FinTech

MDPI

Article

Argumentation Schemes for Blockchain Deanonymisation

Dominic Deuber *, Jan Gruber, Merlin Humml, Viktoria Ronge and Nicole Scheler

Department of Computer Science, Friedrich-Alexander-Universität Erlangen-Nürnberg, 91054 Erlangen, Germany; merlin.humml@fau.de (M.H.); viktoria.ronge@fau.de (V.R.); nicole.scheler@fau.de (N.S.)
* Correspondence: dominic.deuber@fau.de

Abstract: Cryptocurrency forensics have become standard tools for law enforcement. Their basic idea is to deanonymise cryptocurrency transactions to identify the people behind them. Cryptocurrency deanonymisation techniques are often based on premises that largely remain implicit, especially in legal practice. On the one hand, this implicitness complicates investigations. On the other hand, it can have far-reaching consequences for the rights of those affected. Argumentation schemes could remedy this untenable situation by rendering the underlying premises more transparent. Additionally, they can aid in critically evaluating the probative value of any results obtained by cryptocurrency deanonymisation techniques. In the argumentation theory and AI community, argumentation schemes are influential as they state the implicit premises for different types of arguments. Through their critical questions, they aid the argumentation participants in critically evaluating arguments. We specialise the notion of argumentation schemes to legal reasoning about cryptocurrency deanonymisation. Furthermore, we demonstrate the applicability of the resulting schemes through an exemplary real-world case. Ultimately, we envision that using our schemes in legal practice can solidify the evidential value of blockchain investigations, as well as uncover and help to address uncertainty in the underlying premises—thus contributing to protecting the rights of those affected by cryptocurrency forensics.

Keywords: argumentation; legal reasoning; blockchain analysis

JEL Classification: K400

check for updates

Citation: Deuber, D.; Gruber, J.; Humml, M.; Ronge, V.; Scheler, N. Argumentation Schemes for Blockchain Deanonymisation. *FinTech* **2024**, *3*, 236–248. https://doi.org/10.3390/fintech3020014

Academic Editor: David Roubaud

Received: 29 January 2024
Revised: 14 March 2024
Accepted: 21 March 2024
Published: 27 March 2024

1. Introduction

"Follow the money" is arguably the central investigation strategy for any profit-driven offence [1]. Analysing flows of incriminated money is crucial to understanding the business models and inner workings of organised crime groups and the hierarchy of the involved entities, and to identify the groups' members. However, the fight against money laundering is challenging, and criminals utilising virtual currencies, also referred to as cryptocurrencies, aggravate the situation even further. While law enforcement agencies need to expend many resources to follow the complex transnational flows of fiat currencies, blockchain-based investigations pose further challenges. These challenges arise from the fact that cryptocurrencies are generally pseudonymous, with some even being anonymous. Bitcoin [2] is arguably the most famous and widespread cryptocurrency, both for lawful economic purposes and criminal activities [3]. In the early days of Bitcoin, it was already being shown that the currency is not anonymous because it is possible to link multiple pseudonyms belonging to the same person [4–6]. However, supposedly anonymous cryptocurrencies, such as Monero [7] or Zcash [8], have also been the target of deanonymisation attacks [9,10]. All attacks on Bitcoin, Monero, and Zcash are based on partly unreliable assumptions [11]. The reliability of these assumptions determines the quality of the results of an attack. In legal practice, those assumptions are critical for inferring the evidential value of the deanonymisation of a perpetrator. However, no standard practice for deriving and discussing the reliability of these analysis results has been proposed to date. Therefore, we propose argumentation schemes for assessing the reliability of investigations into the Bitcoin blockchain—thus bridging practical cryptocurrency forensics and its scientific analysis. Through their critical questions, our schemes support the critical evaluation of such expert testimonies by legal decision makers.

1.1. Related Work

Argumentation schemes [12], a way to classify arguments according to their underlying principles of convincingness, have been influential in the argumentation theory and the artificial intelligence community [13]. They present the various types of arguments as informal deduction rules, together with accompanying *critical questions*, to aid a human reasoner in evaluating arguments of a particular type.

Given that expert testimonies, as well as the court process itself, is a form of argumentation, it is not surprising that argumentation schemes were applied to legal processes [14]. Walton [15], Walton et al. [16] provide a detailed overview of the applicability of argumentation schemes to representing and analysing legal processes. Similarly, the Toulmin scheme has been applied to legal argumentation [17], but its formalism focuses more on adding structure to individual arguments than on adding hidden information to classes of arguments. This does not mean that Toulmin et al. [17] did not classify arguments, but that Walton-style schemes, with their critical questions, better suit our purpose. For a more complete and general overview of argumentation formalisms, we refer the reader to Kienpointner [18] for informal systems and Baroni et al. [19] for more formal ones. There have also been more formal—and even automated—approaches to legal reasoning based on argumentation theory [14,20]. However, our goal is not to automate parts of the legal process but to aid in evaluating statements about blockchain deanonymisation. While software automates blockchain deanonymisation (e.g., Chainalysis Reactor [21]), in the end, legal decision-makers, i.e., humans, need to evaluate the reliability of the obtained findings.

The use of application-tailored argumentation schemes to capture specialised forms of argument is common practice. Parsons et al. [22] introduce schemes used when providing reasoning regarding trust in entities to specialise arguments building on these statements. Another example from the medical field is the use of specific argumentation schemes to reason about treatment choices in order to aid doctors in their decision making and in producing automated, patient-specific recommendations [23,24].

On the legal side, the evidence must be critically evaluated, as the investigative measures justified by unreliable results potentially impinge upon the fundamental rights of the suspects [25]. Fröwis et al. [26] provide key requirements that must be satisfied to safeguard the evidential value of cryptocurrency investigations, with one of them being reliability. They suggest specific measures to achieve reliability, such as sharing any information necessary to assess reliability, without discussing how they can be implemented in practice. As a step in that direction, Deuber et al. [11] provide a taxonomy for the different assumptions underlying deanonymisation attacks on cryptocurrency users—while only briefly discussing their taxonomy's applicability in legal practice.

1.2. Contribution

In legal practice, the lack of a profound framework means that there is no standard way to assess the reliability of findings from blockchain-based investigations. Less reliable findings might lead to two issues, as follows: First, results with low reliability might not establish the degree of suspicion required by subsequent investigative measures, and thus render them unlawful. In the worst case, any evidence obtained from unlawful investigations might be inadmissible in court, depending on the exclusionary rules of the respective jurisdictions. Second, even if evidence is admissible, low reliability corresponds to low evidential value; thus, the evidence might not be sufficient for a conviction. Given that any findings and the blockchain investigation itself are highly abstract for most parties involved, there needs to be a common ground between technical analysts, investigators, and other legal practitioners to assess these findings.

Our contribution is the application of tailored argumentation schemes to assess heuristics employed in investigations based on the use of the Bitcoin blockchain to deanonymise criminal users. The schemes render the taxonomy proposed by Deuber et al. [11] broadly accessible and easy to use in practice. By presenting the implicit (as critical questions) and explicit premises of those heuristics, our argumentation schemes enable all parties involved in the legal process to systematically assess evidential value. Thus, the schemes can potentially render blockchain-based analyses of Bitcoin transactions more comprehensible and the findings more reliable and conclusive.

2. Preliminaries

2.1. Bitcoin (BTC)

Bitcoin [2] is a cryptocurrency. At its core are transactions that, in their most basic form, are payments. In contrast to fiat currencies, Bitcoin employs a decentralised ledger of transactions. Decentralised means that there is no central authority issuing new units of the currency or settling transactions. Instead, parties maintain the ledger in a peer-to-peer network—a network where all parties are clients and servers simultaneously. The transactions are organised in blocks, which is why the ledger is also referred to as a blockchain. Using a consensus mechanism, the network agrees on which blocks, and thus transactions, should extend the ledger. The network nodes participating in this consensus mechanism are called *miners*.

Transactions consist of a list of inputs and outputs. An output usually states an amount of Bitcoin (v BTC) and the hash h_{pk} of a public key pk, which is also referred to as address a. The public key is part of a digital signature scheme. Such schemes use public and secret key pairs—anyone can check the validity of a signature using the public key, while only the person who knows the corresponding secret key can create a valid signature. An input is a reference to an output of another transaction, which is uniquely described by the hash tx_{hash} of that other transaction and the position out_{id} of the output in the transaction's list of outputs. An example of a transaction with one input and two outputs is given in Figure 1. Usually, transactions have several in- and outputs. Spending the first output of this transaction with an amount of v_1 Bitcoin requires providing a public key pk' whose hash equals h_{pk_1} and a signature that verifies under pk'. This mechanism ensures that, in general, there are no unauthorized transactions, as knowledge of the corresponding secret keys is required to issue a transaction. One property of Bitcoin is that the input amount of a transaction is always entirely consumed. Thus, the second output of the transaction might be a so-called *change* output. A change output pays back to the sender(s) the difference between its input amounts and the amount that the recipient(s) should receive.

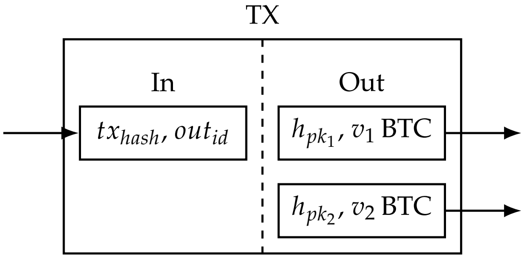

Figure 1. Bitcoin transaction.

Wallets in Bitcoin are programs that allow for transactions to be issued, addresses to be created, and the corresponding secret keys to be stored [27–29]. However, the term is not used consistently, so it can also refer to all addresses controlled by the same entity—which might be stored across several (software) wallets. When only inspecting transactions on the blockchain, it is not immediately obvious which addresses belong to the same wallet.

CoinJoin transactions are a special type of transaction that tries to add anonymity to Bitcoin. The idea is to combine inputs from multiple entities while also having equally valued outputs [30]. In Bitcoin, the concept of transactions being carried out with inputs from multiple users to hinder linking is called *mixing*.

2.2. Bitcoin Investigations

Early research has shown that Bitcoin is not anonymous but pseudonymous, as it is possible to cluster addresses that are likely to be controlled by the same entity, which is referred to as *address clustering*. The most important address-clustering heuristics are the *multi-input heuristic* [4–6] and the *change-address heuristic* [4,5,9]. The multi-input heuristic states that all inputs of a transaction are controlled by the same entity—as previously mentioned in Bitcoin's whitepaper [2]. The multi-input heuristic should not be applied to CoinJoin transactions as they are issued by multiple entities by design. The change-address heuristics utilise the change that often occurs in Bitcoin (see Section 2.1).

The main objective of blockchain investigations is *re-identification*, that is, to determine the natural or legal person who controls an address cluster. This is especially relevant for law enforcement trying to identify persons connected to flows of incriminated virtual currencies. By tracing such transactions and conducting address clustering, they might identify a single relevant address cluster. As addresses typically do not contain any personally identifiable information, the investigation requires re-identification. To facilitate re-identification, address clusters are usually connected with off-chain information—a process also referred to as *attribution tagging* [26]. As its name implies, the tagged information in attribution tagging can be used to identify the actual entity. In practice, the arguably most important attribution information is that an address cluster is related to some cryptocurrency *exchange*—a platform to exchange, buy or sell cryptocurrencies—as law enforcement might request the respective customer data from this exchange.

2.3. Legal Background

Many states have committed themselves to combating cybercrime by ratifying the Convention on Cybercrime [31]. This commitment includes establishing cybercrime offences in their domestic laws and providing investigative measures to facilitate the prosecution of such offences while protecting fundamental human rights and liberties. The domestic laws of the ratifying states dictate the actual balance between the interests of law enforcement and human rights. However, it is crucial to note that the legal issues examined in this section are universal and are not limited to the legal systems or jurisdictions of states that ratified the Convention. This universality is illustrated by considering both the US, representing a common-law jurisdiction, and Germany, indicative of a civil-law jurisdiction—following the example of Deuber et al. [11]. As both states also ratified the Convention, these examples illustrate that the principles of the Convention apply across different legal systems. The starting point for our discussion is the following example case of a typical blockchain-based investigation:

Example 1. *Investigators seized a darknet marketplace (e.g., Wall Street Market [32]) and recovered a local Bitcoin wallet that was presumably used to pay the marketplace's operator. The investigators then employed blockchain analysis software (e.g., Chainalysis Reactor [21]) to discover the wallet that was used by the operator to receive payments. While the discovered operator wallet is a local wallet, the operator is suspected of using another wallet at a cryptocurrency exchange to convert Bitcoin into fiat currency. To prevent the exchange wallet from being linked to the incriminated local wallet, the operator mixed the funds prior to the transfer (e.g., using CoinJoin [30]). Through blockchain analysis, the investigators nevertheless managed to establish a link between the incriminated local wallet and the exchange wallet. Next, the investigators issued a request for the disclosure of customer data to the exchange—which collected these data as part of their Know-Your-Customer policy to comply with anti-money-laundering laws. The goal of this request was to find the natural person that controls the incriminated local wallet. After having identified this suspected operator, the investigators conducted electronic surveillance and executed a search of the suspect's premises.*

In summary, the investigative measures used in the example were the blockchain analysis, a request for the disclosure of customer data, electronic surveillance, and a search of premises. In general, such investigative measures all require a specific degree of suspicion in order to protect the rights of the targeted person.

Under German law, an initial suspicion is sufficient to justify a blockchain analysis (according to Sections 161, 163 German Code of Criminal Procedure (GCCP) [33,34]) or a request for the disclosure of customer data (according to Section 100j GCCP). An initial suspicion must be based on a conclusive and established factual basis (factual quality). Due to lax requirements, these measures may be directed not only against the suspected person but also against other third parties that might somehow be connected [35,36]. There are stronger requirements regarding electronic surveillance pursuant to Section 100a GCCP or a search of premises pursuant to Section 102 GCCP. Beyond the mere 'possibility' of the commission of a crime, in these cases, the suspicion of the crime must be specific and individualised (so-called *qualified initial suspicion*), as well as 'probable' [37,38]. These measures have to be directed only against the accused person [37] and may only involve other persons who are directly connected to the accused person or involved in the crime (see Sections 100a (3) and 103 GCCP).

Under US law, the requirements for the analysis of blockchain data and a request for the disclosure of customer data differ significantly from German law. However, this does not affect the legal issues raised by blockchain analyses, as we will point out below. Both blockchain analyses and the request for the disclosure of customer data are not subject to the probable cause requirement of the Fourth Amendment, given that the third-party doctrine applies [39]. However, electronic surveillance and search of premises are subject to the Fourth Amendment, and therefore require probable cause regarding the degree of suspicion. The Fourth Amendment demands that the suspicion is particularised with respect to the person under surveillance, the premises being searched, or the specific things to be seized.

The most important legal issue concerning blockchain analysis in practice is whether or not the findings of the analysis can establish the required degree of suspicion for subsequent investigative measures. Therefore, the lower requirements for blockchain analysis or a request for the disclosure of customer data under US law do not matter, as the subsequent measures—such as searches of premises—require similar degrees of suspicion as under German law. Thus, the only difference under US law is that the legal issue arises later in the investigation.

To illustrate the legal issue, we return to the example of the darknet marketplace operator. Here, a blockchain analysis was used to link an incriminated wallet to an exchange service. Next, disclosure of customer data was requested from the exchange. Imagine that, solely based on the linkage of the wallets, further investigative measures are conducted against the natural person identified by the customer data. If those measures are electronic surveillance or searches of premises, the required suspicion must be particularised against the person targeted by the measures, both under German and US law. If it is unreliable, blockchain analysis might fail to establish this particularised suspicion. Imagine that the analysis is based on the multi-input heuristic, but the heuristic is applied to CoinJoin transactions. In this case, the analysis would definitely yield false positives as CoinJoin transactions are issued by multiple entities by design. False positives might render the individualisation insufficient, and thus the respective investigative measures would be unlawful.

To summarise, certain invasive and targeted investigative measures require a degree of suspicion that is individualised with respect to the target of these measures. Blockchain analysis based on uncertain assumptions might lead to unreliable findings that are not sufficient to establish the individualisation, and thus the required degree of suspicion, for subsequent investigative measures. If investigative measures are conducted without the necessary degree of suspicion, they are unlawful and thus might render the obtained evidence inadmissible, depending on the exclusionary rules of the respective jurisdiction.

2.4. Argumentation Schemes

Argumentation schemes classify arguments according to their warrant in the sense of Toulmin [40], i.e., their principle of convincingness. They are presented as informal presumptive deduction rules inferring the plausible truth of a conclusion from the truth of multiple premises [12]. For example, the Scheme 1 is tailored towards reconstructing the cause E for a set F of observed findings.

In addition to the deduction rule, representing the informal shape of the argument, an argumentation scheme specifies *critical questions (CQs)* as ways to attack an argument based on the scheme. The critical questions aid both the producer and the receiver of arguments by suggesting relevant statements or relevent questions. There are usually critical questions attacking the individual premises or the conclusion of the argument, as well as ones attacking the applicability of the scheme. Consider, for example, the CQs of the Scheme 1.

Premise: F is a finding or given set of facts.
Premise: E is a satisfactory explanation of F.
Premise: No alternative explanation E' given that is is as satisfactory as E.

Conclusion: Therefore, E is plausible as a hypothesis.

1. How satisfactory is E as an explanation of F, apart from the alternative explanations available so far in the dialogue?
2. How much better an explanation is E than the alternative explanations available so far in the dialogue?
3. How far has the dialogue progressed? If the dialogue is an inquiry, how thorough has the investigation of the case been?
4. Would it be better to continue the dialogue further, instead of drawing a conclusion at this point?

Scheme 1. Abductive Argumentation Scheme [12].

CQs 1 and 2 are direct attacks on the truth of the premises of the rule. CQs 3 and 4 are specific attacks based on the idea that there could be other explanations that have not yet been put forth due to the temporal nature of argumentative dialogues.

By making the premises and possible flaws of an argument explicit, argumentation schemes aid in the critical discussion of expert statements by legal decision-makers and other practitioners, without the need for a deep understanding of the underlying topic. To judge the reliability of a claim from blockchain analysis, it is particularly helpful to have transparency with regards to the underlying assumptions, as they have to be judged on a case-by-case basis [11]. This added transparency can also increase the evidential value of such findings if the reliability of the dependent information is sufficiently well established.

3. Our Argumentation Schemes

In criminal investigations, blockchain analyses are typically conducted to establish a link between an entity and a criminal offence through the involved cryptocurrency addresses. As stated in Section 1.1, software exists that could establish such links in an automated manner. However, the methods used by this software, as well as the employed heuristics, regularly remain opaque. Such insufficient traceability is contrary to the requirements of legal proceedings, which require a high degree of explainability and intelligibility. For this purpose, we present a custom argumentation scheme to argue the involvement of an entity in an offence through the control of an address that is connected to that offence (see Scheme 2).

Premise: Address A is connected to offence O
Premise: Entity E controls address A

Conclusion: Entity E is connected to offence O

1. What circumstantial evidence indicates that entity E controls address A?
2. Could it be that, at the time of offence O, someone else controlled address A instead of entity E?
3. How was address A connected to offence O to indicate that E's involvement is indicated?
4. Are there other indicators that E is connected to offence O?

Scheme 2. Suspicion through Address Control.

We do not need a custom argumentation scheme to represent the link between an entity and an address through the request for data from a cryptocurrency exchange, as this is covered by Argument from Position to Know [12]. This standard scheme covers this case, as exchanges typically collect their customers' personal information as part of the Know-Your-Customer policies, and are therefore in a position to know which customer is using an account.

To establish a link between addresses, software tools implement various heuristics, such as the multi-input heuristic or change heuristics, which can arguably be used by investigators [11]. Due to the nature of heuristics, these arguments will be inherently abductive; thus, our proposed schemes are more specific versions of Scheme 1 or its variant, Argument from Sign [12]. Posing specialised variants for the tools and heuristics that are currently in use is beneficial as the specific premises and critical questions capture the expert knowledge about the specific limitations of the applied method. We propose the Scheme 3 scheme to represent arguments based on the use of such a software tool to establish the link between addresses, thereby forming clusters.

Premise: Software S establishes a link between address A_1 and address A_2.
Premise: Software S is reliable.
Premise: Entity E controls address A_1

Conclusion: Entity E controls address A_2.

1. How does software S establish the link?
2. How reliable is software S? Why is software S considered reliable?
3. Could this link also be established without the use of software S, e.g., by using a different software, human reasoning with the multi-input heuristic, or other non-blackbox methods?
4. What evidence exists that entity E controls A_1?
5. Are there other indicators that E might control A_2?

Scheme 3. Cluster from Software.

Naturally, it is not enough for a software tool to establish a link between addresses without further explanations and evidence backing that claim. Analysts face a myriad of transactions when conducting blockchain analyses. They must assess the results presented by the software for criminalistic and legal reasons. First, analysts must understand the software's processes to infer investigative leads, find connections, and form hypotheses—tasks that cannot be entirely automated. Second, only when they understand the software's results can analysts apply their knowledge of the criminal tactics eventually employed by perpetrators, question the results, and falsify hypotheses they previously posed. Finally, from a legal perspective, the rightfulness of the analysis is crucial, as this affects the lawfulness of further investigations in the pre-trial stages and the evidential value of the findings obtained in the actual trial [11]. However, assessing the results would require that the employed deanonymization software discloses the assumptions that were relied on in the analysis, which are typically not disclosed. Therefore, an investigator would strengthen the findings of the software using manual analysis if the software did not disclose the reasons for linking the addresses. To represent the claims from manual analysis, we present two exemplary schemes that capture the use of the multi-input (see Scheme 4) and the change-address heuristic (see Scheme 5), respectively.

Premise: Transaction T has multiple input addresses.
Premise: Entity E controls some input addresses of T.

Conclusion: Entity E controls all input addresses of T.

1. Could T be a CoinJoin transaction?
2. Could it be that another entity F shares secret keys with E and therefore can control other or all inputs of T?
3. Which input addresses of transaction T does entity E control? What evidence is there for E controlling these addresses?
4. Are there other indicators that E might control other input addresses of T?

Scheme 4. Cluster from Multi-Input.

Premise: Transaction T has multiple output addresses.
Premise: Output address C is a *change* address of transaction T.
Premise: Entity E controls all input addresses of T.

Conclusion: Entity E also controls *change* address C.

1. Could T just have multiple distinct benefactors? Could the change, for example, be donated to a supported unrelated entity?
2. What evidence is there suggesting that client software was used that generates a fresh change address for every new transaction?
3. Are there other indicators that E controls address C?

Scheme 5. Cluster by Change-Address.

For brevity, the argumentation schemes presented in this section only cover the most common Bitcoin blockchain analysis heuristics used in practice, and especially do not cover non-blockchain-specific reasoning. For the latter, we can use the vast array of pre-existing schemes [12]. Together, these schemes can be applied to represent reasoning about Bitcoin blockchain investigations in practice, as we will show in Section 4.

4. Application in the Wall Street Market Case

In order to illustrate our approach and its practical implications, we present the argumentation behind the investigative results of the proceedings against one of the administrators of the infamous Wall Street Market (WSM)—depicted in Figure 2. WSM was one of the largest darknet marketplaces on which illegal narcotics, financial data, hacking software, as well as counterfeit goods were traded between approximately 2016 and its seizure in 2019 [32]. In addition to technical surveillance measures, blockchain-based investigations of Bitcoin transactions conducted by the US Postal Service (USPS) were decisive in identifying the administrators operating the marketplace [29].

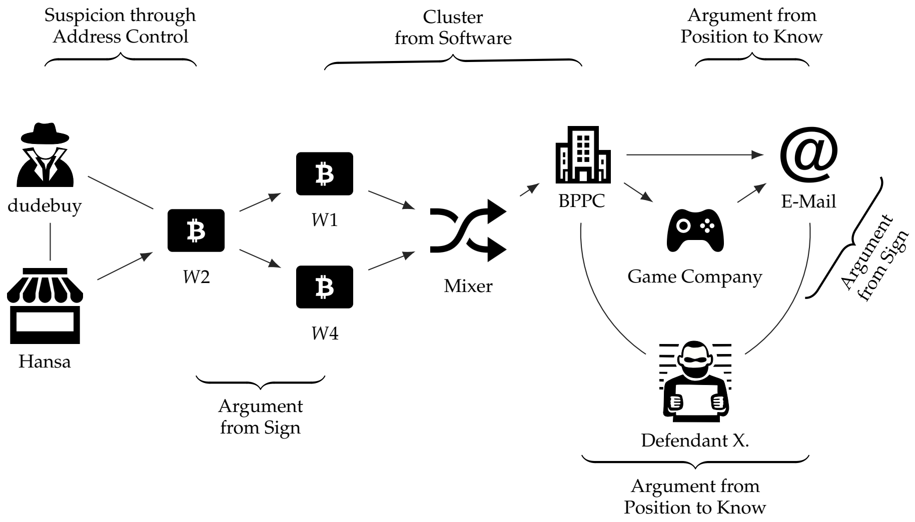

Figure 2. Application of the proposed argumentation schemes to assess the identification of the administrator of the darknet marketplace called Wall Street Market.

The publicly available criminal complaint states that the USPS employed proprietary software of an undisclosed company to conduct its blockchain analyses [29]. Furthermore, neither the exact methods employed during the analyses nor the involved Bitcoin addresses were specified. Instead, the final results—meaning actual investigative findings in the form of off-chain information—were presented on their own. To prove the correctness of the results, it is merely stated that the software was found to be reliable based on numerous unrelated investigations [29]. This might either suggest that the software was utilised as a black box or that the details were (intentionally) not published and kept secret to protect the technical means for tactical reasons. This argumentation might be insufficient to convince legal decision-makers of the correctness of the findings. Thus, we use the criminal complaint to infer the analysis methods that the software might have employed and then apply our argumentation schemes to argue the findings.

The blockchain analyses of the USPS constituted the initial lead that enabled the involved law enforcement agencies to identify 'TheOne'—who acted as one of the administrators of the platform [29]. 'TheOne' is believed to be 'X.' (anonymized by the authors), one of the three defendants, mainly based on the following two findings.

First, the investigators could establish a link between the administrator 'TheOne' from WSM and the user 'dudebuy' from Hansa Market by analysing data seized from both platforms. They found that 'TheOne' used the same PGP public key as 'dudebuy' did at the previously operated and seized darknet marketplace Hansa Market. As a PGP key pair is a highly individual piece of data used to prove one's identity and encrypt communications, it has to be inferred that those two monikers belong to the same real-world entity. As 'dudebuy' used a wallet $W2$ as his refund wallet on Hansa Market, the investigators found an entry point to perform financial investigations concerning this perpetrator, seeming to operate now as 'TheOne'.

Here, the investigators could establish suspicion using the Scheme 2 and infer that the owner of wallet $W2$ seems to be the targeted administrator of the ongoing investigations regarding WSM. This conclusion could be assessed via an evaluation of the critical questions of the scheme. CQ 1—regarding circumstantial evidence indicating address control—leads to a high degree of confidence, as the investigators resorted to seized user data, including an identical PGP public key. However, while CQ 2 (address control by somebody else) does not seem to be of relevance to the investigators at this point in time, CQ 3 (nature of the connection to the offence) reveals at least an indirect involvement of the address in the offence in question.

Second, confident that the owner of wallet $W2$ is the target, the USPS revealed that other wallets that appeared in the investigations, namely wallets $W1$ and $W4$, were funded by transactions originating from wallet $W2$. As this analysis step is basically a rather typical payment flow analysis, which is also employed in traditional money-laundering investigations concerning fiat currencies, it is possible to assess it with a newly formulated argumentation scheme. For example, Argument from Sign or Argument from Abductive Inference would be a suitable fit here [12]. These newly uncovered wallets, in turn, were identified to be the true origin of several payments to various services, which were conducted via a bitcoin payment processing company (BPPC). Prior to these payments, the corresponding funds were supposedly mixed via a commercial mixing service, whose flow of transactions could be 'de-mixed' by the USPS' analysts [29].

Given the fact that no further information regarding the de-mixing is presented in the criminal complaint, we deliberately assume that some sort of software established the link; therefore, the Scheme 3 should be employed to judge the evidential value of this result. The scheme revolves around the mechanism for link establishment (CQ 1), the reliability of the tool itself (CQ 2), human comprehensibility (CQ 3), and additional available evidence (CQs 4 and 5). Here, the most important critical question might be CQ 3, i.e., whether the link could be established by the comprehensible reasoning of a human analyst. As the following requests for the disclosure of customer data were based on this link, it must be considered crucial evidence in this early phase of the investigation. In the course of using CQ 3, a human analyst might establish that the link was a result of the multi-input heuristic. As the multi-input heuristic results in false positives when applied to CoinJoin transactions, it is crucial to challenge whether the involved transactions could be CoinJoin transactions using CQ 1 of the Scheme 4. In this example, the practical relevance of our argumentation schemes becomes particularly apparent. Without the schemes, the argumentation would be limited to whether the analysis software was reliable in the past, not whether false positives were actually excluded in the specific case.

By obtaining user records from the BPPC regarding the payment from wallet $W1$, investigators uncovered an e-mail address, which could be linked to the aforementioned defendant, as it was actually used alongside his real-world identity 'X'. In addition to that, they uncovered that wallet $W4$ served as the suspected source for payments for two accounts at a video gaming company, which were also linked to the suspect, as the records obtained by a subpoena suggest. Furthermore, a second link could be established from another wallet, $W5$, in a similar manner, which was considered to be used to pay for a third account linked to the suspect at the gaming company in a similar manner. Wallet $W5$ was found to be funded by a different wallet that could also be associated with WSM's administrators at a later point in time. While this correlation accumulates reliability, each respective request for the disclosure of customer data might be assessed by employing the Argument from Position to Know scheme [12].

In summary, the USPS's blockchain analyses included the following broader steps: the identification of wallets, the detection of payments between wallets, de-mixing and the association of wallets with off-chain information mainly from other darknet marketplaces, as well as service providers. While the investigators later found various pieces of evidence in the course of their following investigative actions, these steps were central for the case in order to find a starting point for the targeted investigations. We showed that their reliability could be effectively assessed through the utilisation of our argumentation schemes.

5. Conclusions

After having demonstrated the usage of several argumentation schemes for blockchain-based investigations, we conclude by presenting use cases in which the schemes will be especially beneficial and by pointing out directions for future work.

As our argumentation schemes allow for reasoning about the findings of blockchain-based investigations, we see potential use cases wherever such findings have to be communicated to and assessed by the persons involved in respective criminal proceedings. By utilising the schemes, an analyst can clearly articulate the employed heuristics, their individual strengths, and their potential weaknesses. This increases the comprehensibility of such analyses and court proceedings for the decision makers, and also eases the documentation for later verification by an expert witness. Given the high requirements regarding the explainability of legal proceedings, this task cannot be achieved by software in an automated manner at present. Therefore, we intend to support the involved persons with our argumentation schemes. Nevertheless, our considerations could prospectively be integrated into deanonymization software to increase its explainability. To make this example more concrete, standard blockchain analysis tools such as BlockSci [41] could be extended to quantitatively capture the heuristics used when clustering addresses and to qualitatively apply our schemes and critical questions to argue the reliability of the found clusters. Such an extended toolchain also allows for more insights into the reliability of address linking in popular cryptocurrencies, such as Bitcoin. Clear articulation is key to determining the quality of blockchain-based findings, especially if they are not supported, or only weakly supported, by other evidence. On the one hand, applying an argumentation scheme and utilising its critical questions enables law enforcement agencies and the preliminary judge to reason the eventual perpetration of the identified person, and therefore establish a certain degree of suspicion to justify further investigative measures. On the other hand, the rights of suspects can be protected by ensuring that the results obtained from blockchain investigations are of high quality, can be understood, are independently checked for plausibility by the parties to the proceedings, and are actually able to establish the relevant suspicion required by law.

As a result, we consider the application of argumentation schemes in the context of blockchain-based investigations to be a supportive mechanism for making sense of the intangible crime scene and highly abstract commission of cybercriminal offences. Our schemes can be a helpful tool for investigators and prosecutors that strive to identify perpetrators, as well as for legal decision-makers to answer the question of guilt. Finally, the schemes are a step forward in the direction of harmonising the effectiveness and explainability of high-tech investigations.

This work can be extended in multiple directions. Our work only captures the most common blockchain analysis heuristics, while there are many more specific ones [11]. Further schemes for other blockchain analysis heuristics or other cybercriminal investigations could be created, as indicated in Section 3. In addition to this, the critical questions of our schemes could be refined to comprise more specific sub-questions, as for the Argument from Expert Opinion in Walton et al. [12], to capture more expert knowledge.

Author Contributions: All authors contributed equally to the conceptualization, methodology and writing of this work. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by DFG (German Research Foundation) as part of the Research and Training Group 2475 “Cybercrime and Forensic Computing” (grant number 393541319/GRK2475/1-2019). M.H. was also supported by DFG project RAND (grant number 377333057).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: The authors wish to thank Marie-Helen Maras for fruitful discussions.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. Wechsler, W.F. Follow the money. *Foreign Aff.* **2001**, *80*, 40. [CrossRef]
2. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 14 March 2024).

3. European Union Agency for Law Enforcement Cooperation. IOCTA 2021: Internet Organised Crime Threat Assessment 2021. 2021. Available online: https://data.europa.eu/doi/10.2813/113799 (accessed on 14 March 2024).
4. Androulaki, E.; Karame, G.; Roeschlin, M.; Scherer, T.; Capkun, S. Evaluating User Privacy in Bitcoin. In Proceedings of the Financial Cryptography and Data Security, Okinawa, Japan, 1–5 April 2013; pp. 34–51. [CrossRef]
5. Meiklejohn, S.; Pomarole, M.; Jordan, G.; Levchenko, K.; McCoy, D.; Voelker, G.M.; Savage, S. A fistful of bitcoins: Characterizing payments among men with no names. In Proceedings of the 2013 Conference on Internet Measurement Conference, Barcelona, Spain, 23–25 October 2013; pp. 127–140.
6. Reid, F.; Harrigan, M. An analysis of anonymity in the bitcoin system. In *Security and Privacy in Social Networks*; Springer: Cham, Switzerland, 2013; pp. 197–223.
7. The Monero Project. Monero. 2024. Available online: https://www.getmonero.org/ (accessed on 14 March 2024).
8. Zcash Foundation. Zcash. 2024. Available online: https://z.cash/ (accessed on 14 March 2024).
9. Kappos, G.; Yousaf, H.; Maller, M.; Meiklejohn, S. An Empirical Analysis of Anonymity in Zcash. In Proceedings of the 27th USENIX Security Symposium (USENIX Security 18), Baltimore, MD, USA, 15–17 August 2018; pp. 463–477.
10. Möser, M.; Soska, K.; Heilman, E.; Lee, K.; Heffan, H.; Srivastava, S.; Hogan, K.; Hennessey, J.; Miller, A.; Narayanan, A.; et al. An Empirical Analysis of Traceability in the Monero Blockchain. *Proc. Priv. Enhancing Technol.* **2018**, *2018*, 143–163. [CrossRef]
11. Deuber, D.; Ronge, V.; Rückert, C. SoK: Assumptions underlying Cryptocurrency Deanonymizations—A Taxonomy for Scientific Experts and Legal Practitioners. *Proc. Priv. Enhancing Technol.* **2022**, *2022*, 64–84.
12. Walton, D.; Reed, C.; Macagno, F. *Argumentation Schemes*; Cambridge University Press: Cambridge, UK, 2008. [CrossRef]
13. Macagno, F. Argumentation schemes in AI: A literature review. Introduction to the special issue. *Argum. Comput.* **2021**, *12*, 287–302. [CrossRef]
14. Atkinson, K.; Bench-Capon, T.J.M. Argumentation schemes in AI and Law. *Argum. Comput.* **2021**, *12*, 417–434. [CrossRef]
15. Walton, D. Legal Reasoning and Argumentation. In *Handbook of Legal Reasoning and Argumentation*; Springer: Dordrecht, The Netherlands, 2018; pp. 47–75. [CrossRef]
16. Walton, D.; Sartor, G.; Macagno, F. Statutory Interpretation as Argumentation. In *Handbook of Legal Reasoning and Argumentation*; Springer: Dordrecht, The Netherlands, 2018; pp. 519–560. [CrossRef]
17. Toulmin, S.; Rieke, R.D.; Janik, A. *An Introduction to Reasoning*; Macmillan: New York, NY, USA, 1979.
18. Kienpointner, M. *Alltagslogik*; Frommann-Holzboog: Stuttgart, Germany, 1992.
19. Baroni, P.; Gabbay, D.; Giacomin, M.; van der Torre, L. (Eds.) *Handbook of Formal Argumentation*; College Publications: Milton Keynes, UK, 2018.
20. Prakken, H. Historical Overview of Formal Argumentation. In *Handbook of Formal Argumentation Volume 1*; College Publications: Milton Keynes, UK, 2017; Volume 4.
21. Chainalysis Inc. Chainalysis Reactor. 2024. Available online: https://www.chainalysis.com/chainalysis-reactor/ (accessed on 14 March 2024).
22. Parsons, S.; Atkinson, K.; Li, Z.; McBurney, P.; Sklar, E.; Singh, M.; Haigh, K.; Levitt, K.; Rowe, J. Argument schemes for reasoning about trust. *Argum. Comput.* **2014**, *5*, 160–190. [CrossRef]
23. Sanchez Graillet, O.; Cimiano, P. Argumentation Schemes for Clinical Interventions. Towards an Evidence-Aggregation System for Medical Recommendations. In Proceedings of the Informatics and Assistive Technologies for Health-Care, Medical Support and Wellbeing HEALTHINFO 2019, Valencia, Spain, 24–28 November 2019.
24. Sassoon, I.; Kökciyan, N.; Modgil, S.; Parsons, S. Argumentation schemes for clinical decision support. *Argument Comput.* **2021**, *12*, 329–355. [CrossRef]
25. Rückert, C. Cryptocurrencies and fundamental rights. *J. Cybersecur.* **2019**, *5*, tyz004. [CrossRef]
26. Fröwis, M.; Gottschalk, T.; Haslhofer, B.; Rückert, C.; Pesch, P. Safeguarding the Evidential Value of Forensic Cryptocurrency Investigations. *arXiv* **2019**, arXiv:1906.12221.
27. Kus Khalilov, M.C.; Levi, A. A Survey on Anonymity and Privacy in Bitcoin-Like Digital Cash Systems. *IEEE Commun. Surv. Tutorials* **2018**, *20*, 2543–2585. [CrossRef]
28. The Bitcoin Project. Bitcoin Developer Guide-Wallets. 2024. Available online: https://developer.bitcoin.org/devguide/wallets.html (accessed on 14 March 2024).
29. United States District Court for the Central District of California. Criminal Complaint-United States of America v. Tibo Lousee, Klaus-Martin Frost, and Jonathan Kalla-Case No. 19MJ1843. 2019. Available online: https://www.justice.gov/opa/press-release/file/1159706/download (accessed on 14 March 2024).
30. Maxwell, G. CoinJoin: Bitcoin Privacy for the Real World. 2013. Available online: https://bitcointalk.org/index.php?topic=279249 (accessed on 14 March 2024).
31. Council of Europe. Convention on Cybercrime. 2001. Available online: https://www.coe.int/en/web/cybercrime/the-budapest-convention (accessed on 14 March 2024).
32. Department of Justice—Office of Public Affairs. Three Germans Who Allegedly Operated Dark Web Marketplace with Over 1 Million Users Face U.S. Narcotics and Money Laundering Charges. 2019. Available online: https://www.justice.gov/opa/pr/three-germans-who-allegedly-operated-dark-web-marketplace-over-1-million-users-face-us (accessed on 14 March 2024).
33. Safferling, C.; Rückert, C. Telekommunikationsüberwachung bei Bitcoins—Heimliche Datenauswertung bei virtuellen Währungen gem. §100a StPO. *MMR* **2015**, *18*, 788–794.

34. Grzywotz, J.; Köhler, O.M.; Rückert, C. Cybercrime mit Bitcoins—Straftaten mit virtuellen Währungen, deren Verfolgung und Prävention. *StV* **2016**, *11*, 753–759. [CrossRef]
35. Peters, S. § 152 StPO. In *Münchener Kommentar zur Strafprozessordnung*, 2nd ed.; Knauer, C., Kudlich, H., Schneider, H., Eds.; Verlag C. H. Beck: München, Germany, 2024; Volume 2.
36. Rückert, C. § 100j StPO. In *Münchener Kommentar zur Strafprozessordnung*, 2nd ed.; Knauer, C., Kudlich, H., Schneider, H., Eds.; Verlag C. H. Beck: München, Germany, 2023; Volume 1.
37. Rückert, C. § 100a StPO. In *Münchener Kommentar zur Strafprozessordnung*, 2nd ed.; Knauer, C., Kudlich, H., Schneider, H., Eds.; Verlag C. H. Beck: München, Germany, 2023; Volume 1.
38. Hauschild, J. § 102 StPO. In *Münchener Kommentar zur Strafprozessordnung*, 2nd ed.; Knauer, C., Kudlich, H., Schneider, H., Eds.; Verlag C. H. Beck: München, Germany, 2023; Volume 1.
39. *United States v. Gratkowski*, 964 F.3d 307 (5th Cir. 2020). Available online: https://casetext.com/case/united-states-v-gratkowski (accessed on 14 March 2024).
40. Toulmin, S. *The Uses of Argument*; Cambridge University Press: Cambridge, UK, 1958.
41. Kalodner, H.; Möser, M.; Lee, K.; Goldfeder, S.; Plattner, M.; Chator, A.; Narayanan, A. BlockSci: Design and applications of a blockchain analysis platform. In Proceedings of the 29th USENIX Security Symposium (USENIX Security 20), USENIX Association, Boston, MA, USA, 12–14 August 2020; pp. 2721–2738.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.