Summary

Virtual currencies are electronic means of payment that are not controlled, issued or guaranteed by any central bank or government. However, they are accepted as a means of payment by legal entities - private and commercial. Their simple and relatively anonymous use, makes that they also play a facilitating role in the criminal, underground economy. Not only is payment in virtual currency enforced in ransomware attacks, but also in underground marketplaces and as part of a cash-out strategy their use is increasing. Because of this increasing criminal use, it is important that both financial supervision and law enforcement further specialize in identifying and attributing virtual money streams.

This research explores the possibilities for detecting criminal assets through these new, virtual money streams. To this end, various modi operandi are identified in the so-called last mile – the part of the criminal value chain where transactions with the 'end user' take place, such as transactions of illegal narcotics or cybercrime tools. This focus ensures that a wide range of modi operandi in which virtual currencies play a role can be explored.

A large-scale data analysis was performed on criminal payment preferences in the last mile and discussions about this in the underground economy. Paradoxically, we find a certain reticence in the use of crypto currencies. On an unstructured platform, such as Telegram groups, crypto currencies are not the natural payment preference in criminal transactions. Moreover, privacy coins are also conspicuously absent as a payment method. Prepaid debit and credit cards, such as PaySafe, do play a prominent role. We show that these - often in practice unregulated - cards are an important virtual payment method in the last mile we studied, for both drug and cybercrime transactions in Telegram groups.

These results were then enriched with expert knowledge from both law enforcement professionals and exchange services for virtual currencies through interviews. In addition, a synthesis of existing scientific research provided further context to the results of the large-scale data analysis. This threefold approach – consisting of literature, expert interviews and measurements in the underground economy – gave us the opportunity to identify discrepancies with current investigative practices. We conclude that the focus of current law enforcement efforts is only on part of the use of virtual currencies and that this part is not always the one with the greatest impact.

Based on the findings of this study, three actionable perspectives have been identified that can contribute to the successful detection, attribution and seizure of criminal, virtual money streams.

First, ongoing 'phenomenon research' can lead to a more effective deployment of investigative resources by increasing insight into and knowledge of criminal use of virtual currencies. Second, the intelligence position of the investigative services can be increased by creating possibilities for identifying, tracing and analyzing virtual money streams. This concerns both an increase in capacity for this purpose as well as tooling and access to relevant data sources. Finally, tightening supervision of the purchase and transactions with prepaid debit and credit cards offers the third actionable perspective. This task should be explicitly assigned to the companies that issue the licenses for these cards.

With the identification of these actionable perspectives, this research has provided a guideline for a focus on the identification and attribution of virtual money streams. Our work can be further expanded by means of case file research, analyses of closed criminal communication platforms and comparing our findings with international experts and data sources. All this contributes to adaptive law enforcement that moves along with the constantly changing role of virtual currencies in organized crime.