identity v anonymity

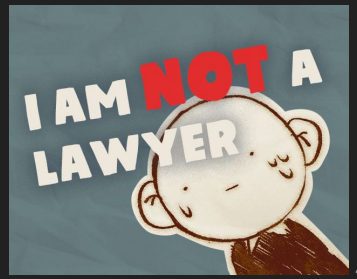
battleground for the future of finance

overview

- key assumptions
- participants
- regulations
- definitions
  - “anonymity enhanced crypto-currency”
- implications
  - MiCA Art. 76 (3)
- response

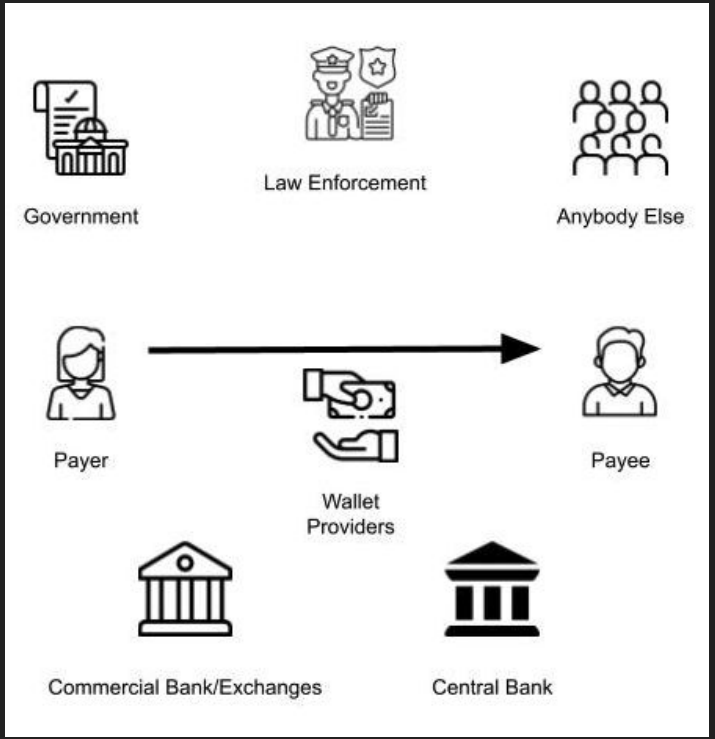
key assumptions

- european regulatory perspective
- XMR to be embedded in the digital payments sphere
- XMR remains a legal crypto-asset



participants

- payer
- payee
- banks // exchanges
- payment service providers // intermediaries // wallets
- government // regulators
- law enforcement agencies
- anybody else
    - {financial data spaces // data lakes // public blockchains}



definitions

Definitions (debated!)

- Anonymity: Data about payer and/or payee identity **does not exist**.
- Pseudonymity: Wallet/account is known, owner is not revealed. Data may or may not exist
- Managed privacy: Central bank provides options (e.g., eCNY)
- Privacy: **Data about the person exists**, but is kept secret to themselves and to self-designated others
- Confidentiality: **Data about transaction exists**, but is accessible on need-to-know basis

Source: Herve Tourpe (IMF) @ https://www.youtube.com/watch?v=kBuMTw6-7pE

regulations (europe skewed)

- FATF Guidance on Virtual Assets
- 6AMLD Package
- MiCA
- PSD2
- eIDAS2
- GDPR
- Data Act
- Data Governance Act
- Digital Services Act

anonymity-enhanced

Anonymity-enhanced CVC transactions are transactions either (a) denominated in regular types of CVC, but structured to conceal information otherwise generally available through the CVC's native distributed public ledger; or (b) denominated in types of CVC specifically engineered to prevent their tracing through distributed public ledgers (also called privacy coins).

Source:
https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

anonymity-enhanced

Anonymity-enhanced cryptocurrency (“AEC”) protocols have the effect of limiting the ability of investigators or other parties to follow transaction flows on their distributed public ledgers, unlike other types of CVC that allow a bank or MSB to identify the full transaction history of the CVC or LTDA value involved in the transaction (i.e. the entire transaction history of the value from the transaction block it was mined).

Source: https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28437.pdf, p83843

implications

"Crypto-assets' transfers would need to be **traced and identified**...

Aim is to ensure crypto-assets can be **traced** in the same way as traditional money transfers

Source:
https://www.europarl.europa.eu/news/en/press-room/20220324IPR26164/crypto-assets-new-rules-to-stop-illicit-flows-in-the-eu

implications

Traceability of transfers of crypto-assets

…all transfers of crypto-assets will have to include information on the source of the asset and its beneficiary…The rules would also cover transactions from so-called unhosted wallets (a crypto-asset wallet address that is in the custody of a private user). Technological solutions **should ensure that these asset transfers can be individually identified.**

Source:
https://www.europarl.europa.eu/news/en/press-room/20220324IPR26164/crypto-assets-new-rules-to-stop-illicit-flows-in-the-eu

implications

The aim is to **ensure that crypto transfers can be traced** and suspicious transactions blocked. The **rules would not apply to person-to-person transfers** conducted without a provider, such as bitcoins trading platforms, or among providers acting on their own behalf.

Source:
https://www.europarl.europa.eu/news/en/press-room/20220324IPR26164/crypto-assets-new-rules-to-stop-illicit-flows-in-the-eu

implications

No minimum thresholds

MEPs decided therefore to remove minimum thresholds and exemptions for low-value transfers.

Source:
https://www.europarl.europa.eu/news/en/press-room/20220324IPR26164/crypto-assets-new-rules-to-stop-illicit-flows-in-the-eu

MiCA Art. 76(3)

Article 76

Operation of a trading platform for crypto-assets

3. The operating rules of the trading platform for crypto-assets shall prevent the admission to trading of crypto-assets that have an inbuilt anonymisation function unless the holders of those crypto-assets and their transaction history can be identified by the crypto-asset service providers operating a trading platform for crypto-assets

Source: http://data.europa.eu/eli/reg/2023/1114/oj

response


ANONYMITY
IS A SHIELD
for the tyranny of the majority
MONERO


DO NOT
SURVEIL
MY MONEY
getmonero.org


AVG Resident Shield
Threat Detected!
While opening file: C:/Program Files/Trojan Horse.exe
Ignore
Info
Heal
Move to Vault


ANONYMOUS
IS NOT
ILLEGAL
getmonero.org


OBFUSCATE
YOUR
IDENTITY
USE MONERO