Money laundering: Virtual assets and cash

Why cash is still king

Fiat currencies such as the US dollar offer:
Stable value, fungibility and international acceptance

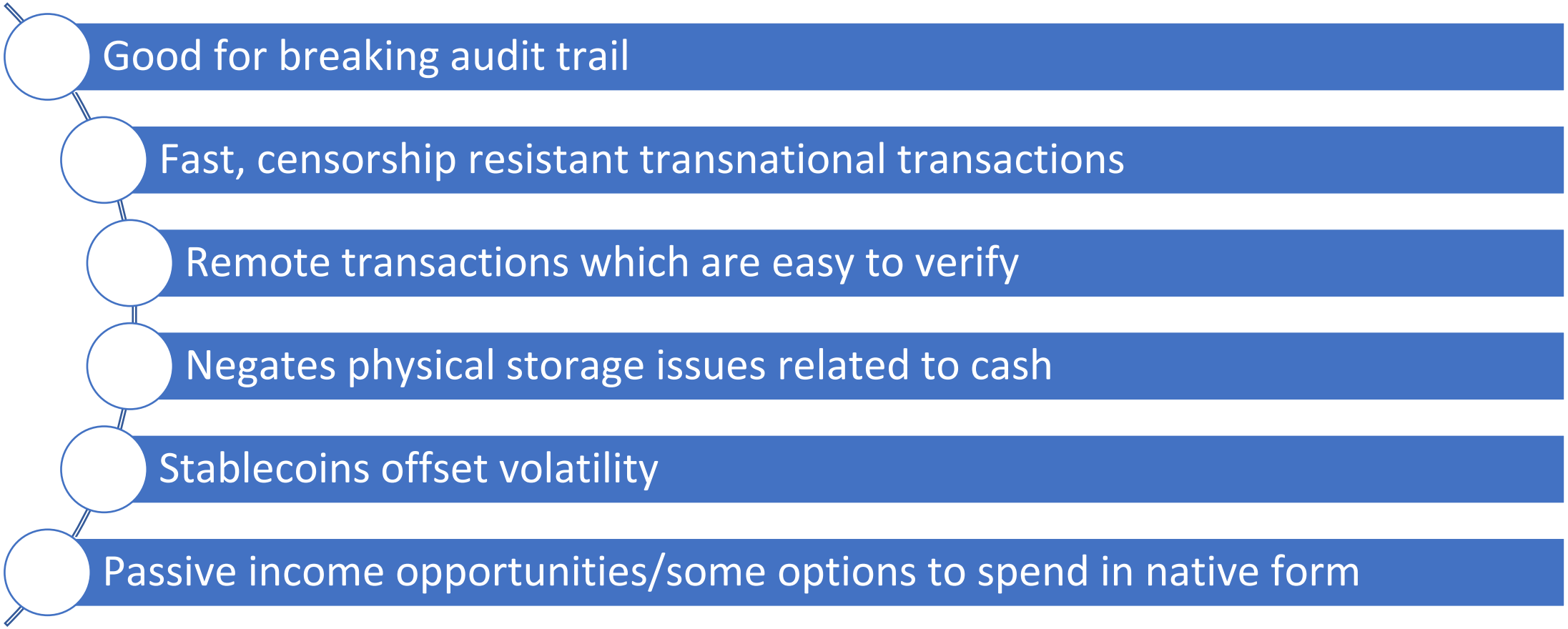
Legal tender laws: Businesses require legal tender to operate/appear legitimate

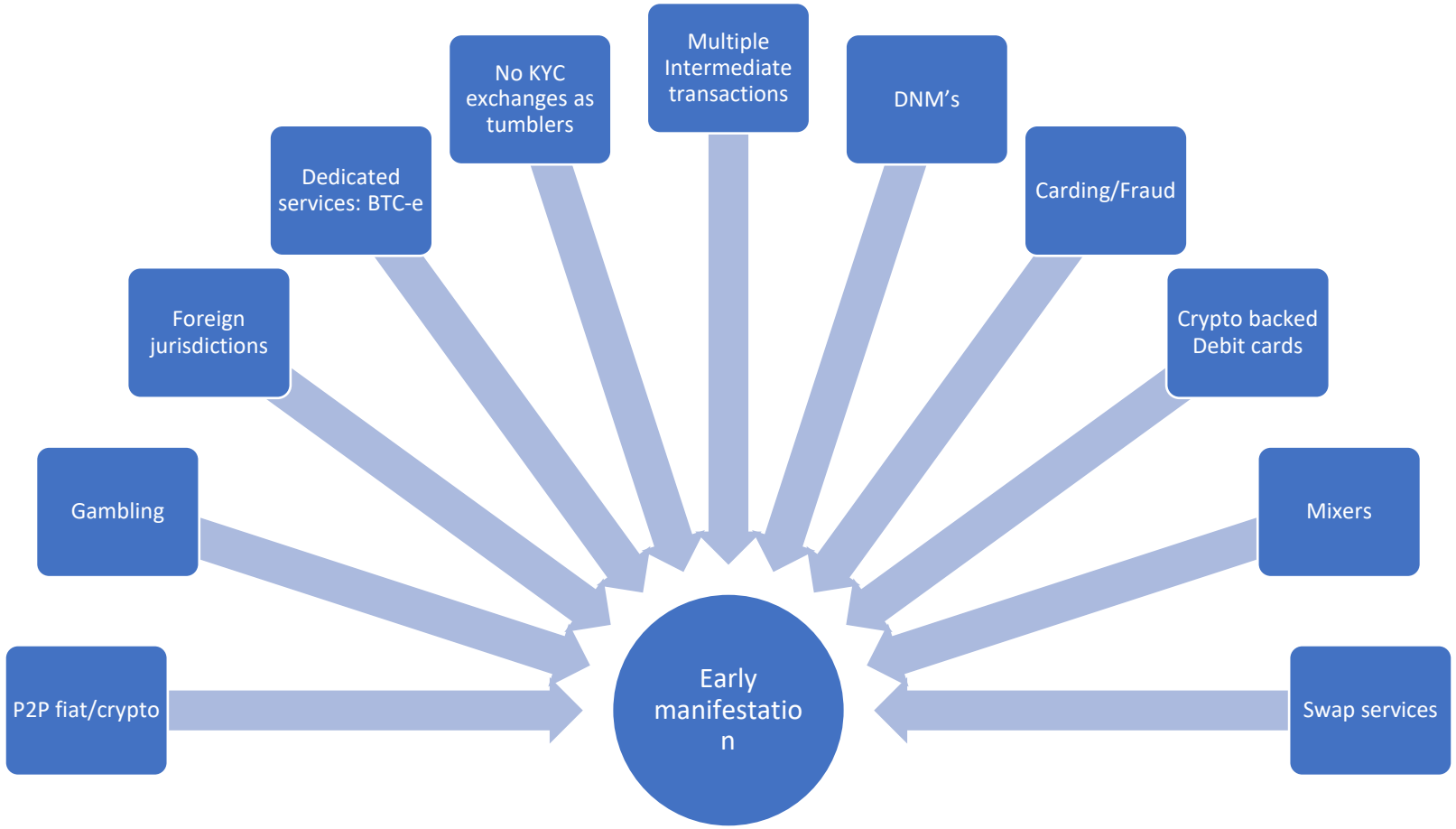
No technical barriers to use/easy to understand

Provides good levels of anonymity and difficult to censor

Shell company opportunities: cash intensive businesses being vehicles for trade based money laundering.

What value do virtual assets add?





- Money laundering between 2009 – 2017 was challenging due to a number of factors:
  - Technical barriers to usage were high: limited tools, not user friendly, unreliable
  - Liquidity in the market was limited
  - Wild volatility in some assets and stablecoin options were only released in 2014

- These challenges meant that much of the criminality linked to early instances of money laundering were involved in digital crime: DNM's, ransomware, protocol compromises, ICO's

Current manifestation

Informal Value Transfer Systems:

Virtual assets sent internationally to trigger movement of assets in another jurisdiction

Obtain benefit from criminality in virtual assets:

Utilise mixing/CoinJoin/peel chains/chain swapping/P2P/Gift cards to break audit trail

Layering activity:

Criminal cash exchanged for virtual assets, sent to exchange for conversion to fiat bank transfer.

Incorporating virtual asset shell companies into methodologies:

Formation of digital payment businesses, creating virtual asset protocols

Investment:

Utilising DeFi/CeFi services to stake assets and earn interest/rewards (also validation).

Professional Money Laundering Networks/Operatives (PMLN/PMLO):

OCG's from broad range of criminality identifying and utilising entities who incorporate virtual assets into methodology

- There are a number of nuances to the incorporation of virtual assets:
  - Less sophisticated methodologies tend to involve the predicate crime offender also being responsible for the money laundering process e.g. sim swapping. They tend to make use of mixer/CoinJoin services and gambling sites.
  - More sophisticated operations will incorporate PMLN/PMLO who have access to large, international money mule/facilitator networks and significant liquidity on exchanges.
  - Digital criminality will also re-invest in services which facilitate further offending e.g. VPN's, VPS's, carding/fraud sites.
  - PMLN/PMLO will utilise various assets as part of the overall money laundering methodology. Within this TBML will often be used to help legitimise/obfuscate the origin of funds. There will also be multiple aspects such as payments to associates, purchasing of goods etc.
  - The layering process can involve variations on the detail outlined. For example an entity may wish to prevent a bank freezing funds so will exchange the fiat currency for virtual assets.

Challenges in utilising virtual assets

- Financial surveillance is becoming ubiquitous: Companies actively correlating data from multiple sources to target money laundering processes. All of the traditional financial sector has caught up with the concept of virtual assets and proactively file suspicious activity reports on customers using such assets.
- International community signing up to common principles on targeting money laundering and data sharing agreements. FATF pressure on any jurisdiction not complying: UAE example.
- Regulation becoming more aggressive: Travel rule, transaction values, registration with regulators, broad suspicious activity indicators, significant cost to supporting privacy protocols, more invasive AML/KYC provisions.
- Many virtual asset networks are heavily centralised and open to asset freezing and censorship.
- Deployment of legislation which utilises broad definitions to describe entities liable to anti-money laundering compliance.
- Blockchain and intel analytic firms solidifying a business case for their services and providing ever more effective surveillance tools.
- The regulated sector provides the liquidity required by money laundering operatives which increases the risks to the process. The unregulated P2P market is difficult to utilise as a means of regularly and efficiently laundering virtual assets at scale.

- Technical barriers are still apparent and many do not understand how to securely self custody assets. This is being exacerbated by the current resolution to this subject which is the creation of 3rd party custodian applications.
- The need to integrate at least a subset of virtual assets into fiat currency means money laundering operations have to become more complex to legitimise this process.
- To become stand alone assets for the proceeds of crime virtual assets would need a circular economy. There are several issues to overcome before this transpires:
- The majority of current adoption is purely speculative. This means that real world use cases are limited and tooling is still nascent.
- Speculation has led to many different virtual assets being created and any attempt to utilise these as money devolves into barter.
- Privacy and thus fungibility is becoming a serious problem. There is a potential for networks to bifurcate into white and black market assets. This would mean the same asset type had differing values and purchasing opportunities.
- Mainstream adoption into commerce and business is still some way off and again the multitude of different assets is potentially undermining this ever happening.
- Some countries have been cut off from the financial sector or have serious problems with inflation. This puts a demand on assets which are stable in value, widely adopted, reliable and fungible. Cash in the form of the US dollar is the epitome of these attributes. As a result international money laundering operations will always need to utilise cash. Virtual assets are not as attractive as they need to interact with fiat on/off ramps to be realised.

The Future

- Central bank digital currencies (CBDC's): Greater control over access and use of fiat currency. Significant societal change required to implement and eradicate cash. AI could be implemented into the wallet to detect suspicious activity, report this to the authorities and freeze funds. If CBDC's do replace cash then it will be difficult to circumvent as likely that legal tender laws will reflect change. AML/KYC changes will also be a part of this, potential that any attempt to not use the CBDC will be seen as suspicious activity. It may also be that additional taxes are levied on any assets that are not CBDC's.
- The ability to surveil an entities entire existence (smartphone applications, smart fitness devices, Bluetooth/WiFi/NFC tracking, financial records, smart home devices, vehicle telematics, facial recognition, IP address surveillance, device metadata) is an avenue which could be leveraged to take AML/KYC measures to a whole new level of intrusion. This could make it very difficult to obfuscate money laundering activity.
- Regulations could seek to have virtual asset protocols fork to incorporate AML/KYC processes into the core components of code. This could be mandated or pressure applied through classifying node operators and miners as entities subject to AML/KYC compliance.
- Criminality will seek to innovate in step with the challenges which arise. It's likely that they will leverage new technology in unforeseen ways. This is however not something which will invalidate traditional methods. There will still need to be a holistic process for effective laundering funds.