



# Cryptocurrency and investigators

WHY THERE IS NOTHING  
TO WORRY ABOUT

# Current climate

---

- **Growing number of investigations involving cryptocurrency:**

- Money laundering techniques affecting a broad range of criminality have evolved to encompass cryptocurrencies. Evidence of this is apparent in intelligence research on the subject.
- Increased subject awareness and regulatory oversight of the cryptocurrency financial sector, has led to a greater volume of SAR/STR reporting.
- Proactive engagement from Virtual Asset Provider's (VASP's) has assisted law enforcement agencies (LEA) in identifying criminal activity on a significant scale.
- Private industry partners are conducting their own investigations and disseminating intelligence to LEA's.

- **Challenges:**

- LEA need to rapidly respond to counter evolving threat. This may be particularly difficult as historically LEA have been renowned for a lack of dynamism.
- Criminal exploitation of new technologies is nothing new, but the rate of development makes it a fast-paced environment. Cryptocurrencies are being embedded into money laundering tactics across a spectrum of criminal activity. This can be especially challenging for LEA's who historically have had inflexible, narrowly focused operational structures.
- Training and knowledge are needed at scale. Despite this there are few tried and tested training pathways.
- Regulation may drive criminal evolution as the financial rewards provide the incentive to innovate around AML/KYC procedures.

# Opportunities

---

Despite the challenges there are also lots of opportunities:

- Many of the most significant blockchains are transparent and publically viewable. This provides investigators with the opportunity to track money flows without court orders.
- There are open and closed source tools available to assist in tracing money flows.
- The vast majority of fiat money gateways are heavily regulated meaning there will often be financial institutions holding relevant user account data.
- There are a growing number of investigators worldwide who are proficient in investigations involving cryptocurrencies. Some jurisdictions have set up task forces dedicated to the subject. This means that there is always someone who you can approach for assistance: internal organisation, partner agencies, regional and international agencies.
- Law enforcement globally have had many successful outcomes in investigations involving cryptocurrencies. Whilst cryptocurrencies have introduced some new considerations they have not radically changed the paradigm. Traditional financial investigation still has a huge role to play in such investigations. Think “Old wine, new bottles”.

# Non technical considerations

---

- Effective collection, analysis and dissemination of intelligence is key. At present there is a tendency to upskill investigators but leave intelligence analysts behind. This needs to be challenged as effectively processing information such as STR's/SAR's will provide significant benefits to investigations.
- Identifying potential sources of intelligence relevant to criminality involving cryptocurrency is also worth considering. There are opportunities to utilise covert tactics, human intelligence sources and private industry intelligence inputs.
- Establishing internal networks is another important consideration. To make greatest use of this training it is necessary to review and repeat the content. This is most efficiently done through engaging internal and external criminal justice colleagues to take part in training and discussion on the topic. Ideally colleagues of all rank should be encouraged to engage so understanding of the subject is disseminated as broadly as possible.
- Policy and procedure needs to be considered at an early point. Engaging senior management and relevant stakeholders to draft and implement policy/procedure in respect of this subject is vital. Without guidance and parameters there is a risk of relevant evidence being undermined.



# Successful investigations

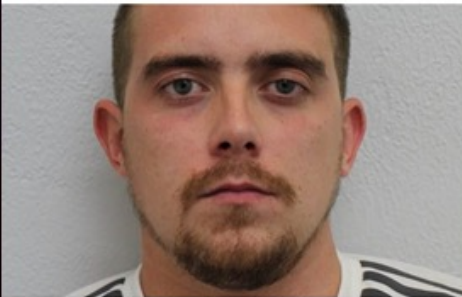
## The Telegraph

Subscribe Now

Coronavirus News Politics Sport Business Money

### Prolific hacker ordered to pay back nearly £1m in Bitcoin to victims

Twitter Facebook WhatsApp Email



Grant West, 27, accrued nearly £1m in cryptocurrency via cyber-attacks on hundreds of companies CREDIT: METROPOLITAN POLICE

By Tom Hoggins  
23 AUGUST 2019 · 4:35 PM


A prolific hacker has been ordered to pay back over £900,000 worth of Bitcoin and other

## itv

NEWS Your Area Topics

### Dark web criminals who sold fentanyl globally from Leeds jailed

FENTANYL | LEEDS | Friday 18 January 2019, 8:11pm



Jake Levene, Lee Childs and Mandy Lowther. Credit: NCA

Three men who ran a dark web business which sold potentially deadly drugs around the world were told their actions had brought "misery" as they were jailed.


Lee Childs, 45, Jake Levene, 23, and Mandy Lowther, 22, were told by a Leeds Crown Court judge that they had run a "sophisticated operation" involving the

## BBC NEWS

### Criminal's Bitcoin seized in Surrey

21 July 2018 | Surrey

Email Facebook Twitter WhatsApp





SURREY POLICE

Serejgs Teresko was jailed for more than nine years for money laundering and drugs offences

More than £1.2m worth of Bitcoins have been

## MailOnline News

787 shares



787 shares

95 comments

- Nigel Wright from Lincolnshire tried to extort Tesco for nearly £1.4million bitcoin
- The 45-year-old was angry at the supermarket chain for 'underpaying for milk'
- He laced children's baby food with metal by planting contaminated jars in Tesco
- Two mothers were moments away from feeding their children the laced food