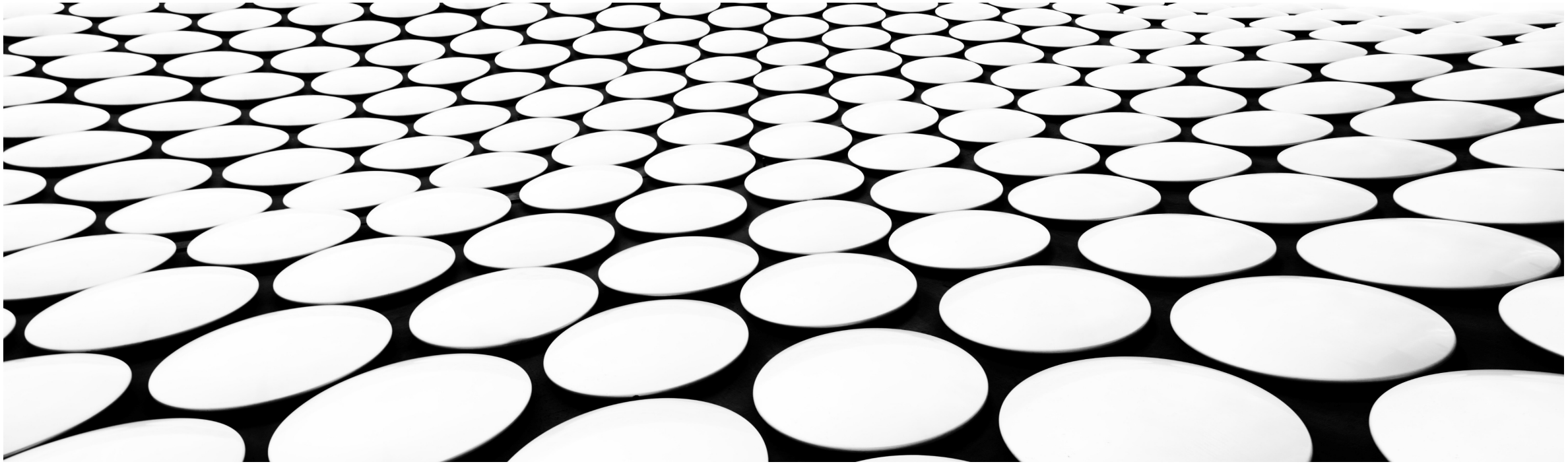
VIRTUAL ASSETS: EVOLUTION NOT REVOLUTION



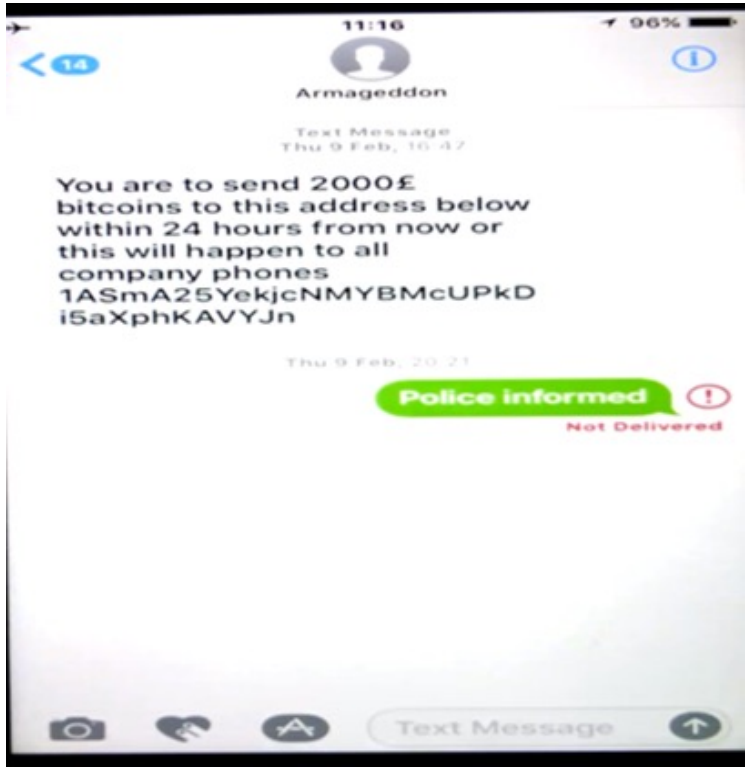
DYNAMIC ADVERSARIES

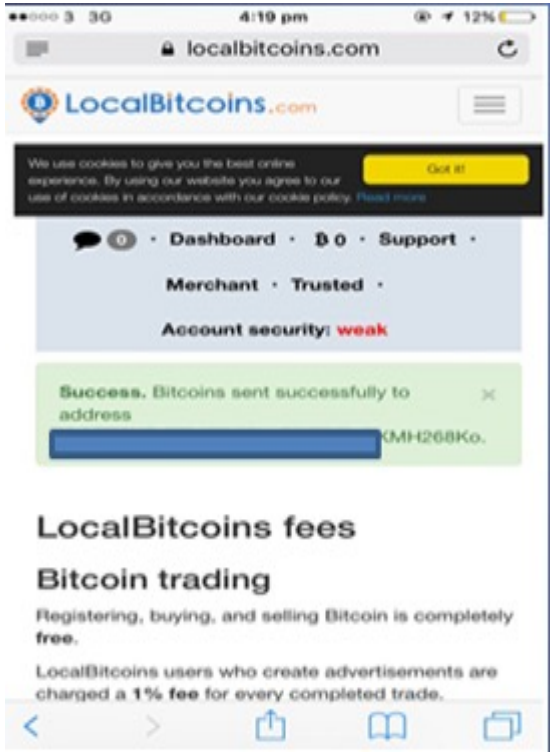
- The ability of criminality to rapidly adapt and develop methodologies according to technological and environmental opportunities is well documented. Cryptocurrencies/virtual assets are no exception with a growing number of investigations identifying their presence in money laundering typologies.
- The technical nature of these assets is often perceived to be a barrier to effectively investigating relevant criminality. There is an argument that this is a flawed perception. This is based on the consideration that money laundering tactics are evolutionary. The strongest features remain and are built upon as criminality adapt to changes in their environment.
- This means that changes to money laundering methodologies are more often incremental and not revolutionary. For investigators many existing skillsets will still be relevant to investigations involving virtual assets as they will only be one aspect of a much broader money laundering strategy.

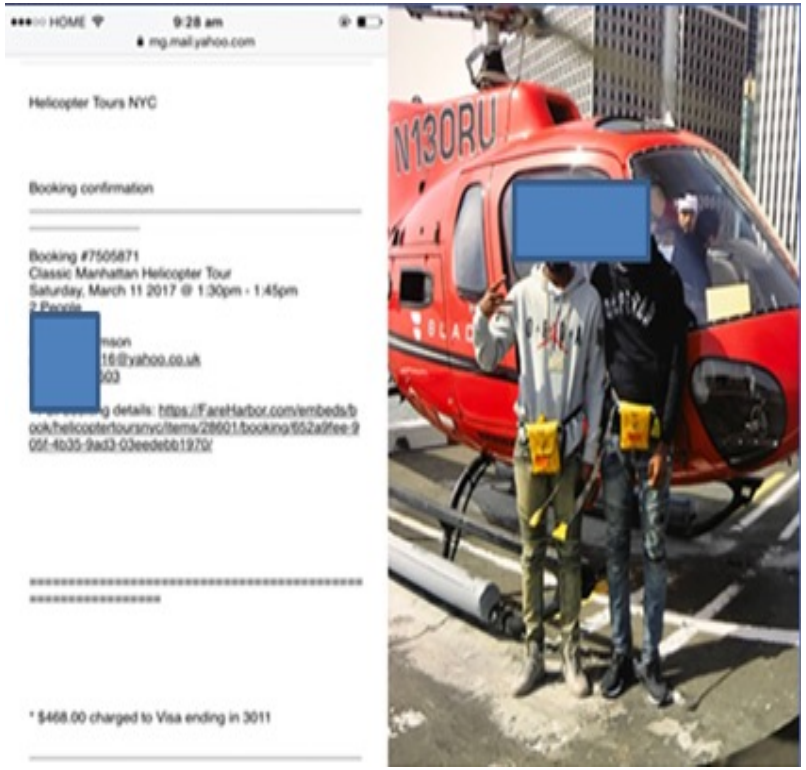
INTRODUCTION

- Money laundering is the key threat emerging from the rapid mainstream adoption of cryptocurrencies/virtual assets. This is not restricted to digital crime.
- Investigations into acquisitive crime of almost every nature are encountering these assets.
- Focusing on purely “cyber crime” is too narrow a focus to effectively deploy LE capability.
- Almost every instance of criminal activity involving cryptocurrencies also encompasses other financial mechanisms.
- As a result it is vital to acknowledge that investigation teams have a mix of financial and digital skillsets.
- The full process of gathering evidence relevant to cryptocurrencies needs to be considered i.e. intelligence, evidence capture, presentation of evidence in court documents, expert witnesses.
- Digital forensics are a key component of this. Whilst there are advanced concepts relevant to this environment (interrogating mining setups, locked hardware wallets, etc.), there is much that can be done with mainstream tools.
- In particular mobile phone examinations can provided key evidence in progressing investigations.

GRAYKEY ACQUISITION

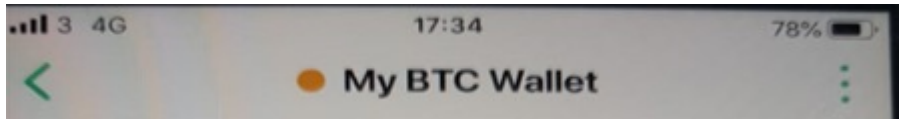




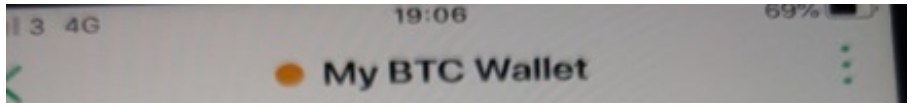


EXAMPLE 2

•Suspect acting as intermediary for associates brokering money laundering deal: highlights they have a *"new associate selling Bitcoin for "paper" (cash), 5% (seller takes 5% extra in cash for amount of Bitcoin sold)".*



From these photo's taken by the suspect it was possible to identify the movement of £300,000 in bitcoin to an OCG member.



In the video identifying the "bitcoin.com" wallet it is possible to identify that the suspect has several other cryptocurrency related applications:

- Shapeshift: Allows for trading and conversion between different cryptocurrencies
- Two Factor authentication applications: Used as added security feature on the majority of cryptocurrency applications to authorise access/transactions.
- Swap wallet: Unknown if this is a cryptocurrency app, search on iOS store cannot find a result for this. Open source also unclear.
- Telegram: Numerous groups and bots available for transacting cryptocurrencies.

EXPLOITING EXISTING SKILLSETS

- As outlined earlier to enjoy the proceeds of crime it is still necessary in most instances to integrate into the traditional financial system. Given this a holistic analysis of financial lifestyle will identify key opportunities to develop an investigation regardless of technical cryptocurrency knowledge.
- Utilising Suspicious Activity Reports to identify use of virtual assets and effectively developing this intelligence does not require any in-depth knowledge of virtual assets. Research on individuals, associated companies, financial accounts, digital footprints and associates can all significantly progress an investigation involving virtual assets.
- Proactively utilising the Proceeds of Crime provisions for restraint orders can negate a number of concerns about dissipation and seizure of virtual assets. Exploiting civil processes such as Unexplained Wealth Orders could also provide opportunities to target those utilising virtual assets for money laundering.
- Reviewing digital forensic opportunities to identify communications relating to money laundering methodologies is not hampered by the presence of virtual assets. If anything the use of cryptocurrencies will leave a greater digital footprint and provide significant evidential opportunities.
- Advanced concepts are not currently common practice as the demand is not at a critical point. This provides opportunity to prepare for such circumstances. Specialist research and development teams could be tasked with this work.

GROUP DISCUSSION

- What proceeds of crime legislation is available in your jurisdiction?
- How effective is the SAR/STR regime in your jurisdiction?
- What digital forensic capabilities do you have in your agency?
- Have you had any experience of investigations involving in cryptocurrency?