



Usable Security of Cryptocurrencies

Katharina Pfeffer

Motivation

Man accidentally threw away \$127 million in bitcoin and officials won't allow a search

Shawn M. Carter | @shawncarterm | 12:30 PM ET Wed, 20 Dec 2017



Sam Hodson | Bloomberg | Getty Images



The FSA is yet to confirm whether or not the exchange has sufficient funds to reimburse customers

Herausforderung

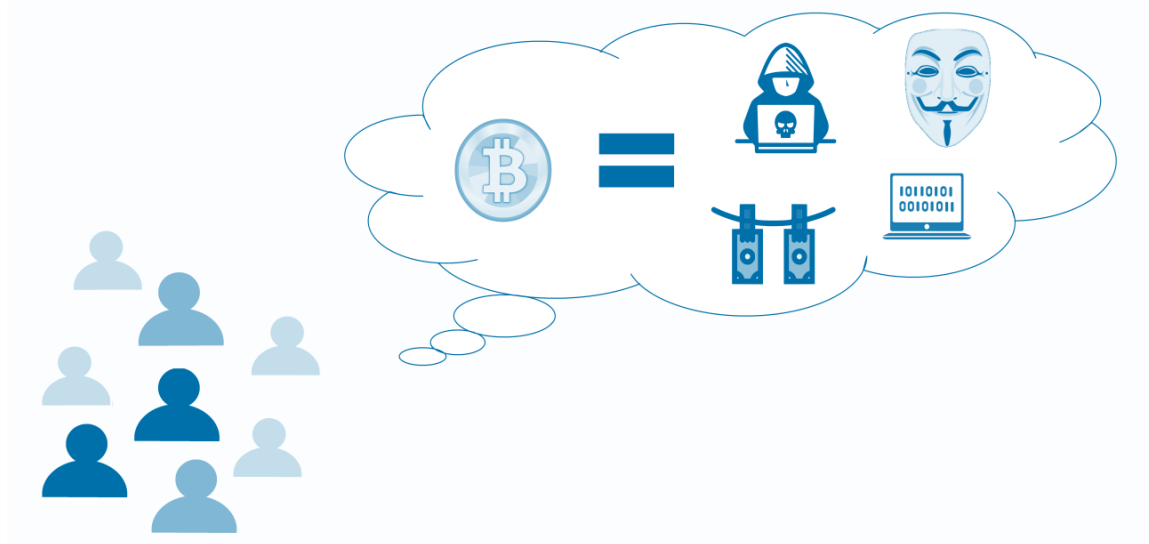
- Fehlvorstellungen von Bitcoin-Nutzern
 - 22% haben bereits Bitcoins verloren
 - 1/3 glaubt Bitcoin sei per-se anonym



- Gefährdung der Sicherheit und Privatsphäre

Unser Ansatz – Schritt 1

- Kognitive Karten der Nutzer verstehen

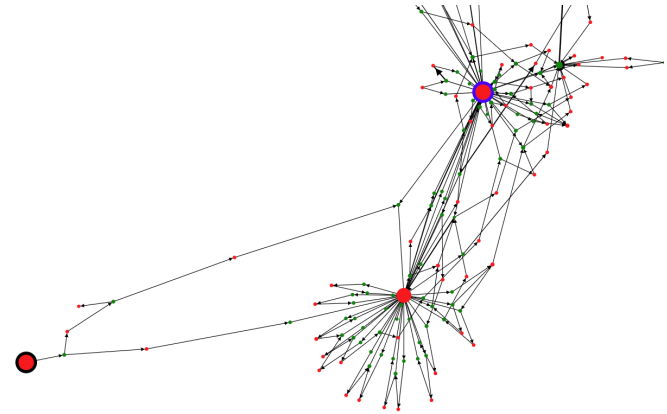


Unser Ansatz – Schritt 2

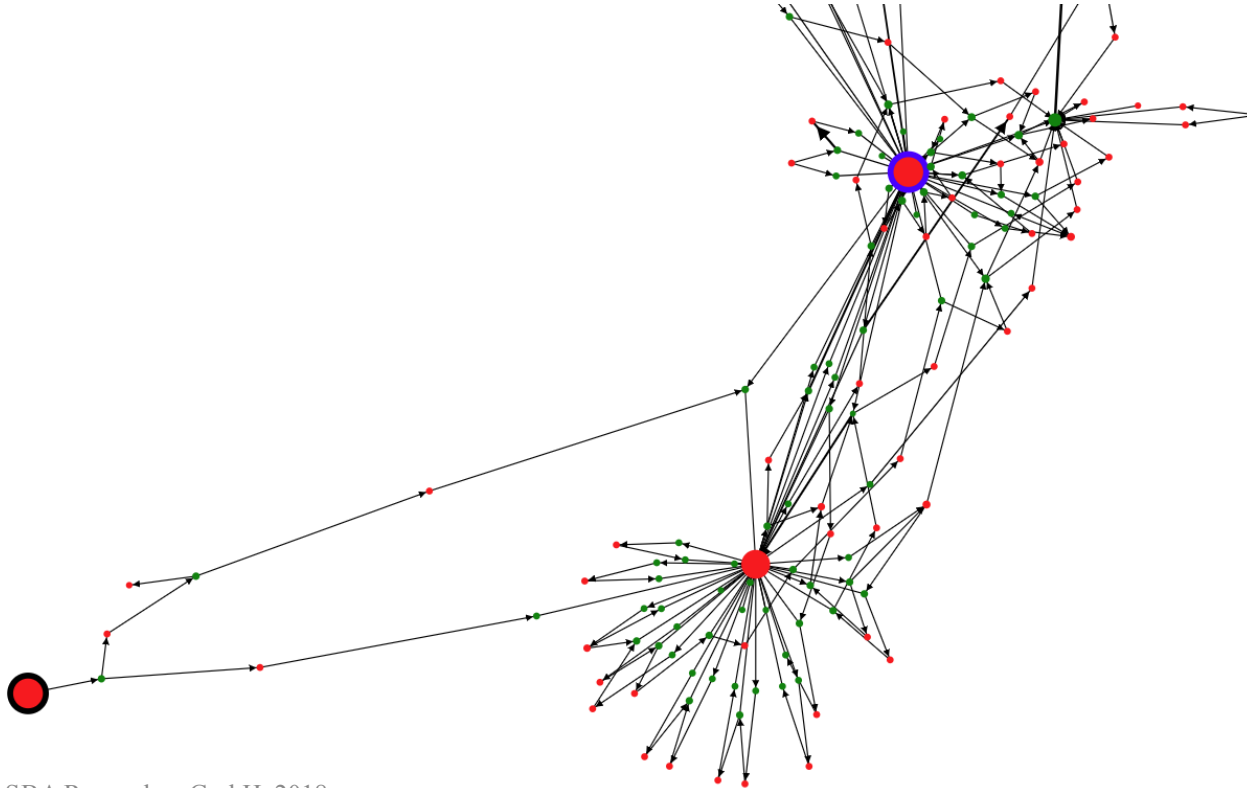
- Tools dementsprechend anpassen
- Blockchain-Visualisierung

```
{ "hash": "f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16",  
  "ver": 1,  
  "vin_sz": 1,  
  "vout_sz": 2,  
  "lock_time": 0,  
  "size": 275,  
  "in": [  
    { "prev_out": {  
      "hash": "0437cd7f8525ceed2324359c2d0ba26006d92d856a9c20fa0241106ee5a597c9",  
      "n": 0  
    },  
    "scriptSig": "304402204e45e16932b8af514961a1d3a1a25fd3f4f7732e9d624c6c61548ab5fb8cd4102  
0181522ec8eca07de4860a4acdd12909d831cc56cbbac4622082221a8768d1d0901" } ],  
  "out": [  
    { "value": "10.00000000",  
      "scriptPubKey": "04ae1a62fe09c5f51b13905f07f06b99a2f7159b2225f374cd378d71302fa28414e7aab  
37397f554a7df5f142c21c1b7303b8a0626f1baded5c72a704f7e6cd84c OP_CHECKSIG"  
    }  
  ]  
}
```

VS.



Blockchain-Visualisierung



Unser Ziel ist...

- den Weg zu ebnen um Kryptowährungen als Zahlungssystem für den täglichen Gebrauch anwendbar zu machen



Katharina Pfeffer

SBA Research gGmbH

Favoritenstraße 16, 1040 Vienna

kpfeffer@sba-research.org