Office of the Attorney General of the federal state of Hessia
Cybercrime-Center

Prosecution of crimes involving e-currency-transactions

Cai Rueffer
Public Prosecutor
Agenda

1. General rule in prosecuting cybercrime: follow the way of the money
2. Crypto-currencies a new way of payment – what is this?
3. Crypto-currencies make investigations more difficult
4. Possible angles and solutions
5. Sequestration of crypto-currencies
6. Case study: OP Sushi
Following the way of the money as a general rule • Cybercrime is all about anonymity: VPN, Darknet (TOR, I2P ...) etc.

Hi [Redacted]

Please send $1.0M from the USD cash pool account at [Redacted] at the instructions below. Please send this first thing tomorrow morning (Wednesday). This will go as a loan decrease with [Redacted]. Please note we will use only Deutsche Bank for USD transactions as of now and have the details saved for future payments.

- Bank Name: Deutsche Bank Europe S.A.
- USD:
- Account Name: [Redacted]
- IBAN: PL051 [Redacted]
- BIC/SWIFT: DEUTPLPX
Following the way of the money as a general rule
• Cybercrime is all about anonymity: VPN, Darknet (TOR, I2P…)
• Criminals do their best to obfuscate their identity
• In many cases criminals don’t leave any leads to identify them
• A viable way to yet identify criminals is to follow the money
A cryptocurrency (or crypto-currency) is a digital or virtual currency designed to work as a medium of exchange through a computer network that is not reliant on any central authority, such as a government or bank, to uphold or maintain it. Cryptocurrencies are often based on an open-source protocol and use cryptography for security. Bitcoin became the first widely known and accepted cryptocurrency in 2009. Since then, others have become widely used, but only a few dozen have reached a market capitalization above $10 million as of early 2017.

### List of cryptocurrencies

From Wikipedia, the free encyclopedia

This is a list of cryptocurrencies. There were more than 710 cryptocurrencies available for trade in online markets as of 11 July 2016 and more than 740 in total\(^1\) but only a few dozen had reached a market capitalization above $10 million above as of early 2017.

<table>
<thead>
<tr>
<th>Release</th>
<th>Status</th>
<th>Currency</th>
<th>Symbol</th>
<th>Founder</th>
<th>Hash algorithm</th>
<th>Timestamping (POW, POS, or other)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>Active</td>
<td>Aurorcoin</td>
<td>AUR</td>
<td>Baldur Odinsson (pseudonym)(^2)</td>
<td>Scrypt</td>
<td>POW</td>
<td>Created as an alternative to fiat currency in Iceland.</td>
</tr>
<tr>
<td>2009</td>
<td>Active</td>
<td>Bitcoin</td>
<td>BTC (XBT)</td>
<td>Satoshi Nakamoto(^1)</td>
<td>SHA-256d(^3)</td>
<td>POW(^6)(^7)</td>
<td>The first decentralized ledger currency. Cryptocurrency with the most famous, popular, notable and highest market capitalization.</td>
</tr>
</tbody>
</table>

\(^1\) [1](https://en.wikipedia.org/wiki/Cryptocurrency)  
\(^2\) [2](https://en.wikipedia.org/wiki/Scrypt)  
\(^3\) [3](https://en.wikipedia.org/wiki/SHA-256)  
\(^4\) [4](https://en.wikipedia.org/wiki/Bitcoin)  
\(^5\) [5](https://en.wikipedia.org/wiki/Satoshi_Nakamoto)  
\(^6\) [6](https://en.wikipedia.org/wiki/Proof_of_work)  
\(^7\) [7](https://en.wikipedia.org/wiki/Proof_of_stake)
Crypto-currencies as a new way of payment

• No centralised institution which administers or controls currency (e.g., central bank)

• No banks or bank accounts

• No real credit or debt

• No real coins or paper money

• Only wallets, addresses, transactions and the blockchain

**How a Bitcoin transaction works**

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

1. **Creating a new address**
   - Bob and Alice both have Bitcoin "wallets" on their computers.

2. **Submiting a payment**
   - Alice tells her Bitcoin wallet that she'd like to transfer the purchase amount to Bob's address.

3. **Verifying the transaction**
   - Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

4. **Transaction verified**
   - As time goes on, Alice’s transfer to Bob gets buried beneath other, more recent transactions. For anyone trying to modify the details, it would be extremely difficult to do so, because the work that Gary did—because any changes require a complicated sequence of steps to make the blockchain valid for all of the subsequent miners. Such a feat is nearly impossible.
Crypto-currencies as a new way of payment

- No centralized institution which administers or controls currency (e.g., central bank)
- No banks or bank accounts
- No real credit or debt
- No real coins or paper money
- Only wallets, addresses, transactions and the blockchain

Thus:
- Only transactions can be tracked, but the link between the wallets and the owners can't necessarily be established

Example image of a Bitcoin wallet interface.
Crypto-currencies make investigations more difficult:

- Since no ID is required when setting up wallets or exchanger-accounts, transactions can't be linked to certain individuals.
- Since there are no centralized institutions, no one can be addressed with a production order or information request.
- Since crypto-currencies become more and more popular, traditional ways of payment slowly disappear.
- Money laundering becomes much easier.
- Crypto-currencies exist worldwide without any boundaries.
- Increasing use of mixers and tumblers makes it even more difficult.

Tainted bitcoins → CoinMixer.se → Anonymized bitcoins:

Server 1: We mix coins while breaking them to random outputs.

Server 2: We send the mixed coins to another server and we mix them while sending.

We mix the mixed users coins with ours multiple times.
Since transactions are laid down in the blockchain, each transaction of each single wallet can be traced (e.g. blockcin.info)
Possible angles and solutions

• Since transactions are laid down in the blockchain, each transaction of each single wallet can be traced (e.g. blockcin.info) and linked to a certain bitcoin address.

• As a possible tool to identify the owner of a particular wallet, try to cross-check with other platforms.

• At a certain point, the suspects may want to exchange bitcoins into fiat money – try to establish the link.
Sequestration of crypto-currencies

• In general no specific provisions on sequestration of crypto-currencies in domestic laws
• Thus, we apply the general rules for sequestration
• During house search we try to get access to the wallet...
• ...and wire the coins to a police-wallet
• For this purpose we’ve registered with commercial exangers
• Since the exchange-rates are generally extremely volatile, we apply same provisions as for perishable goods (e.g. fish etc.)
• Thus no court order is required to transfer crypto-money into fiat
Case study: Operation Sushi
Any questions?

Thanks for your attention!