.

Examples of incidents in Japan where anonymizing networks were used illegally	
Case	**Description**
Remote controlled PC	• In October 2012, a PC that was infected with malware was used to make a threat/for blackmail. After conducting an investigation, the police arrested the owner of the PC that matched the IP address, but the arrest ended up being incorrect. • It is thought that the criminal used Tor to upload malware and remotely control the infected PC.
Pension information leak	• In May 2015, the Japan Pension Service suffered a cyber attack that caused the personal information of about 1.25 million people to be leaked. • Estimations suggest that Tor was used, making it difficult to identify the criminal. Police documents were sent to the prosecutor's office without any known suspects.
School bomb threat	• In January 2017, an e-mail containing a bomb threat was sent several times to a vocational school, resulting in the arrest of a student from that school. • The student had used Tor to send the e-mails, but the arrest was made based on the contents of the e-mail etc.
Child pornography release	• In June 2018, a suspect accused of publishing child pornography on a membership web site on the dark web using Tor, was arrested. • It was the first time that the owner of a dark web site using Tor was arrested in Japan. Only a few arrests like this have been made worldwide.

3.3.1.2 Classification of anonymizing networks – Main points of classification

From a technological point of view and the viewpoint of the authorities, we have classified anonymizing networks based on their routing method.

➢ Routing is a way to determine transmission paths, and it concerns the strength of anonymization, performance of communication (both technologically-speaking) and the identification of regulatory targets (system-related). Most routing methods are divided into two types: source routing and hop-by-hop routing.

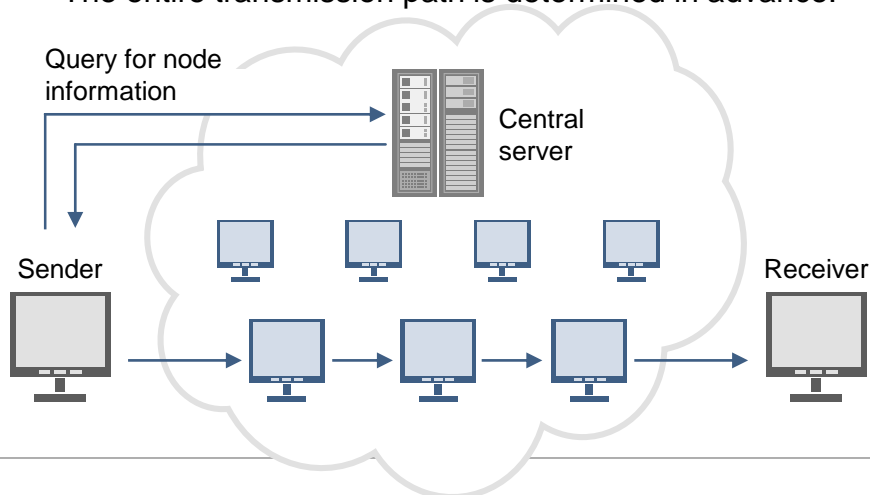| Illustration of source routing	Illustration of hop-by-hop routing
The sender determines the entire transmission path from the relay nodes up to the receiver and also its order, in other words a route. Therefore, it is necessary for the sender to know all the relay nodes in advance. As a specific entity is needed to manage the node information, this entity will become a regulatory target.	The sender does not decide the transmission path in advance, and each relay node determines the next destination at the time when the IP packet is being relayed by the node. Since there is no entity that manages node information, regulatory targets become ambiguous.

The entire transmission path is determined in advance.

The entire transmission path is not determined in advance. (Packets are transferred while trials are repeated.)
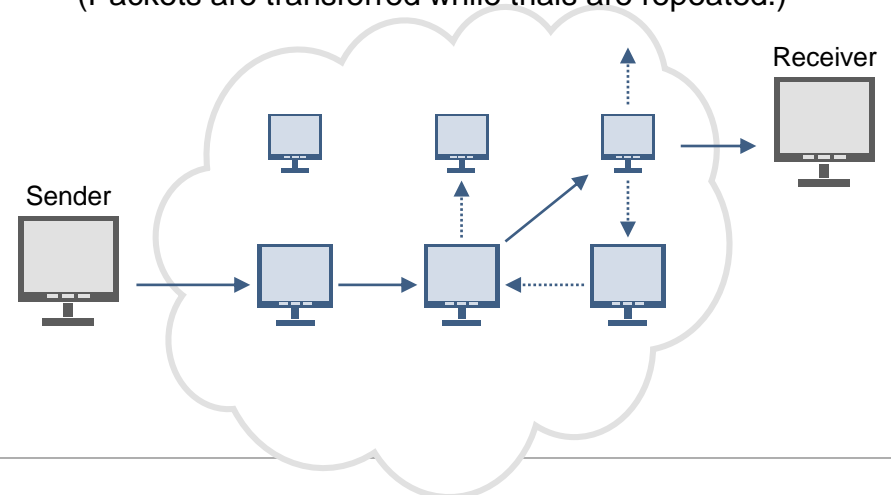
3.3.1.2 Classification of anonymizing networks – List of anonymizing networks

Each project is described in the subsequent slides.

List of anonymizing networks			
Type of routing	**Source routing**		**Hop-by-hop routing**
Major project	Tor (The Onion Router)	I2P (Invisible Internet Project)	Freenet
Method of managing node information	Centralized management using specific nodes	Distributed management using specific nodes	Each node manages only neighboring nodes' information
Principal use	Anonymous communications with surface web sites	Closed anonymous communications within its own network	Closed anonymous information sharing within its own network
	Since Tor is mainly designed for web browsing, it focuses on reducing communication delays.	I2P focuses on reducing communication delays in the I2P network. However, surface web site communication delays are long.	As files are managed in a distributed manner, access to these files is possible even if the original holder is offline.
Degree of anonymity	The entire transmission path is concealed from any third parties including relay nodes. (However, the exit node can work out the content of a communication if HTTPS is not used.)	The entire transmission path is concealed from any third parties including relay nodes.	The entire transmission path is concealed from any third parties including relay nodes.

# 3.3.1.3 Major examples of anonymizing networks – Tor (The Onion Router)

Tor is the most popular anonymous communication tool. It focuses on reducing communication delays for the uses such as web browsing.

Tor can easily be used from a smartphone, and it is currently estimated that there are more than 200 million users and around 7,500 relay nodes (including 1,150 exit nodes).

Number of Tor users

Number of Tor relay nodes
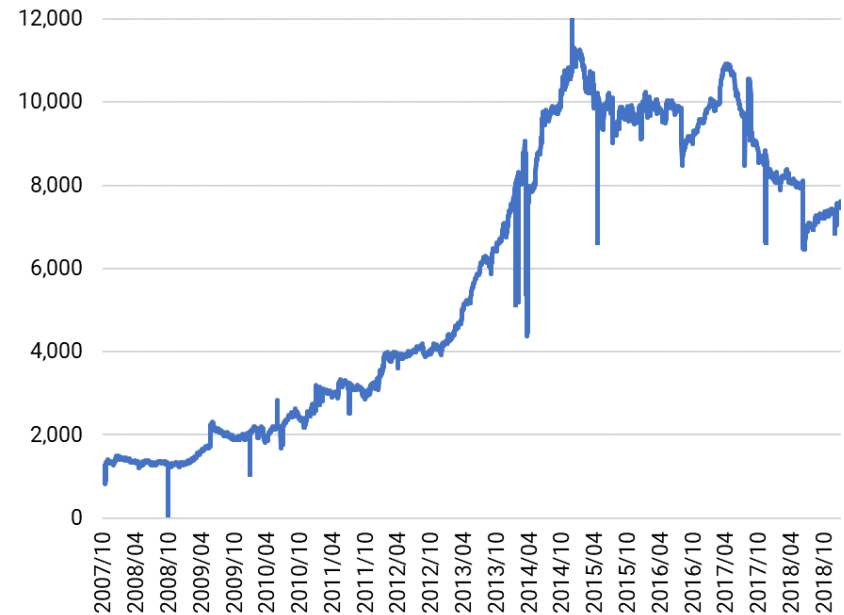
3.3.1.3 Major examples of anonymizing networks – Tor for the surface web

Tor anonymizes an entire transmission path by (1) relaying the IP packets from the sender several times using relay nodes, which consist of the entry node, the intermediate node, and the exit node, and (2) making it so that each relay node only knows the nodes before and after itself. Separate procedures such as SSL are required to anonymize communication content. *It is assumed that the destination's IP address is made public.

Tor flowchart

1. Query for node information
Directory server
Sender
2. Creation of a "circuit"
Circuit
Tor
Entry node   Intermediate node   Exit node
3. Sending of data to the receiver
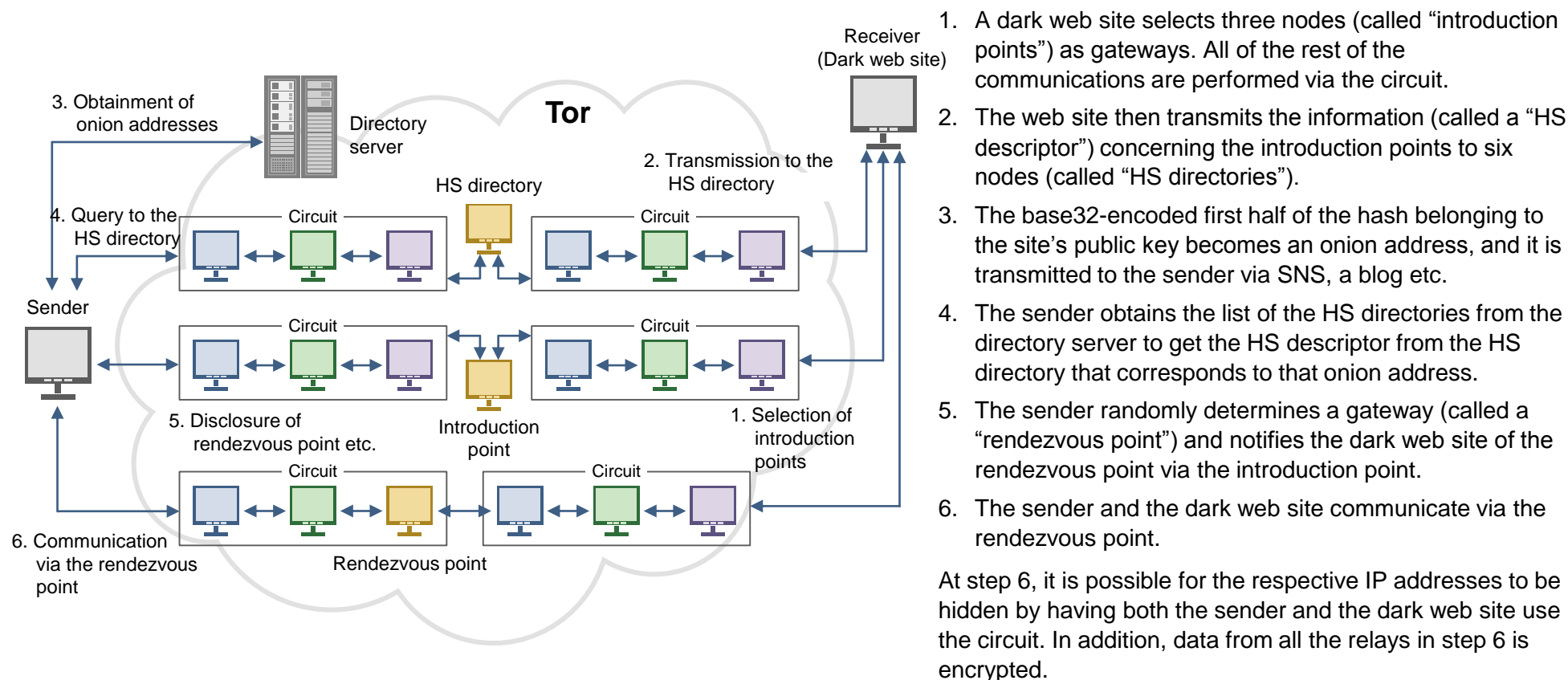Receiver (Web site)
4. Response of the receiver
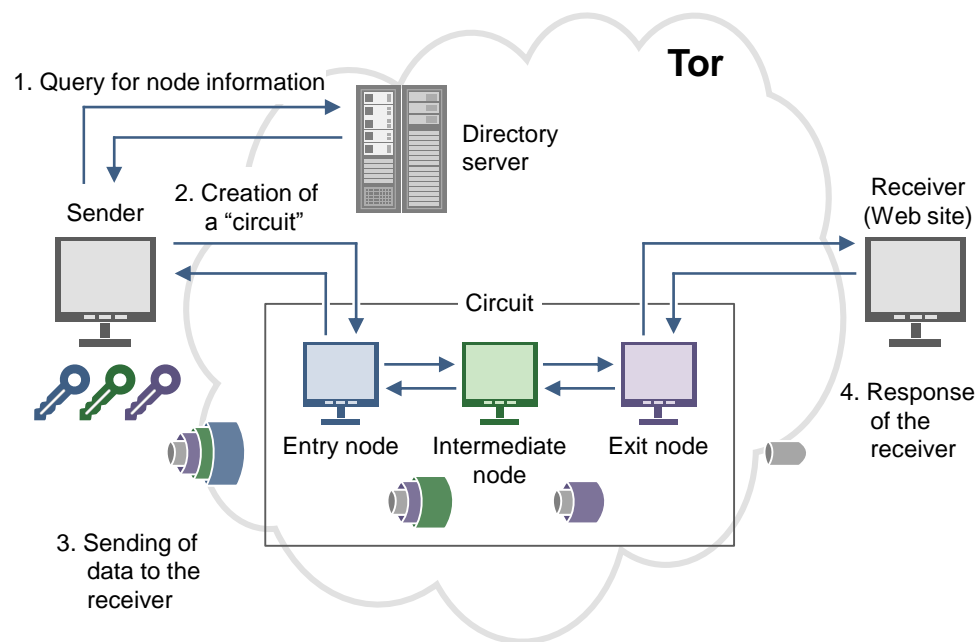
1. The sender obtains information about the relay nodes (IP address, public key etc.) from the directory server (there are a total of 10 at the time of writing) that manages all node information.

2. The sender determines the relay nodes to be used, and creates a bidirectional communication path (called a "circuit") between them. A common key shared between the sender and each relay node is created by combining one's own secret key and with the other's public key (a Diffie-Hellman key exchange). To improve anonymity, the circuit is recreated every ten minutes.

3. The sender sends data to the entry node. The entry node decrypts the received data with the common key that is shared with the sender and forwards it to the next node. The data is then relayed multiple times, and finally transferred to the receiver via the exit node.

4. The receiver sends the response data to the exit node. The response data is transferred to the sender via the same circuit and encrypted with a common key every time it is relayed.

It is important to note that the exit node can see the contents of the communication if they are not encrypted by SSL/TLS secure channels.

98

3.3.1.3 Major examples of anonymizing networks – Tor for the dark web

Tor has a mechanism, called Tor Hidden Services, that anonymizes the IP addresses of receivers in addition to those of senders. Sites that use Tor Hidden Services are generally referred to as the "dark web". A unique form of URL (http: //***.onion) is used to specify these server addresses.

Tor Hidden Services flowchart

1. A dark web site selects three nodes (called "introduction points") as gateways. All of the rest of the communications are performed via the circuit.

2. The web site then transmits the information (called a "HS descriptor") concerning the introduction points to six nodes (called "HS directories").

3. The base32-encoded first half of the hash belonging to the site's public key becomes an onion address, and it is transmitted to the sender via SNS, a blog etc.

4. The sender obtains the list of the HS directories from the directory server to get the HS descriptor from the HS directory that corresponds to that onion address.

5. The sender randomly determines a gateway (called a "rendezvous point") and notifies the dark web site of the rendezvous point via the introduction point.

6. The sender and the dark web site communicate via the rendezvous point.

At step 6, it is possible for the respective IP addresses to be hidden by having both the sender and the dark web site use the circuit. In addition, data from all the relays in step 6 is encrypted.

3.3.1.3 Major examples of anonymizing networks – Censorship-resistance using protocol spoofing

Users can connect to bridge nodes that do not have published IP addresses in locations where IP addresses are restricted by the government etc. (Since the IP addresses of entry, intermediate, and exit nodes are published, the government can restrict these.) By carrying out protocol spoofing that disguises communications from the sender to the bridge as ordinary ones, it prevents communications from being detected even when deep packet inspections that examine the contents of IP packets are carried out.

Tor bridge mode flowchart
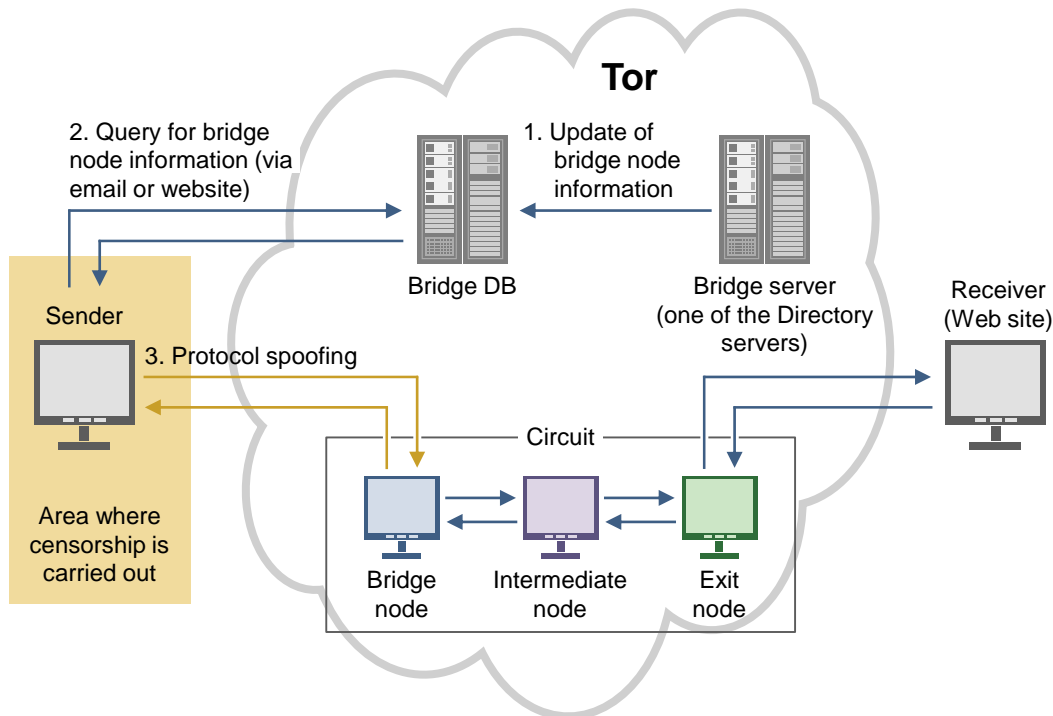
1. In Tor bridge mode, bridge nodes are used instead of entry nodes. A bridge node encrypts its information and sends it to the bridge server, which periodically stores the collected information about the bridge nodes in the bridge DB.
2. The sender queries the bridge DB for information on the bridge nodes via HTTPS web sites or e-mails. The sender obtains the information of three bridge nodes. Information from only a few bridge nodes can be obtained at a time as so not to identify all the bridge nodes.
3. The sender connects to the bridge node by disguising the protocol. There are several disguising patterns, such as normal TLS connections or random noises, and the patterns can be changed according to the type of censorship. The disguised connections cannot be distinguished from normal connections, and censorship systems find it difficult to recognize them as Tor connections.
4. The sender and the receiver communicate via a circuit the same as with a normal Tor connection.

It is important that communications between the sender and the bridge node are disguised. However, it has been pointed out that vulnerabilities exist including the fact that bridge node IP addresses could become exposed, and also that academic safety verifications are said to still be in progress.

3.3.1.3 Major examples of anonymizing networks－I2P (Invisible Internet Project)

Within I2P, communications are anonymous within their own closed network, and there are big communication delays when browsing surface web sites.

I2P is very similar to Tor but there are minor differences: for example, node information is managed in a distributed manner, communications travel in one direction, the type of relay nodes is the same, and multiple messages are encrypted at a time.

I2P flowchart
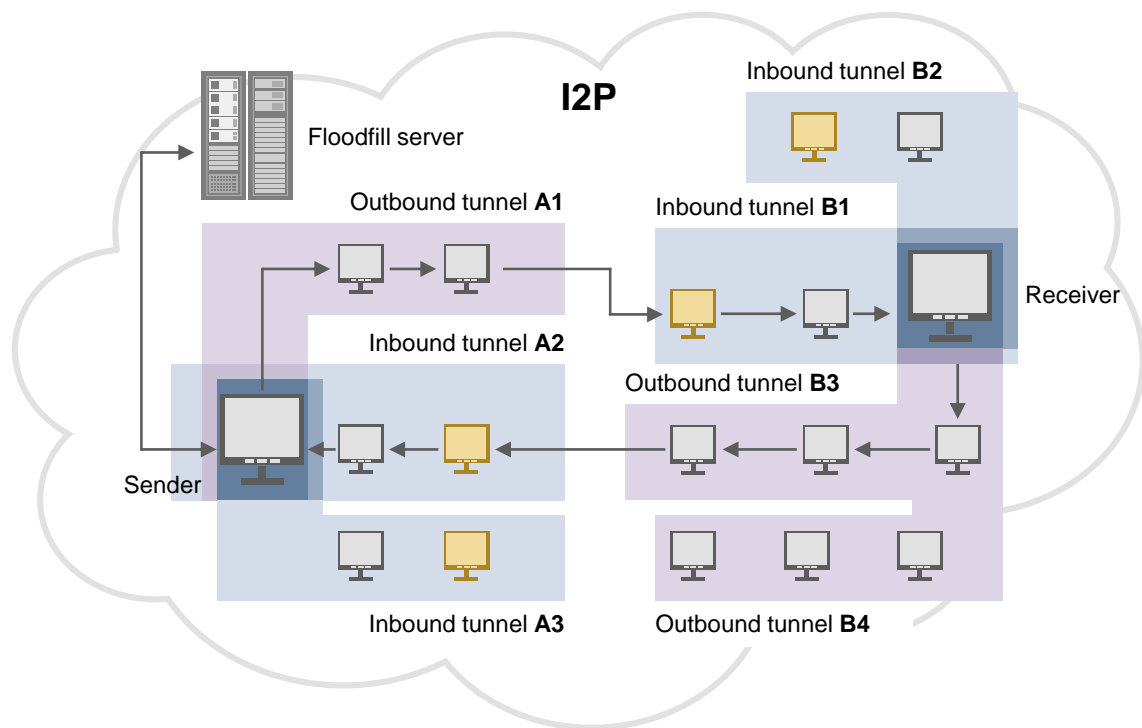
1. Both a sender and receiver prepare multiple communication paths, or "tunnels", for transmission and reception. During the creation of a tunnel, as with Tor, a common key is created between the sender and each relay node. The tunnel is recreated every ten minutes to increase anonymity.

2. The sender obtains the gateway information (the yellow node in the figure) about the receiver's inbound tunnel (B1 in the figure) from the floodfill server that is managing all the node information in a distributed manner.

3. The sender transfers data to the gateway (the yellow node in the figure) of the receiver's inbound tunnel (B1 in the figure) by using their own outbound tunnel (A1 in the figure). The gateway in turn transfers the data to the receiver.

4. The receiver sends a response message through its outbound tunnel (B3 in the figure) to the gateway (yellow node in the figure) of the sender's inbound tunnel (A2 in the figure). The data is then transferred to the sender.

The data in all routes is encrypted.

3.3.1.3 Major examples of anonymizing networks – Freenet

Freenet also anonymously shares information (such as anonymous file sharing, bulletin boards etc.) within its own closed network. Since node information management entities do not exist in hop-by-hop routing, there are sizable communication delays. Data is stored in each node participating in the network, and the data remains on within Freenet even when the original sender goes offline.

Freenet flowchart
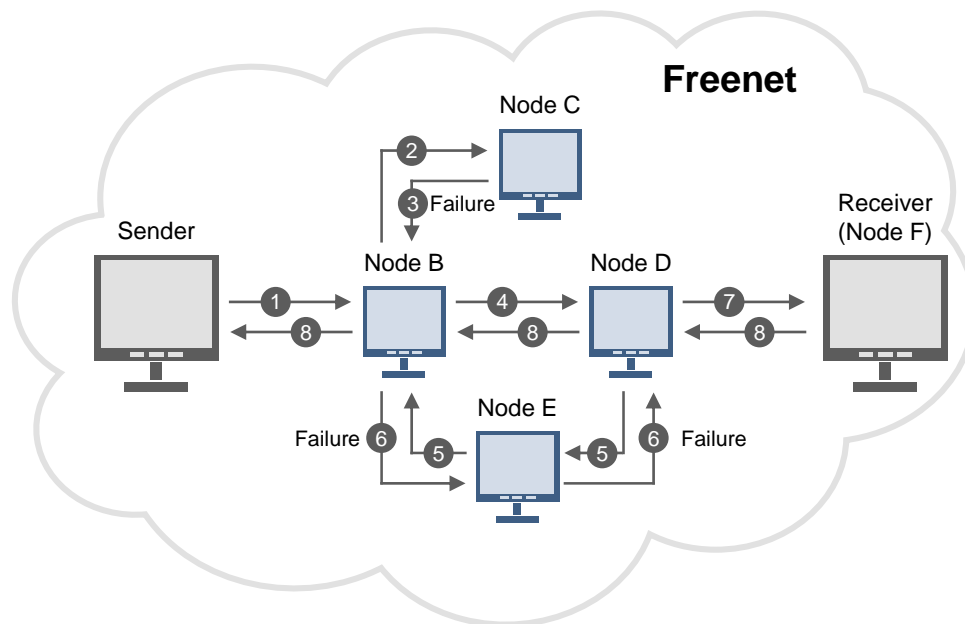
1. The sender sends a request message, which includes a GUID (Globally Unique Identifier) key pertaining to the data to be acquired, to the neighboring node B.

2. Node B sends the request message to node C which is the closest to the requested key on node B's GUID key table.

3. Node C returns a response indicating a failure.

4. Node B sends the request message to node D which is the second closest to the requested key on its GUID key table.

5. Node D sends the request message to node B via node E.

6. Node B returns a response indicating a failure via node E.

7. Node D sends the request message to node F which is the second closest to the requested key on its GUID key table.

8. Since node F has the data, node F transfers the data to node D. The data is then transferred to the sender in the order node D first, and then node B. The data is cached and the GUID key table is updated on each node.

It is predicted that communication delays (that is, the number of relay nodes) increase exponentially as the total number of nodes increases, but this has not been fully confirmed in an actual network.

3.3.1.4 Challenges and new anonymizing network initiatives

No serious vulnerabilities have been reported so far but securing anonymity as a whole when combined with other applications is considered to be an important issue in the future.

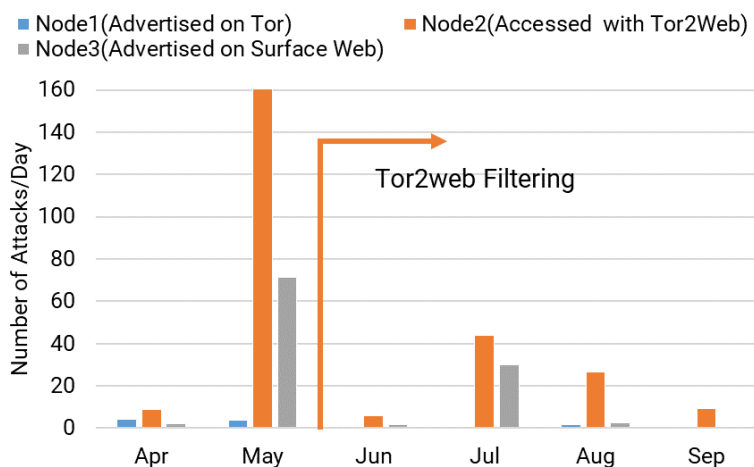| List of challenges and new initiatives of anonymizing networks	
Challenge	**Content**
Vulnerabilities due to combinations with other applications	• Tor functions as a proxy server so it is easy to use Tor in combination with other applications. However, methods that tackle reducing anonymity considerably when combining Bitcoin and Tor have been proposed. • Using a combination of applications may pose new vulnerability risks and technical problems that do not occur when each application is used individually.
Tradeoff between size and quality of anonymous sets	• It is desirable to secure a sufficient number of users (anonymous set) to achieve anonymization. • On the other hand, when the number of users increases, communication performance may be lower, or anonymity may be reduced due to relaxed settings by beginners.
Existence of a single point of trust and single point of failure	• For example, in Tor and I2P, there exist specific entities (directory server etc.) that manage node information and users trust these entities to respond correctly as well as relay nodes to transfer the data properly. • Therefore, these single points of trust can be the targets of attacks that disrupt anonymous networks. For example, it has been pointed out that by putting a majority of directory servers in control as well as returning incorrect node information to senders, anonymous communications using Tor can be interrupted.
Other vulnerabilities	• For example, it has been proposed that by conducting statistical analyses on network traffic, attackers can specify a transmission path or a relationship between a sender and a receiver (called a "timing attack"). A lot of effort has been put into overcoming this problem by anonymizing network communities.

3.3.1.4 Challenges and new anonymizing network initiatives

While anonymous communication tools are becoming more readily available, phishing fraud targeting dark web users and conflicts within the dark web are also intensifying, and these trends look to continue.

Attacks on dark web sites	Phishing scams on dark web users

The number of attacks on dummy dark web sites (such as marketplaces or blogs) reached a maximum of 170 times per day. The majority of attacks were conducted via Tor2web that enables normal web browsers to connect to dark web sites. Even after Tor2web related attacks were filtered out, attacks such as site tampering continued to happen. Therefore it appears that attackers were making a considerable effort to attack or interfere with rival dark web sites by manually searching them.
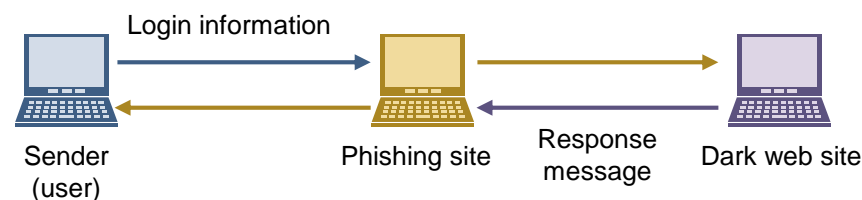
For example, Tor is easily accessible from a smartphone.

Since dark web sites do not want to reveal their identities, they generally do not obtain certificates from a root certificate authority. Therefore, users can not judge the authenticity of dark web sites, and it becomes difficult to be aware of phishing fraud.

(Left) Created by MRI based on Catakoglu, O., et al, madlab.it, "Attacks Landscape in the Dark Side of the Web", http://www.madlab.it/papers/sac17_darknets.pdf, Jan 30, 2019
(Top right) Guardian Project, guardianproject.info, "Orbot: Tor for Android", https://guardianproject.info/wp-content/uploads/2010/02/featuregraphic.png, Dec 14, 2018

104

3.3.2 P2P layer/Internet layer de-anonymization technologies

3.3.2 P2P layer/Internet layer de-anonymization technologies

There are suggestions of a method that identifies entire transmission paths by conducting traffic pattern analyses of a network or collecting information from prepared relay nodes/exit nodes. However, it should be noted that these identified paths are still just based on estimations.

Illustration of the de-anonymization of an entire transmission path

Particularly in the case of Tor, in order to reduce communication delays, the time for data to travel from the source node and to the destination node is likely to be relatively short. Therefore, the relationship between the source node and the destination node can be estimated from similarities in traffic patterns.
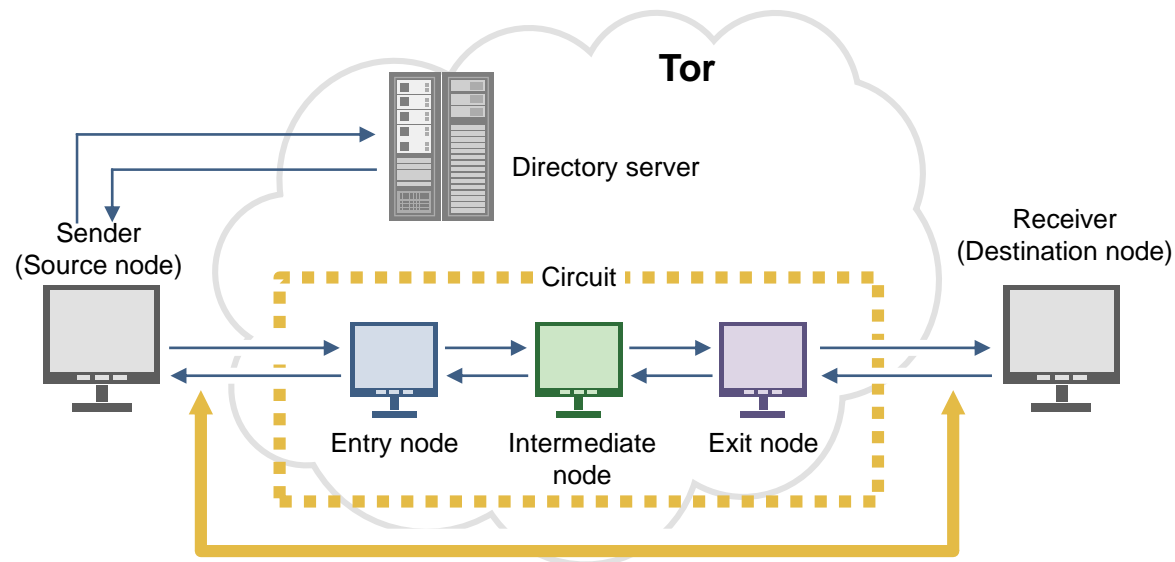
Estimations based on the similarity in traffic patterns

3.4 Physical layer

3.4.1 Physical layer anonymization technologies

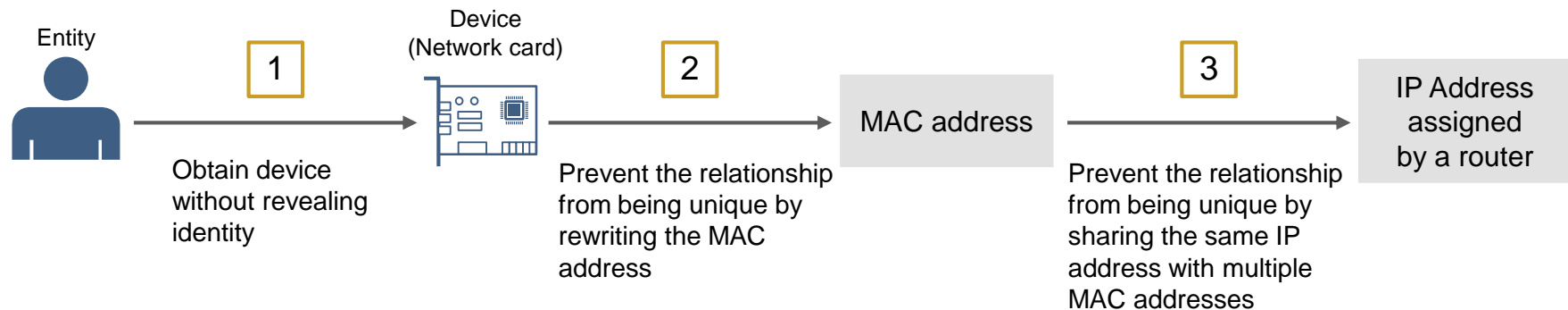3.4.2 Physical layer de-anonymization technologies

3.4.1 Physical layer anonymization technologies

3.4.1 Physical layer anonymization technologies − Anonymizing principles

Three types of relationships that are anonymized when accessing the Internet include: (1) the relationship between an entity and a device (or a network card), (2) the relationship between a device and a MAC address*, and (3) the relationship between a MAC address and an IP address. Anonymizing principles include the following:

- Regarding (1) entity-device relationships, it is important for an individual to obtain a device without revealing their identity.
- It is essential to prevent (2) device-MAC address relationships from being unique (e.g., by rewriting the MAC address) .
- (3) MAC address-IP address relationships must also not be unique (e.g. by sharing the same IP address).

Anonymizing principles among entities, devices, MAC addresses, and IP addresses

Entity

1
Obtain device without revealing identity

Device (Network card)

2
Prevent the relationship from being unique by rewriting the MAC address

MAC address

3
Prevent the relationship from being unique by sharing the same IP address with multiple MAC addresses
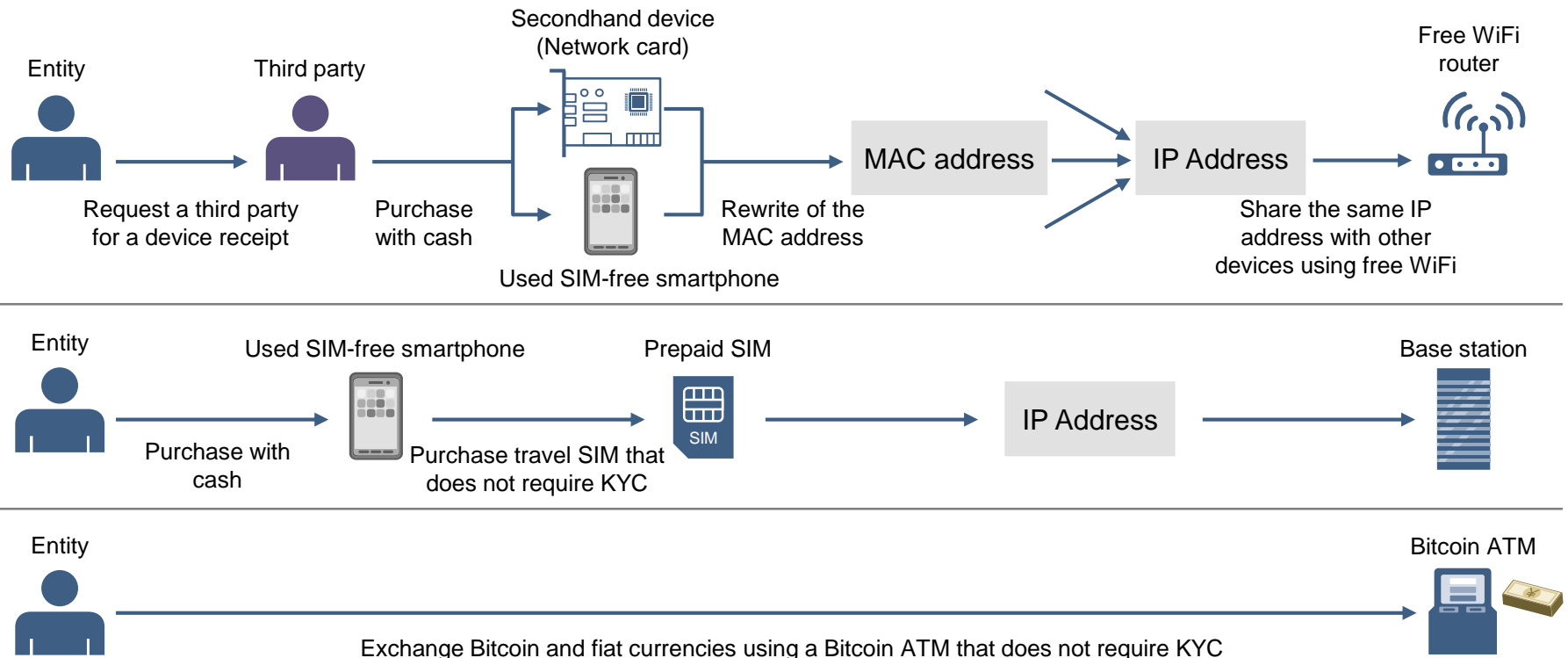
IP Address assigned by a router

* A MAC address is a 6 byte identifier assigned to each network interface when manufactured, and they are generally unique as a rule.

3.4.1 Physical layer anonymization technologies

A device can also be procured by purchasing one secondhand (and requesting a third parties for a device receipt) or through theft. After the MAC address is changed, the Internet can be accessed by either (1) using free Wifi or (2) using a prepaid SIM that does not require KYC. An alternative anonymization technique is (3) using a Bitcoin ATM that does not require KYC.

An example of anonymization in the physical layer

Entity

Third party

Secondhand device
(Network card)

MAC address

IP Address

Free WiFi router

Request a third party for a device receipt

Purchase with cash

Rewrite of the MAC address

Share the same IP address with other devices using free WiFi

Used SIM-free smartphone

Entity

Used SIM-free smartphone

Prepaid SIM

IP Address

Base station

Purchase with cash

Purchase travel SIM that does not require KYC

SIM

Entity

Bitcoin ATM

Exchange Bitcoin and fiat currencies using a Bitcoin ATM that does not require KYC

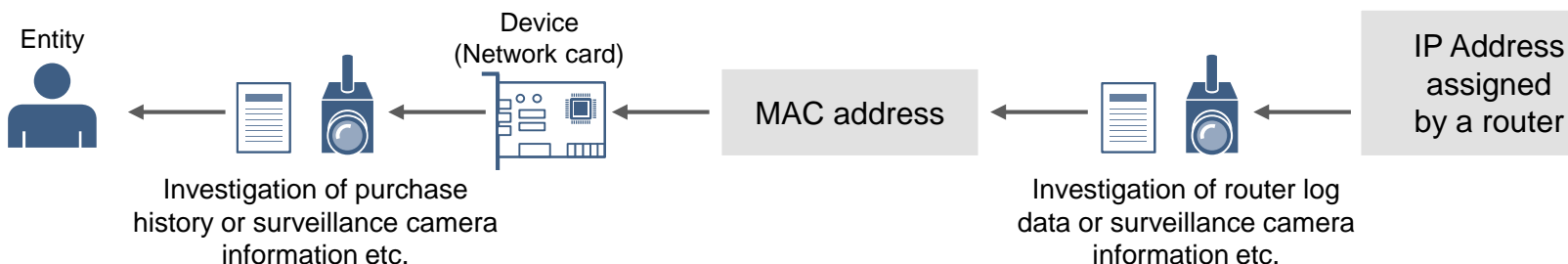# 3.4.2 Physical layer de-anonymization technologies

3.4.2 Physical layer de-anonymization technologies

There are two main methods of identifying an entity from its IP address: by (1) using log data or (2) using registry data. Both methods depend heavily on the quality and quantity of the data, including log data, purchase history and registry data. However, in many cases, identification can be a challenge as there are cases in which such data cannot be used: e.g. when the data has discarded after a certain period of time or when its quality is low.
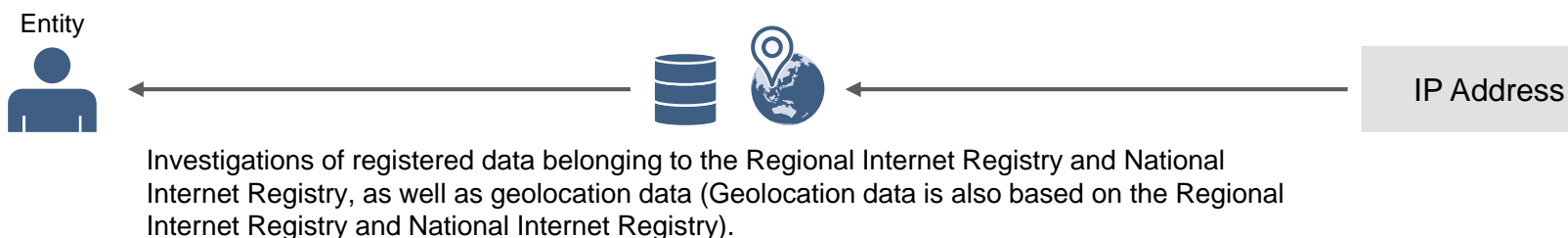
An example of de-anonymization in the physical layer

1 **Identification using log data**
Although the log data at a time around the time a crime was committed is required, there is always a possibility that the data was discarded after a certain period of time.

Entity

Device
(Network card)

MAC address

IP Address
assigned
by a router

Investigation of purchase
history or surveillance camera
information etc.

Investigation of router log
data or surveillance camera
information etc.

2 **Identification using registry data**
There are cases where the registry data includes missing items or has not been updated.

Entity

IP Address

Investigations of registered data belonging to the Regional Internet Registry and National
Internet Registry, as well as geolocation data (Geolocation data is also based on the Regional
Internet Registry and National Internet Registry).

4. Experiments

4.1 List of experimental scenarios

4.2 Crypto-laundering using lightning networks

4.3 Crypto-laundering using mixing services

4.4 Countermeasures using risk scoring tools

Summary of this chapter

- Our experiments aim to identify possible areas where current technology developments and those in the near future could lead to serious AML/CFT concerns regarding crypto-asset transactions.

- We assessed three scenarios: (1) crypto-laundering using lightning networks, (2) crypto-laundering using mixing services, and (3) countermeasures using risk scoring tools, assuming that criminal proceeds were laundered using crypto-assets.

- Concerning (1) crypto-laundering using lightning networks, identifying and tracing transfer routes using blockchain data or network packet data proved to be quite difficult in the case of all four lightning networks. Anonymity looks to be further enhanced in the near future which reflects the improvements being made in regards to lightning network techniques.

- (2) Crypto-laundering using mixing services was easy to achieve, and identifying and tracing transfer routes using blockchain data was quite difficult. It was assumed that these mixing services deal with a considerable amount of crypto-assets.

- As for (3) countermeasures using risk scoring tools, several tools were assessed using real Bitcoin addresses. However, the estimated scores did not fully reflect the actual risk in most cases.
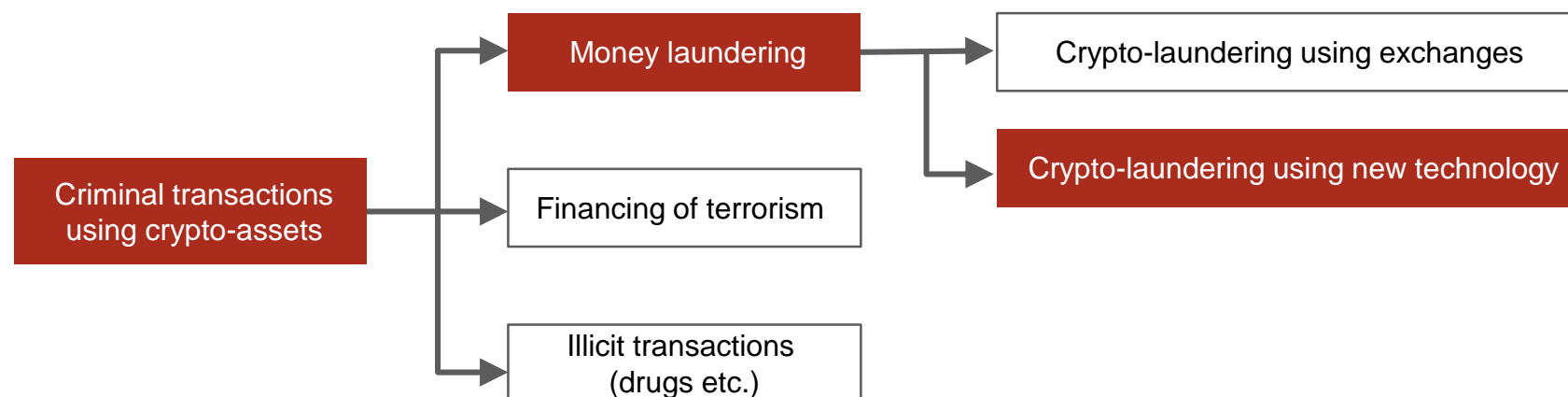
4.1 List of experimental scenarios

The purpose of our experiments was to identify possible areas where current technology developments and those in the near future could lead to serious AML/CFT concerns regarding crypto-asset transactions.

Considering the fact that money laundering accounts for all criminal transactions in Japan to date, we considered cases where criminal proceeds were gained through the laundering of crypto-assets.

Scenarios considered in our experiments
There are different types of criminal transactions that use crypto-assets - money laundering, financing of terrorism, illicit transactions etc. - and the best technology and corresponding countermeasures are thought to be different for each case. However, in our experiments, we only considered money laundering as this accounts for all criminal crypto-asset transactions in Japan to date.

4.1 List of experimental scenarios

The following experiments were conducted as per advice from experts.

	List of experiments		
No.	**Name**	**Content of Experiment**	**Issues to be verified**
1	Crypto-laundering using lightning networks	Transferring crypto-assets through multiple relay nodes using lightning networks	• Identification of transfer routes using blockchain data → Quite difficult • Identification of transfer routes using network packet data → Quite difficult
2	Crypto-laundering using mixing services	Transferring crypto-assets using publicly available mixing services	• Usability → Easy to use • Identification of transfer routes using blockchain data → Quite difficult (presumed that it is difficult to identify whether mixing services were used or not)
3	Countermeasure using risk soring tool	Assessing the risk of actual bitcoin addresses using multiple risk scoring tools	• Validity of risk → Evaluated risks are not always accurate • Identifying the fact that mixing services are used → Most of the tools could not identify this

4.2 Crypto-laundering using lightning networks – Overview

The Bitcoin network (testnet) was used to transfer bitcoins, which were treated as criminal proceeds, via two nodes on the lightning network. Four different types of lightning networks were used. When evaluating traceability, the following points were assessed; (1) whether transfer routes could be identified using blockchain data, (2) whether transfer routes could be identified using network packet data.

Illustration of relay remittance using lightning networks

1. Open each payment channel

Node A — Payment Channel — Node B — Node C — Node D
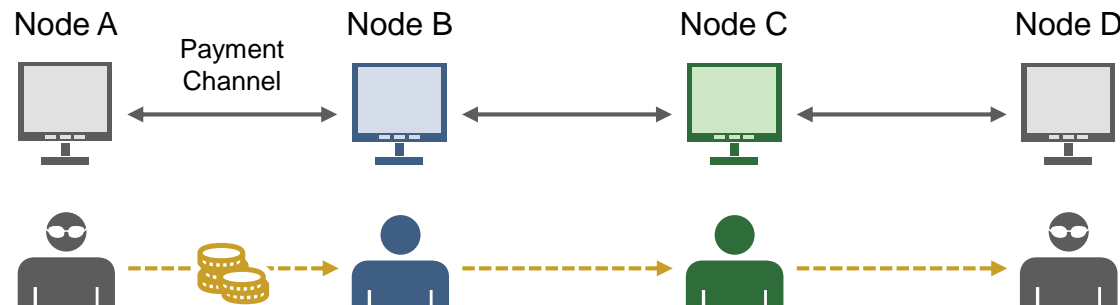
2. Transfer bitcoins from node A to node D

It was assumed that bitcoins stolen from exchanges had already been transferred to the address held by node A. With this in mind, we considered a case in which a criminal transfers said bitcoins to the address of another node (node D) held by the criminal via relay nodes B and C using the lightning network.

1. The criminal opens a payment channel between nodes A and B, and nodes C and D (the payment channel between node B and C had already been opened).

2. The criminal decides on the transfer route (node A → B → C → D) and transfers bitcoins from node A.

* Four types of lightning networks (c-lightning, LND, eclair, ptarmigan) were used.

4.2 Crypto-laundering using lightning networks – Blockchain data

Since different bitcoins are used during relay remittances, the entire transfer route cannot be identified by third parties using blockchain data.

The transfer routes that can be identified using blockchain data
(Above: how the relay remittance transpired, Bottom: Illustration of blockchain data)
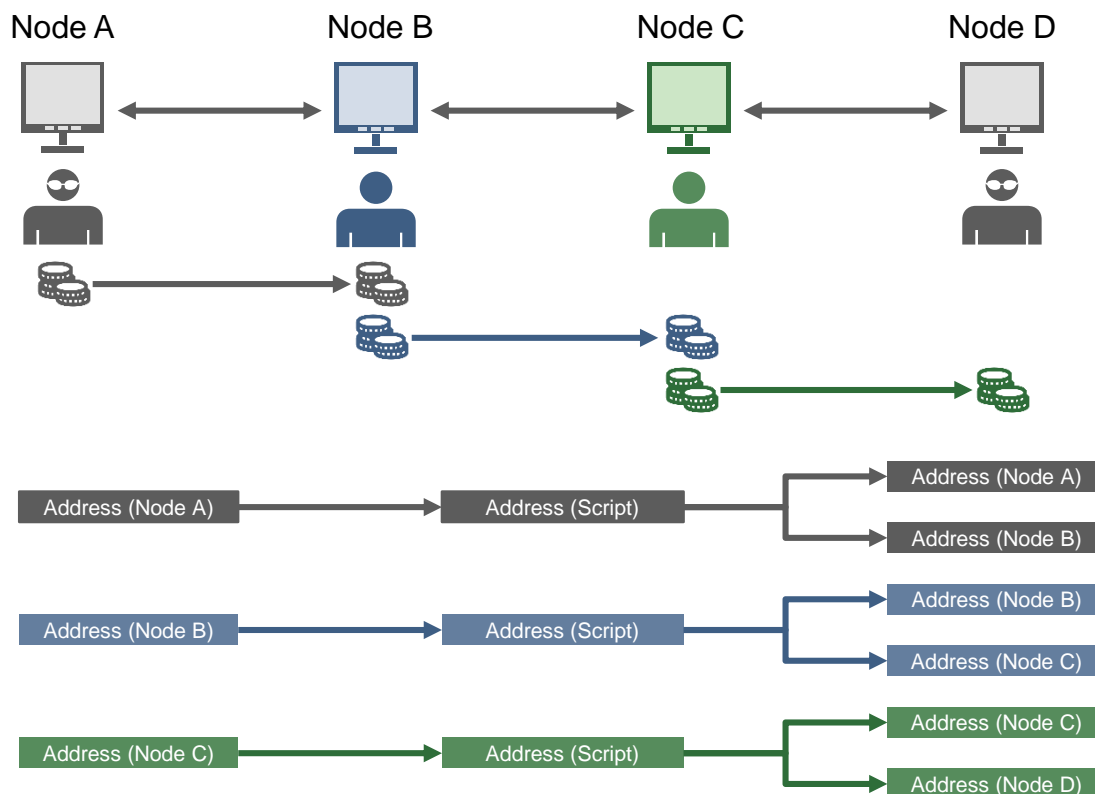
Relay remittances using lightning networks are carried out by remitting the bitcoins to a relay node, and this node then sends that same amount in other bitcoins to the next node.

Therefore, the relationship between the bitcoins remitted by node A and the ones received by node D cannot be identified by third parties.

All that could be identified using blockchain data was that the bitcoins from node A (upper left) were ultimately divided into two addresses (top right).

The transfer route from node A (black), one from node B (blue), and one from node C (green) are not necessarily recorded in chronological order.

* According to the specifications at the time of writing, only one party in the transaction will make a deposit.

4.2 Crypto-laundering using lightning networks – Network packet data

Since network packet data is encrypted, it is not possible for third parties to see the content of transactions. It is also not possible for anyone except the sender to know the entire route.

The transfer route that can be identified using network packet data
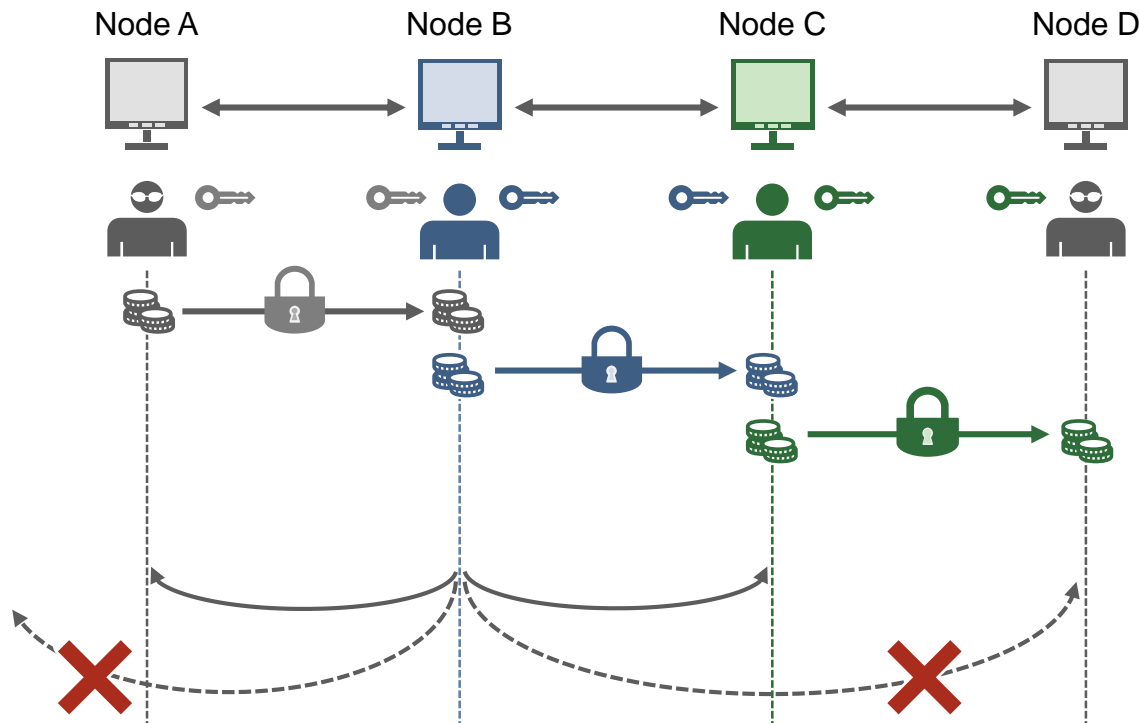
In relay remittances using lightning networks, the IP packet data within the transfer route is encrypted and only the involved parties can see its content.

Furthermore, since only the preceding and succeeding nodes can be identified by each relay node, node B cannot know about the existence of node D and whether node A is one of the relay nodes or the sender's node.

Therefore, the entire transfer route including the sender (node A) and the receiver (node D) can be known only to the sender.

4.2 Crypto-laundering using lightning networks – Further increase of anonymity

Transfer route anonymity can be further increased by making a path longer or going through the relay node that serves as the hub among other relay nodes. As "Scriptless Scripts" and "Multi-Hop Locks" become more readily available in the future, this anonymity could increase even further. Crypto-laundering can also be achieved by becoming a relay node.

Illustration of laundering through a hub relay node	Illustration of a criminal becoming a relay node

The probability of being identified can be reduced by going through a relay node that serves as a hub among other relay nodes (Node B and C below). It can also be reduced by making the path longer.
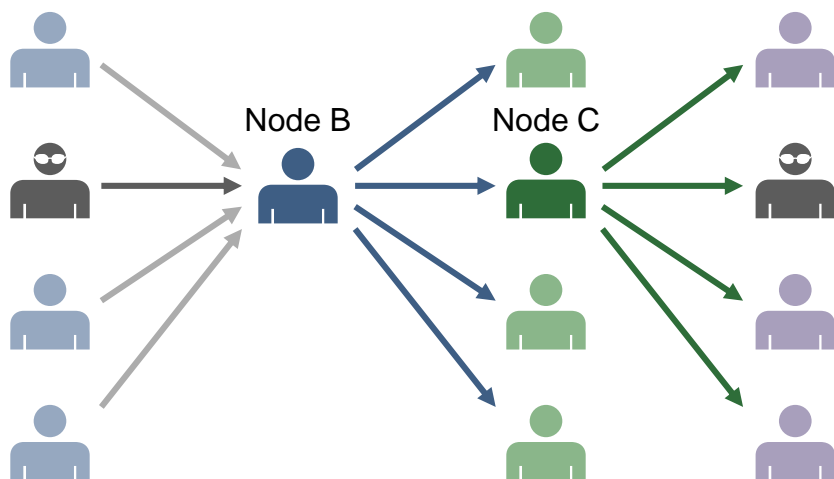
The criminal can also become a relay node. In the figure below, crypto-laundering can be achieved by remitting one's own criminal proceeds to node B and receiving the same amount of clean coins from node A in place of them.

However, several factors are required to carry out this kind of laundering: (1) The sender (Node A) needs to be holding the clean coins, (2) the criminal needs to hide its own identity by using the dark web (Tor hidden services etc.), and (3) the criminal needs to be a hub relay node.
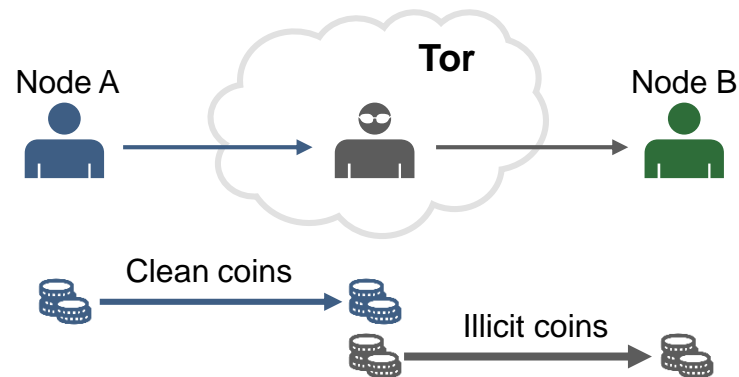
4.2 Crypto-laundering using lightning networks – De-anonymization

De-anonymization of transfer routes requires involved relay nodes to be identified and for all of them to give their support. Regulators need to clarify regulatory interpretations regarding relay nodes in the future as relay remittance using lightning networks is highly anonymous.

Illustration of de-anonymizing relay remittances using lightning networks

1. All involved relay nodes need to be under control

Node B   Node C

2. Estimations based on traffic patterns
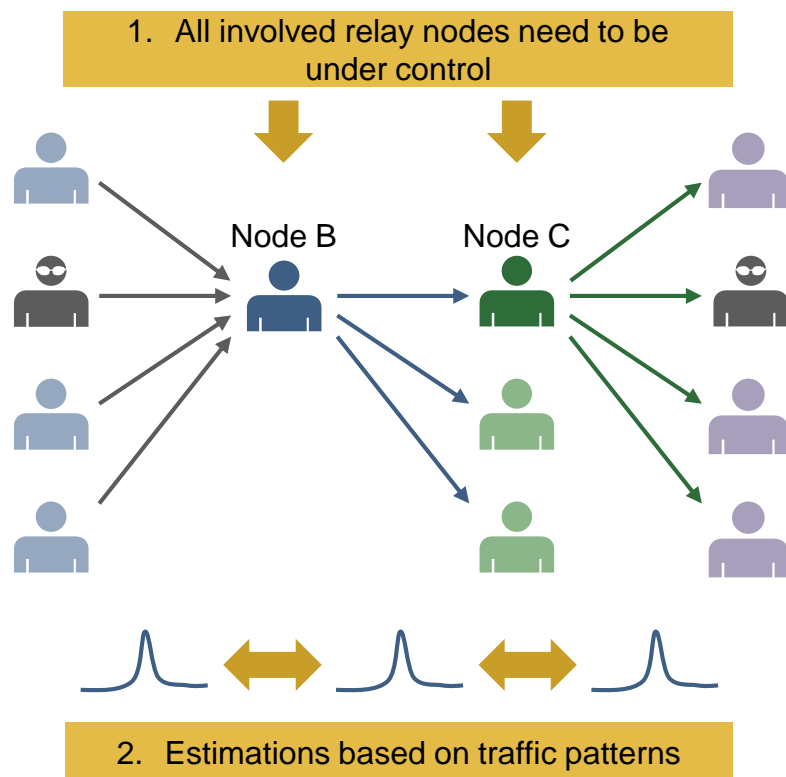
Identification of transfer routes by assessing transaction data across all involved relay nodes requires the relay nodes to not discard their decryption keys.

Therefore, it should be clarified in the future whether relay node providers need to be subject to regulatory supervision such as that of money transmitters.
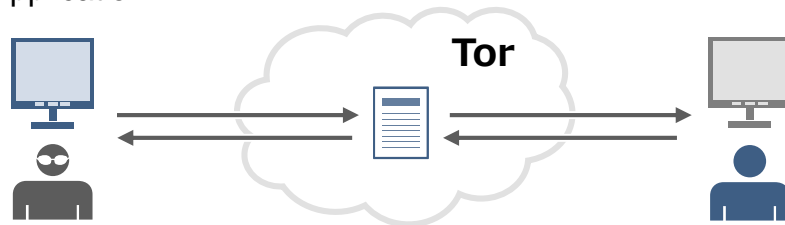
* It has been noted that predicting the prevalence of lightning networks is difficult from the perspective of relay nodes' economic incentives. For example, a relay node needs to have a deposit in each payment channel (initial cost) and cannot use the deposited coins for any other purpose (opportunity cost). Relay remittance fees alone may not be able to cover these costs.

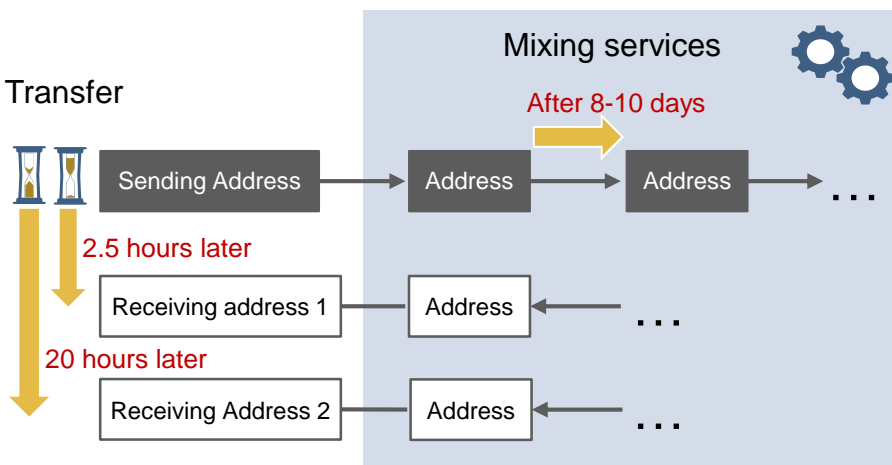# 4.3 Crypto-laundering using mixing services – Overview

We assessed how crypto-laundering is conducted by using two major mixing services. While mixing services were readily available, identifying and tracing transfer routes using blockchain data proved to be quite difficult.

Illustration showing the usage of mixing services

1 Application

Tor

2 Transfer

Mixing services

After 8-10 days

Sending Address → Address → Address → . . .

2.5 hours later

Receiving address 1 ← Address ← . . .

20 hours later

Receiving Address 2 ← Address ← . . .

3 Reception

We considered the case where a criminal carries out crypto-laundering using mixing services.

1. The criminal applies to a mixing service on the dark web. After entering the receiving addresses and the reception time, the deposit address is displayed.

2. The criminal sends the bitcoins to be laundered to the deposit address.

3. Refunds will be made from a completely different address after the specified time.

As the bitcoins were received via a completely different route than just directly from the original remittance address, the relationship between the transferred bitcoins and the received bitcoins is unknown to third parties.

Furthermore, as it is possible to specify multiple receiving addresses and have a time delay for each receiving address, it is considered quite difficult for third parties to connect these receiving addresses.

It is thought to be difficult to specify mixing service addresses or if indeed mixing services have actually been used because an infinite number of addresses can be created.

4.3 Crypto-laundering using mixing services – Other issues

Research suggests that it is difficult to specify the location of mixing service providers because services are primarily offered on the dark web. Although income that mixing services receive from fees is about 1-3% of the total amount of transferred crypto-assets, mixing service providers may be able to conduct business elsewhere.

Characteristics of mixing services
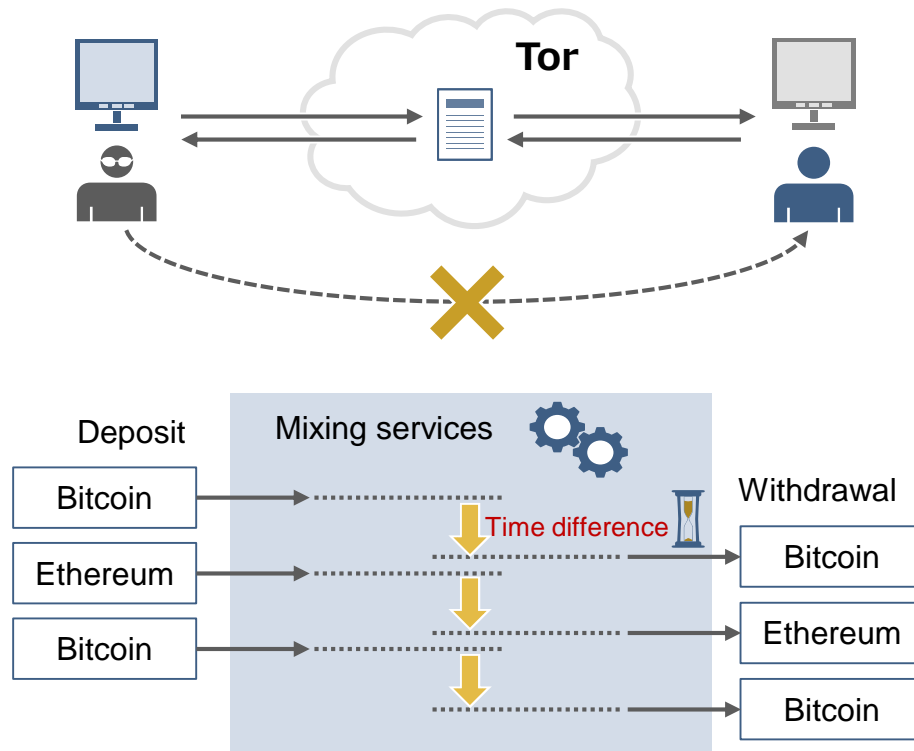
When a mixing service provider uses Tor hidden service, it is quite difficult to identify the location of and entities involved with the service.

It is assumed that mixing service providers deal with a considerable amount of crypto-assets. It is possible that they also can utilize crypto-assets from the balance created by the time difference between deposits and withdrawals.

Furthermore, when mixing service providers accept multiple kinds of crypto-assets such as Bitcoin and Ethereum, they are able to offer crypto-to-crypto exchange services.

Therefore, it is possible that mixing service providers can have other revenue models besides the fee-for-service model.

4.4 Countermeasures using risk scoring tools

We assessed the risks of actual Bitcoin addresses using the multiple risk scoring tools that are currently available. Overall, we confirmed that the estimated risks are not always accurate. Most of the tools could not identify that mixing services were actually being used.

No	Bitcoin Address	Risk Score			
		A	B	C	D
1	1F****************************	███	██	███	███
2	3H****************************		█	██	███
3	16****************************		█	██	███
4	1N****************************	█		█	██
5	14****************************			█	█
6	bc******************************		█	██	███
7	17****************************			██	██
8	3D****************************			█	███
9	34****************************			██	██

Risk scoring was conducted using multiple tools on addresses that were actually being used by mixing services and also those of exchanges, but the estimated risks were different from one tool to another.

- In general, many tools estimated the risks to be inadequately low.

- Only a limited number of tools successfully identified that mixing services were being used.

- Many tools could not correctly estimate the risks when illicit crypto-assets were transferred many times. Some tools did not seem to take into account the links among addresses.

- The risk of addresses that were used many times, such as the ones of exchanges, were estimated to be rather low, even if they were involved in illicit transactions. This means that a criminal can lower these risk estimations by going through such addresses.

5. Conclusions

5.1 Issues that have been identified through qualitative and quantitative assessments

5.2 Recommended countermeasures

Summary of this chapter

- Highly anonymous crypto-laundering is already possible and it is not particularly difficult technologically or mentally to carry out. Anonymization technology is rapidly evolving, and there are concerns that the risks of crypto-laundering are reaching critical levels.

- Traditional regulatory approaches may not to be effective due to the autonomously distributed nature of the crypto-asset ecosystem. Tightening of regulations may result in unintended consequences including an increase in risks that could reduce legitimate transactions rather than illegal ones.

- The findings of this research show that regulators may need to deepen their dialogue with a range of stakeholders in order to make a safe, reliable and fair crypto-asset ecosystem a reality.

- Based on our findings, possible regulatory measures could include the following:

  - Given the fact that technological developments are happening quite rapidly and ensuring the enforcement of laws is difficult on a technological level, it is advisable to clearly define to what extent legislation is required in order to ensure that regulators have the ability to respond to instances of crypto-laundering.

  - It is also advisable for regulators to deepen their mutual understanding with various stakeholders and be more cooperative with them in search of the common goal that is to increase social welfare.
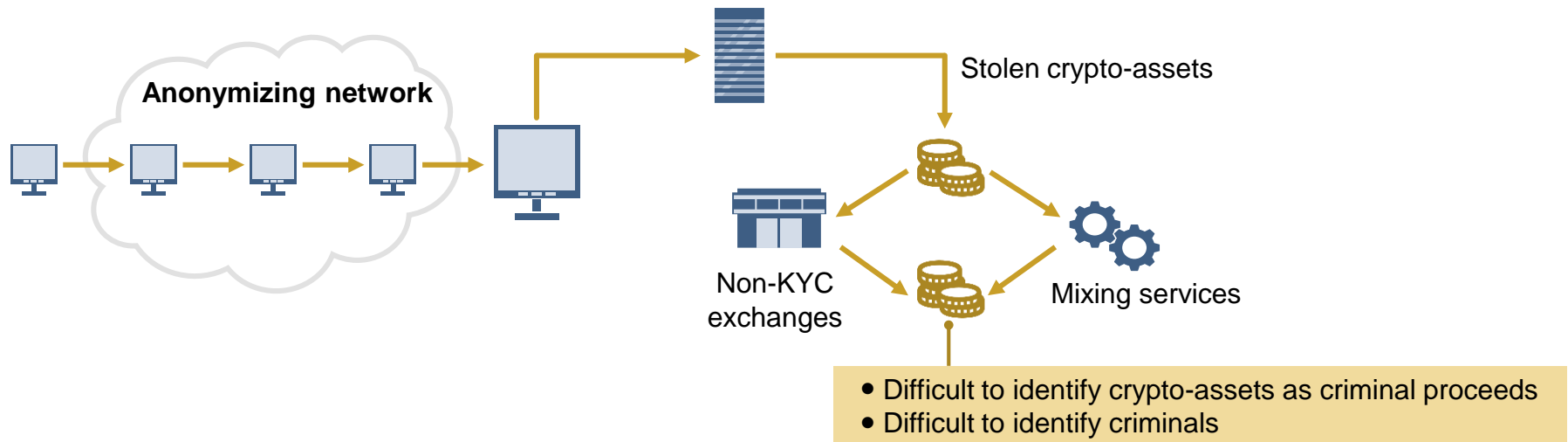
5.1 Issues that have been identified through qualitative and quantitative assessments

When properly anonymized, identifying a criminal is quite difficult from a technological standpoint. Because of this, highly anonymous crypto-laundering is already possible and it is not particularly difficult technologically or mentally to carry out. This means that there are concerns that only regulating exchanges, the intersections between fiat currencies and crypto-assets, may be insufficient.

- De-anonymization highly depends on the errors of criminals and any vulnerabilities in the software used.
- Risk scoring tools are not always effective when estimating the risks of crypto-asset addresses.

Technical limitations when identifying and tracing illicit crypto-assets

Proper risk assessment and the tracing of illicit crypto-assets are quite difficult when the crypto-assets are transferred to mixing services or non-KYC exchanges using anonymizing networks.

Anonymizing network

Stolen crypto-assets

Non-KYC exchanges

Mixing services

- Difficult to identify crypto-assets as criminal proceeds
- Difficult to identify criminals

5.1 Issues that have been identified through qualitative and quantitative assessments
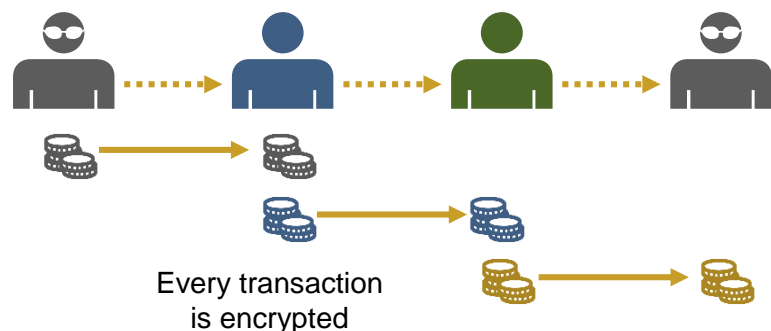
Anonymization technology is being proactively developed for not only crypto-assets like Monero or Zcash but for Bitcoin as well. Therefore, there are concerns that regulating only anonymous altcoins will not be sufficient.

The expansion of crypto-asset trading and the development of crypto-asset technologies will increase the risks of crypto-laundering occurring and these risks could reach critical levels in the future.

Crypto-laundering using lightning networks	Crypto-laundering using new exchange protocols
Transfer routes cannot be identified using blockchain data and network packet data when a relay remittance using lightning networks is carried out.	The trading of different assets without using traditional exchanges, such as DEX and atomic cross-chain swaps, is being developed.

Relay remittance using lightning networks

Every transaction is encrypted

Atomic Cross-chain Swaps

Network of crypto-asset A

Criminal

Network of crypto-asset B

Criminal

Transfer routes cannot be identified by third parties
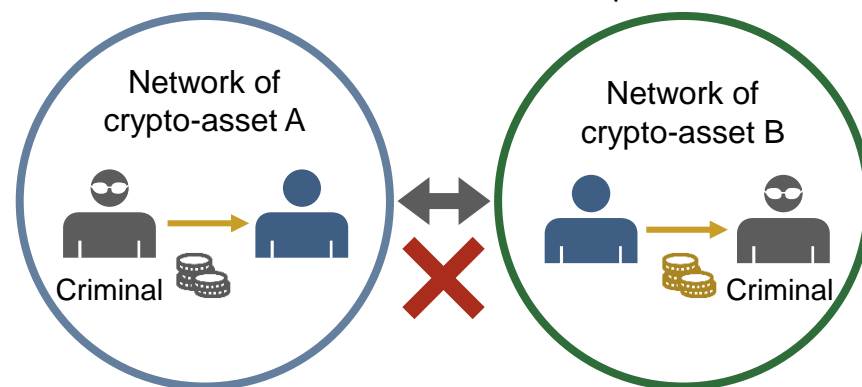
Associating two different transfers Is difficult for third parties

5.2 Recommended countermeasures

Traditional regulation approaches may not be very effective due to the autonomous distributed nature of the crypto-asset ecosystem. Tightening of regulations may result in unintended consequences including an increase in risks that could reduce legitimate transactions rather than illegal ones.

Major characteristics of the crypto-asset ecosystem

Crypto-asset ecosystem

Borderless

Crypto-assets are exchanged globally which means they exceed the jurisdiction of a single country, making law enforcement as well as access to user and transaction records by regulators more difficult.

Autonomous Decentralization

There is not a single administrator. Service providers include offshore companies, individuals, and computer programs that do not require a centralized administrator. They act autonomously to maximize their own profits. Because of this, there are concerns that regulations will have no clear targets, and enforcing such regulations will not be effective.

Openness

There are no barriers preventing technology development and the provision of services. Therefore, there are concerns that targets of regulations will increase and/or remain underground due to the increase of various new service providers.

Tamper-resistant, High availability

Blockchain networks cannot be stopped and changed in an ex-post facto manner which means that there are fears that services will not be able to be stopped and programs modified.

Trustless, Elimination of intermediaries

Crypto-assets allow peer-to-peer trading eliminating intermediaries. Consequently, there are worries that regulators will not be able to detect the existence and the content of transactions.

Technology-oriented

New services are closely related to technological developments. Consequently, there are concerns that regulators will face difficulties when updating regulations and enforcing them in a timely manner.

5.2 Recommended countermeasures

This research found that regulators may need to deepen dialogue with a range of stakeholders in order to make a safe, reliable and fair crypto-asset ecosystem a reality.

Conceptual mapping of monetary flows between ecosystems

- As the crypto-asset ecosystem expands, the type of stakeholders will diversify and the monetary flow among fiat currencies and crypto-assets will become more complicated.

- A lack of mutual understanding among stakeholders will lead the crypto-asset ecosystem to a "war of all against all".
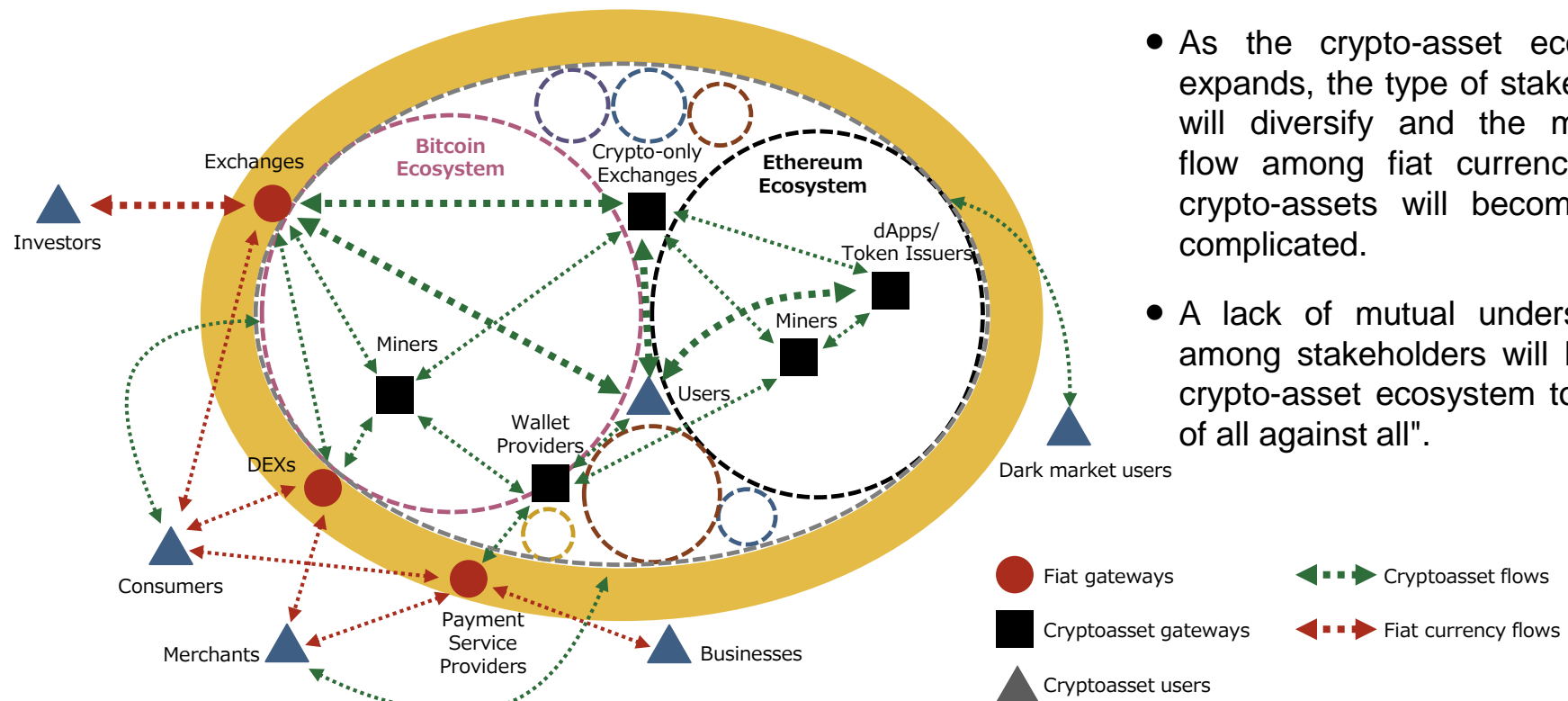
5.2 Recommended countermeasures – Basic concepts

Given the fact that technological developments are rapid and ensuring the enforcement of laws is technologically difficult, it is advisable to clearly define to what extent legislation is required in order to ensure that regulators have the ability to respond to cases of crypto-laundering.

Cases where enforcing regulations is difficult (targets)	Cases where enforcing regulations is difficult (effectiveness)

When conducting AML/CFT, it is essential to block loopholes on a large scale. However, it will be a challenge to close all the laundering routes that lead to criminal proceeds due to the characteristics of the crypto-asset ecosystem.

Overseas exchanges, wallet custodians and individuals

Overseas payment service providers and individuals (Shapeshift, CoinPayments etc.)

Mixing service providers, DEX operators and individuals (Bestmixer.io, Idex etc.)

Relay node operators and individuals affiliated with lightning networks

Service providers and individuals in FATF non-compliant countries

Deployed programs (DEX etc.)

It is difficult to enforce laws and regulations on exchanges, individuals and programs in FATF non-compliant countries, from an authority point of view.
It is also difficult for regulated entities to properly assess the risks of transactions that have been anonymized through various means.

Network of crypto-asset A

Criminal   Mixing services   DEX

Network of crypto-asset B

DEX

Exchanges in FATF non-compliant countries

Network of crypto-asset C

Difficult to estimate any risks properly

Exchanges in our country
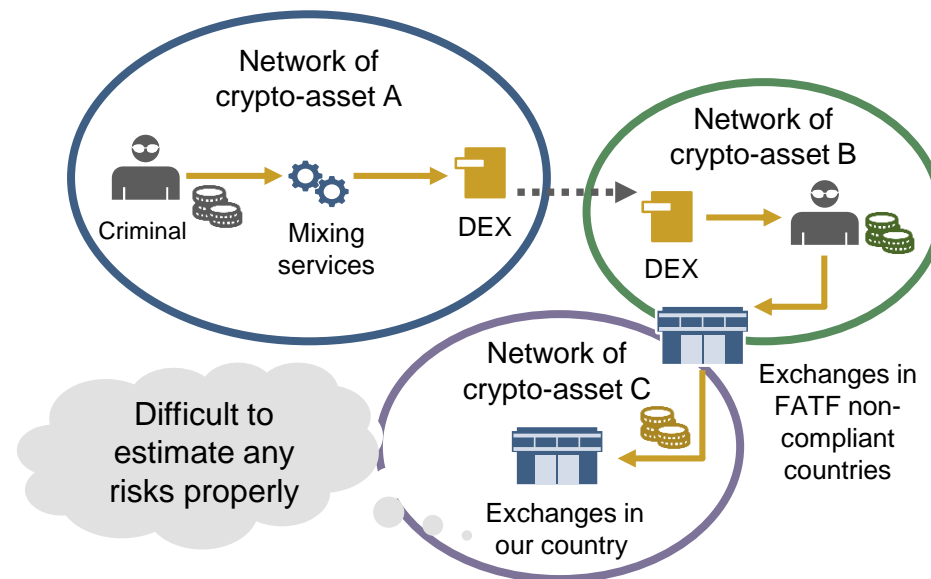
5.2 Recommended countermeasures – Basic concepts

It is also advisable for regulators to deepen their mutual understanding with various stakeholders and increase their cooperation with them to achieve the common goal that is to increase social welfare.

Possible regulatory measures

Approaches needed in the future

AML/CFT outreach in a multilateral framework	Promotion of multilateral cooperation (Incident response team, Incident information sharing)	Promotion of mutual understanding with various stakeholders and cooperative relationships towards common goals
Financial authorities including FATF non-compliant countries	Police, public security organizations and private companies	Developer Communities / Academia and labs / Miners / Users / Service providers

Financial authority

Self-regulatory organization

Financial Institutions — Financial Institutions — Financial Institutions — Financial Institutions — Financial Institutions