S. Wendzel et al. (Hrsg.): SICHERHEIT 2024,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2024 153

0 Sterne für die Sicherheit: Wie Kundenbewertungen die Bitcoin-Adressen von Darknet-Händlern verraten

Jochen Schäfer[1], Christian Müller[2], Frederik Armknecht[3]

Abstract: Bitcoin spielt als Zahlungsmethode auf Online-Marktplätzen eine immer größere Rolle, sowohl im legalen als auch im illegalen Raum. Solche Marktplätze verwenden in der Regel ein Bewertungssystem, mit dem Kunden ihre Einkäufe und einzelne Händler bewerten können. Dementsprechend haben Verkäufer ein Interesse daran, so viele positive Bewertungen wie möglich zu sammeln und diese öffentlich zu machen. In dieser Arbeit präsentieren wir einen Angriff, der diese öffentlich verfügbaren Informationen ausnutzt, um diejenigen Bitcoin-Adressen zu identifizieren, mit denen die Händler ihre Auszahlungen von den Marktplätzen erhalten. Wir demonstrieren die Anwendbarkeit des Angriffs, indem wir Bitcoin-Transaktionen auf der Grundlage von Kundenbewertungen für zwei Darknet-Marktplätze zunächst modellieren und dann passende Transaktionen aus der Blockchain abrufen. Auf diese Weise können wir für 44, 4% der auf den beiden Marktplätzen aktiven Händler mindestens eine Bitcoin-Adresse identifizieren.

Keywords: Bitcoin; Darknet; Kryptowährungsforensik

1 Einleitung

Die Popularität von Bitcoin[4] und anderen Krytowährungen ist in den letzten Jahren stark gestiegen. Während die Datenschutzimplikationen von Bitcoin im Allgemeinen bereits umfangreich untersucht wurden, ist dies für die Nutzung von Bitcoin als Zahlungsmittel in E-Commerce-Anwendungen noch nicht der Fall.

In dieser Arbeit[5] zeigen wir, dass Bitcoin-basierte Zahlungssysteme in Online-Marktplätzen zu erheblichen Datenschutzproblemen führen können, wenn ein Angreifer Kenntnisse über die Funktionsweise des Zahlungssystems und über durchgeführte Zahlungen erlangt. Zu diesem Zweck entwickeln wir einen neuartigen Angriff, mit dem Bitcoin-Adressen identifiziert werden können, die mit hoher Wahrscheinlichkeit zu Verkäufern auf Online-Marktplätzen gehören. Im Gegensatz zu früheren Arbeiten ist unser Angriff vollständig

[1] Universität Mannheim, Fakultät für Wirtschaftsinformatik und Wirtschaftsmathematik, 68131 Mannheim, jochen.schaefer@uni-mannheim.de
[2] Universität Mannheim, Fakultät für Wirtschaftsinformatik und Wirtschaftsmathematik, 68131 Mannheim, christian.mueller@uni-mannheim.de
[3] Universität Mannheim, Fakultät für Wirtschaftsinformatik und Wirtschaftsmathematik, 68131 Mannheim, armknecht@uni-mannheim.de
[4] Im Kontext dieser Arbeit bezeichnen wir das Protokoll als *Bitcoin* (großgeschrieben) und die zugehörige Währungseinheit als *bitcoin (BTC)*.
[5] Hierbei handelt es sich um eine Zusammenfassung und Übersetzung von zuvor bereits auf dem *Privacy Enhancing Technologies Symposium 2022* präsentierten Ergebnissen.

automatisiert und stützt sich ausschließlich auf *öffentliche* Informationen. Wir demonstrieren die praktische Anwendbarkeit unseres Angriffs am Beispiel der beiden Darknet-Marktplätze Cryptonia Market und Cannazon. Dabei können wir Bitcoin-Adressen von 308 Cryptonia Market- und 45 Cannazon-Verkäufern identifizieren, zusätzlich auch Adressen von Kunden und den Marktplätzen selbst.

2 Forschungsstand

In einer zu dieser Arbeit methodisch ähnlichen Untersuchung zeigen Goldfeder et al. [Go17b], dass ein externer Beobachter die Bitcoin-Adressen von Kunden eines Onlineshops mit personenbezogenen Daten verknüpfen kann. Dies geschieht anhand des Bestellvolumens und des Zeitstempels eines Kaufs. Der Angreifer ist dabei ein Web-Tracking-Dienst oder ein anderer Dienstanbieter, der Bestelldetails über Datenlecks in der Implementierung des Online-Shops erhält. Zwar sind die Datenschutzimplikationen dieser Ergebnisse schwerwiegender als unsere, allerdings geht dies auch mit einem deutlich stärkeren Angreifermodell einher. Zudem ist eine ex-post Durchführung des Angriffs nicht möglich.

Chen et al. [Ch19] untersuchen die Zahlungssysteme von Darknet-Märkten. Die Autoren führen eine deskriptive Analyse des Zahlungsvorgangs für sechs große Kryptomärkte durch und untersuchen die Datenschutzimplikationen der unterschiedlichen Zahlungsabwicklungen. Durch das Tätigen von Testkäufen sind sie zudem in der Lage, Händleradressen zu identifizieren. Im Unterschied zu unserer Arbeit ist hier aber ein aktiver Angreifer erforderlich, der selbst Käufe tätigt.

Jawaheri et al. [Ja19] zielen darauf ab, Benutzer von Tor Hidden Services durch ihre Bitcoin-Zahlungen zu identifizieren. Zu diesem Zweck führen die Autoren groß angelegte Auswertungen von Twitter-Posts und dem `BitcoinTalk.org`-Diskussionsforum durch. Dabei gelingt es ihnen, Verbindungen zwischen identifizierten Benutzern von Online-Communitys und dem Darknet-Markt Silk Road herzustellen. Allerdings beruht der Angriff darauf, dass Bitcoin-Benutzer ihre persönlichen Bitcoin-Adressen selbst aktiv veröffentlichen.

Sabry et al. [Sa19] identifizieren Benutzer von `LocalBitcoins.com`. Sie verwenden hierfür öffentlich verfügbare Informationen über abgeschlossene Transaktionen sowie aktive und vergangene Angebote auf der Website. Ihr Ansatz ähnelt unserem dahingehend, dass er die Charakteristika einer Plattform ausnutzt und ausschließlich auf öffentlich verfügbaren Informationen beruht. Voraussetzung ist allerdings auch, dass ein Angreifer bereits im Vorfeld weiß, welche Adressen zu `LocalBitcoins.com` gehören. Dies ist im Fall dieser speziellen Website zwar durchaus realistisch, jedoch kann diese Annahme nicht unbedingt auf andere Bitcoin-basierte Zahlungssysteme verallgemeinert werden.

Unserer Ansicht nach geht unsere Arbeit über den bisherigen Forschungsstand hinaus, da sie eindeutige Zuordnungen zwischen Bitcoin-Adressen und Verkäuferprofilen auf einem Markt herstellt, dabei *vollständig automatisiert* ist, ausschließlich *öffentliche Informationen* verwendet und *keine Interaktion* zwischen Angreifer und Markt oder Verkäufern erfordert.

3 Hintergrund

Analog zu früherer Forschung [Jo18; MMG18] interpretieren wir die Bitcoin-Blockchain als komplexen Graphen, in dem Adressen, Transaktionen und Blöcke verschiedene Arten von Knoten bilden, die über gerichtete Kanten miteinander verbunden sind. Abb. 1 gibt einen kurzen visuellen Überblick darüber, wie diese Interpretation in einer Graphendatenbank umgesetzt werden könnte. Die Attribute und zugehörigen Datentypen sind in den beigefügten Infoboxen aufgelistet, Schlüsselwerte sind unterstrichen.

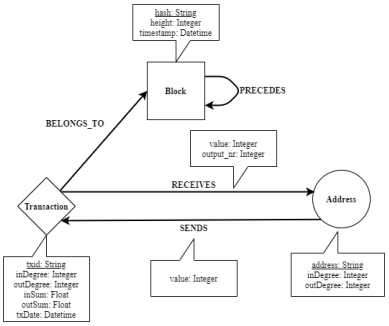


Abb. 1: Datenbankschema (basierend auf Sommer [So19]).

Neben der Bitcoin-Blockchain spielen auch die untersuchten Marktplätze eine Rolle. Auf einem solchen Marktplatz $\mathcal{M}$ verkauft mindestens ein Verkäufer $\mathcal{V}$ Waren und Dienstleistungen an mindestens einen Kunden C. Als Bitcoin-Wallets bezeichnen wir dabei die Mengen der unter Kontrolle des Kunden bzw. Händlers stehenden Adressen $C = \{a_C^1 \dots a_C^c\}$ und $\mathcal{V} = \{a_\mathcal{V}^1 \dots a_\mathcal{V}^v\}$. Die Wallets werden dabei mit den gleichen Symbolen referenziert wie ihre Besitzer.

Kauft ein Kunde C ein Produkt von einem Verkäufer $\mathcal{V}$, so kann die entsprechende Bestellung als das Tupel $(C, \mathcal{V}, \tau, \alpha) = \vec{o}$ beschrieben werden, wobei τ der Zeitpunkt und α das Gesamtvolumen der Bestellung ist.

Um die bestellten Produkte zu bezahlen, erstellt C eine Bitcoin-Transaktion, die wir als $\vec{t}$ modellieren: $\vec{t} = (A_{\text{in}}, A_{\text{out}}, \tau_{\text{t}}, \alpha_{\text{t}})$, wobei $A_{\text{in}} = \{a_{\text{in}}^1, \dots, a_{\text{in}}^i\}$ und $A_{\text{out}} = \{a_{\text{out}}^1, \dots, a_{\text{out}}^o\}$ die Mengen von Sender- und Empfänger-Adressen sind. τ_{t} ist der Zeitstempel der Transaktion und α_{t} das Transaktionsvolumen. A_{in} umfasst mindestens eine Adresse a_{in}, welche in $\vec{t}$ einzahlt. Entsprechend enthält A_{out} mindestens eine Adresse, welche Bitcoin von $\vec{t}$ empfängt. Die gleiche Adresse kann in beiden Mengen enthalten sein, beispielsweise, wenn „Wechselgeld“ an den Absender zurückgegeben wird.

Um das Problem des fehlenden Vertrauens bei Geschäften zwischen Kunden und Händlern zu minimieren, bieten Marktplätze üblicherweise einen Treuhanddienst an, mit dem eine faire Kaufabwicklung sowohl gegenüber C als auch gegenüber $\mathcal{V}$ garantiert werden soll [Go17a]. Wird dieses System genutzt, zahlt C den Kaufpreis zunächst in einer Transaktion $\vec{t}_{\text{dep}}$ auf eine vom Marktplatz kontrollierte Einzahlungsadresse a_{dep} ein. $\mathcal{M}$ hält die Gelder dort solange

in treuhänderischer Verwahrung, bis der erfolgreiche Abschluss der Bestellung von beiden Seiten bestätigt wurde. Im Falle von Problemen kann C eine Beschwerde bei $\mathcal{M}$ einreichen, der dann eine Lösung vermittelt. Wenn keine Probleme auftreten, gibt $\mathcal{M}$ die Zahlung frei, d.h. der Kaufpreis wird in einer Auszahlungstransaktion $\vec{t}_{\text{pay}}$ auf eine vom Verkäufer definierte Auszahlungsadresse $a_{\mathcal{V}}$ überwiesen. Je nach Implementierung kann $\mathcal{M}$ eine dedizierte Treuhandadresse a_{esc} verwenden, oder aber die Gelder auf der Einzahlungsadresse belassen. In letzterem Fall gilt dann $a_{\text{dep}} = a_{\text{esc}}$. Üblicherweise verlangt $\mathcal{M}$ eine Gebühr von den Verkäufern, meist in Form einer Verkaufsprovision φ, die sich anteilig aus dem Kaufpreis α ergibt. Die Höhe des Anteils kann von Faktoren wie der Produktkategorie oder dem Ruf des Verkäufers beeinflusst werden, wobei p_{min} die minimale und p_{max} die maximale prozentuale Gebühr sind. Somit gilt: $\varphi_{\text{min}} = \text{p}_{\text{min}} \cdot \alpha \leq \varphi \leq \text{p}_{\text{max}} \cdot \alpha = \varphi_{\text{max}}$.

Auch wenn ein Treuhandsystem vorhanden ist, müssen Kunden immer noch den Verkäufern vertrauen, dass sie Produkte von angemessener Qualität verkaufen. Daher bieten Marktplätze in der Regel ein Bewertungssystem an, mit dessen Hilfe C Bewertungen für Verkäufer und/oder Produkte hinterlassen kann. Eine solche Bewertung enthält immer Informationen zum bewerteten Verkäufer oder Produkt, oft aber auch weitere Daten wie ein Datum oder den Kaufpreis. Abb. 2 zeigt exemplarisch Kundenbewertungen auf zwei Darknet Marktplätzen.

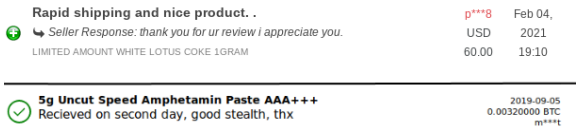


Abb. 2: Beispiele von positiven Bewertungen auf Darknet Marktplätzen.

Unter Berücksichtigung der oben genannten Informationen ist es möglich, die Transaktionsmuster, die das Zahlungssystem eines Marktplatzes verursacht, als einfachen gerichteten Graphen $\text{G} = (\text{V}, \text{E})$ zu modellieren. Dabei sind die Knoten des Graphen definiert als $\text{V} = \{a_C, a_{\text{dep}}, a_{\mathcal{V}}, a_{\mathcal{M}}, \vec{t}_{\text{dep}}, \vec{t}_{\text{pay}}\}$ und die Kanten als $\text{E} = \{(a_C, \vec{t}_{\text{dep}}), (\vec{t}_{\text{dep}}, a_{\text{dep}}), (a_{\text{dep}}, \vec{t}_{\text{pay}}), (\vec{t}_{\text{pay}}, a_{\mathcal{M}}), (\vec{t}_{\text{pay}}, a_{\mathcal{V}})\}$. Zusätzlich besitzen die Transaktionen $\vec{t}_{\text{dep}}$ und $\vec{t}_{\text{pay}}$ auch Zeitstempel τ_{dep} bzw. τ_{pay}. Die Kanten sind wiederum mit den Werten α_{in} und α_{out} verbunden, welche die übertragene Menge bitcoin angeben. Abb. 3 ist eine visuelle Darstellung dieses Graphen.

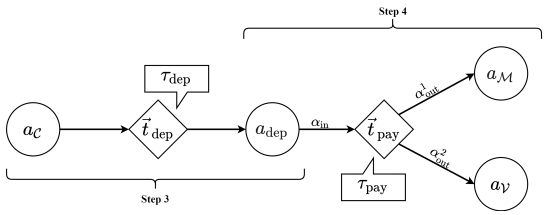


Abb. 3: Transaktionsgraph eines Zahlungssystems für den Fall $a_{\text{dep}} = a_{\text{esc}}$.

Der Graph lässt sich trivial auf Fälle erweitern, in denen eine dedizierte Treuhandadresse genutzt wird.

4 Angriffsbeschreibung

Frühere Forschung hat gezeigt, dass ein Angreifer eine Bitcoin-Transaktion und somit die sendenden und empfangenden Adressen identifizieren kann, wenn der genaue Zeitstempel τ und der transferierte Betrag α bekannt sind [Go17b].

Solche Informationen lassen sich beispielsweise aus einer Kundenbewertung $\vec{r} = (\tau_r, \alpha_r)$ ableiten, sofern diese einen (ungefähren) Kaufpreis α_r und Zeitstempel τ_r enthält. Mit Stand Juni 2021 enthielten 4 der 15 von uns untersuchten Darknet Marktplätze solche Bewertungen, wobei weitere zwei Marktplätze immerhin Intervalle der relevanten Werte zeigten. Es wird ferner angenommen, dass der Angreifer eine Schätzung des Parameters $\delta = |\tau_r - \tau_{pay}|$ erhalten kann, der die Zeitdifferenz zwischen der durch Abschluss einer Bestellung ausgelösten Auszahlungstransaktion und der Veröffentlichung einer Bewertung durch den Kunden darstellt. Im Kontext dieser Arbeit gehen wir davon aus, dass Kunden ihre Bewertungen zeitnah nach dem Abschluss einer Bestellung hinterlassen. Die genaue Begründung dieser Annahme kann in der Ursprungspublikation nachgelesen werden. Das Intervall $[\tau_r - \delta, \tau_r + \delta]$ dient dann als Schätzung für τ_{pay}.

Um den Angriff durchzuführen, sammelt ein Angreifer auf dem gewählten Marktplatz zunächst so viele Kundenbewertungen wie möglich. Anschließend definiert der Angreifer einen Transaktionsgraphen analog zu Abb. 3, der die Struktur des Zahlungssystems des Marktes repräsentiert und leitet Schätzungen für die Zeitpunkte und Volumina der Transaktionen aus den Bewertungen ab. Daraufhin beginnt der Angreifer damit, die gesamte Bitcoin-Blockchain nach Subgraphen zu durchsuchen, die zum Zahlungssystem und den Bewertungen passen: Zu diesem Zweck durchläuft der Angreifer die gesammelten Kundenbewertungen eines Händlers und identifiziert diejenigen Subgraphen in der Blockchain, welche strukturell dem Transaktionsgraph des Zahlungssystems enstprechen und zudem die korrekten Schätzwerte für α und τ aufweisen. Der Angreifer speichert im nächsten Schritt alle Adressen, die in den gefundenen Subgraphen an der Position von a_V vorkommen. Dies entspricht der Menge der potenziellen Auszahlungsadressen (sog. Kandidatenadressen) für eine gegebene Bewertung $\vec{r}$. Ab der zweiten betrachteten Bewertung wird die Menge der Kandidatenadressen des aktuellen Durchlaufs mit denen der vorherigen Durchläufe geschnitten und so die Menge der potenziellen Auszahlungsadressen schrittweise reduziert. Wenn der Schnitt mit der aktuellen Kandidatenmenge zu einer leeren Menge führen würde, wird der aktuelle Durchlauf übersprungen. Der Prozess endet, sobald die Schnittmenge nur noch eine einzige potenzielle Auszahlungsadresse enthält oder wenn keine Bewertungen mehr zu verarbeiten sind.

Eine Variation des oben beschriebenen Angriffs lässt sich auch in Fällen durchführen, in denen Händler ihre Auszahlungsadresse nach jeder erhaltenen Zahlung tauschen. Details zu dieser Variation sind der Ursprungspublikation zu entnehmen.

Bei der Interpretation der Resultate des Angriffs muss beachtet werden, dass die so gefundenen Adressen auch falsch positive Ergebnisse enthalten können, d.h. Adressen, die

nicht zu Händlern auf dem Marktplatz gehören, sondern deren Transaktionsverhalten nur zufällig mit den Erwartungen des Angreifers übereinstimmt. Daher werden die gefundenen Adressen einer weiteren Validierung unterzogen:

Für jede potenzielle Auszahlungsadresse eines Verkäufers durchsucht der Angreifer die Blockchain nach Subgraphen, die strukturell den erwarteten Transaktionsgraphen entsprechen und bei denen die Kandidatenadresse an der Position von $a_{\mathcal{V}}$ vorkommt. Der Angreifer erstellt dann die Menge W, indem er das Tupel $w = (\alpha_{\text{pay}}, \tau_{\text{pay}})$ für jeden dieser Graphen extrahiert. Hierbei bezeichnet α_{pay} den Betrag, der von $\vec{t}_{\text{pay}}$ an die Kandidatenadresse gezahlt wird und τ_{pay} den Zeitstempel von $\vec{t}_{\text{pay}}$. Sollte ein Transaktionsgraph existieren, der mit einer Bewertung $\vec{r}$ übereinstimmt, so existiert auch ein $w \in W$, so dass $w = \vec{r}$. Die Menge der Transaktionsgraphen, für die eine übereinstimmende Bewertung existiert, wird somit als $M = W \cap R$ definiert.

Um zu bewerten, wie gut eine Kandidatenadresse zu einem Verkäufer passt, kann die Übereinstimmung zwischen den beobachteten Bitcoin-Transaktionen und den Bewertungen eines Verkäufers berechnet werden. Ein einfaches Maß wäre $J(W, R)$, der Jaccard-Index zwischen den beobachteten und erwarteten Transaktionsgraphen für ein gegebenes Verkäufer-Adress-Paar. Das Ergebnis kann intuitiv als die Wahrscheinlichkeit interpretiert werden, dass ein Element mindestens einer der Mengen ein Element beider ist [Le71]. Um genauere Aussagen hinsichtlich der Übereinstimmung treffen zu können, berechnen wir zwei separate Jaccard-Werte: $J(M, R)$ und $J(M, W)$, wobei $M \subseteq R$ und $M \subseteq W$. Somit ist $J(M, R)$ die Wahrscheinlichkeit, dass, gegeben eine Bewertung, ein passender Transaktionsgraph für die untersuchte Adresse existiert. Wir bezeichnen diese Maßzahl als Bewertungsabdeckung (engl. review coverage) RC:

$$\text{RC} = J(M, R) = \frac{|M \cap R|}{|M \cup R|} = \frac{|M|}{|R|} \tag{1}$$

Analog ist die Adressabdeckung (engl. address coverage)(AC) die Wahrscheinlichkeit, dass eine übereinstimmende Bewertung für eine auf der untersuchten Adresse eingehende, potenzielle Auszahlungstransaktion existiert.

$$\text{AC} = J(M, W) = \frac{|M \cap W|}{|M \cup W|} = \frac{|M|}{|W|} \tag{2}$$

Allein die Bewertungs- und Adressabdeckung verhindern keine falsch positiven Ergebnisse, da Verkäufer mit sehr wenigen Bewertungen oder Kandidatenadressen, die in sehr wenigen Zahlungssystem-Teilgraphen enthalten sind, trivialerweise hohe Abdeckungen in einem der beiden Maße erreichen könnten. Unter Bezugnahme auf das Konzept des *F-Score* kombinieren wir daher die beiden Abdeckungen zu einem kombinierten Abdeckungsmaß

(engl. combined coverage score) (CCS), das als harmonisches Mittel aus Bewertungs- und Adressabdeckung definiert ist:

$$\mathrm{CCS} = \frac{2 \cdot \mathrm{RC} \cdot \mathrm{AC}}{\mathrm{RC} + \mathrm{AC}} \tag{3}$$

Ein Angreifer kann nun auf der Grundlage der eigenen Unsicherheitstoleranz eine CCS-Schwelle wählen. Nur Adressen, die einen CCS-Wert größer oder gleich der gewählten Schwelle aufweisen, werden als wahrscheinliche Auszahlungsadressen des Verkäufers akzeptiert. Sollte eine Adresse zu zwei verschiedenen Verkäufern passen, so ermöglicht der CCS-Wert zudem eine eindeutige Zuordnung.

5 Experiment

Nicht alle Marktplätze sind gleichermaßen anfällig für unseren Angriff. Beispielsweise sind Marktplätze, auf denen Nutzer ihre Guthaben beliebig ein- und auszahlen können, schwierig anzugreifen, da sich das Auftreten der Auszahlungstransaktionen nicht eindeutig vorhersagen lässt. Besonders geeignet erscheinen daher sog. *walletlose* Marktplätze: Hier verfügen die Nutzer über kein Guthaben, sondern müssen den Kaufpreis für jede einzelne Bestellung gesondert an den Marktplatz transferieren. Ebenso erhalten Verkäufer ihre Erlöse für jeden Verkauf einzeln ausgezahlt.

Wir demonstrieren die Anwendbarkeit unseres Angriffs daher anhand von zwei real existierenden, walletlosen Darknet Marktplätzen: Cryptonia Market und Cannazon.

5.1 Transaktionsgraphen

Die Hilfe- und FAQ-Seiten von Cryptonia Market bieten eine recht detaillierte Beschreibung des zu Grunde liegenden Zahlungssystems. Screenshots der entsprechenden Seiten finden sich im Appendix. Daraus ergibt sich der in Abb. 4 gezeigte Subgraph als typisches Muster einer Cryptonia Market-Auszahlungstransaktion. Während des Angriffs können die in Orange markierten Werte mittels der Bewertungen geschätzt werden, während das Intervall der möglichen Marktplatzprovision (in Blau markiert) aus der Bewertung und den auf der FAQ-Seite bereitgestellten Informationen berechnet werden kann.

Ähnlich zu Cryptonia Market bietet auch Cannazon eine recht detaillierte Beschreibung des Bestell- und Zahlungsvorgangs. Auch hier sind die relevanten Screenshots im Anhang aufgeführt. Im Wesentlichen gleichen sich die Zahlungssysteme beider Marktplätze, allerdings verwendet Cannazon eine dedizierte Treuhandadresse. Zudem berechnet Cannazon die Verkaufsprovision basierend auf der Aktivität und dem Ruf des Verkäufers, während die Provision bei Cryptonia Market zufällig festgelegt wird. Eine Schätzung der Verkaufsprovision ist jedoch auch bei Cannazon möglich. Das Verfahren wird in der Ursprungspublikation ausführlich beschrieben.

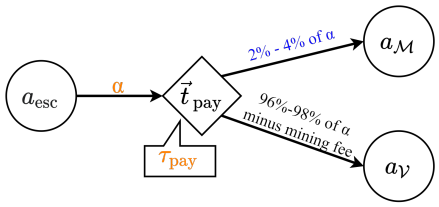


Abb. 4: Erwarteter Währungsfluss auf Cryptonia Market. Orangefarbe Werte können aus Bewertungen geschätzt und die blauen Werte durch zusätzliche Informationen berechnet werden. Die schwarzen Werte sind unbekannt.

Abb. 5 visualisiert den Währungsfluss, der mit einer Cannazon-Transaktion verbunden ist, sofern das Treuhandsystem genutzt wird.

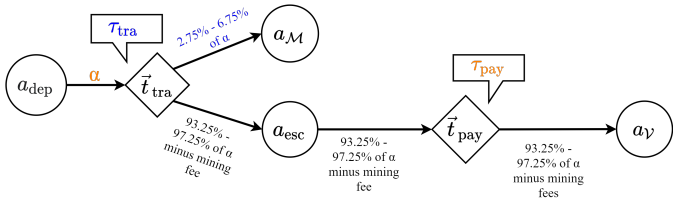


Abb. 5: Erwarteter Währungsfluss auf Cannazon. Orangefarbene Werte können aus Bewertungen geschätzt und die blauen Werte durch zusätzliche Informationen berechnet werden. Die schwarzen Werte sind unbekannt.

5.2 Ergebnisse

Im Zuge der Untersuchung konnten insgesamt 28.966 Bewertungen auf Cryptonia Market und 351.769 Bewertungen auf Cannazon gesammelt werden. Dabei wurden Bewertungen, die sich auf andere Währungen als Bitcoin beziehen ausgeschlossen, ebenso wie Bewertungen für Käufe ohne Treuhandservice, da hier der zeitliche Abstand zwischen Zahlung und Abgabe der Bewertung unklar ist. Ebenso ausgeschlossen wurden negative Kundenbewertungen, da auch in diesen Fällen Schlichtungsverfahren o.Ä. zu unbekannten Verzögerungen führen können. Abschließend wurden auch Verkäufer mit weniger als vier abgeschlossenen Käufen oder weniger als zwei positiven Kundenbewertungen ignoriert. Die CCS-Schwelle wird auf $0,4$ festgelegt.

Mit unseren Verknüpfungsangriffen finden wir potenzielle Auszahlungsadressen für 308 Cryptonia Market- und 45 Cannazon-Verkäufer. Angesichts der 559 Anbieter, die auf Cryptonia Market mindestens zwei positive Bewertungen hatten, entspricht dies einer Erfolgsrate von etwa 55.1%. Der Erfolg unseres Angriffs auf Cannazon ist deutlich geringer: Von den 236 Anbietern, die mindestens zwei positive Bewertungen haben, konnte nur

19.1% mindestens eine Bitcoin-Adresse zugeordnet werden. Interessanterweise scheint es dabei keine klare Beziehung zwischen der Anzahl der verfügbaren Bewertungen für einen Anbieter und der Erfolgschance zu geben. Abb. 9 und Abb. 15 im Anhang bieten einen kurzen Überblick über die Erfolgsraten für verschiedene Zahlen verfügbarer Bewertungen pro Händler. Grundsätzlich lässt sich die niedrigere Erfolgsrate auf Cannazon aber durch die höhere Unsicherheit erklären, da die Kaufbeträge in den Bewertungen dort erst von Euro in bitcoin (BTC) konvertiert werden mussten, während bei Cryptonia Market direkt BTC-Beträge vorlagen.

5.3 Diskussion

Größte Schwachstelle unserer Arbeit ist die fehlende externe Validierung unserer Ergebnisse. Obwohl die Resultate plausibel erscheinen, ist ein Beweis, dass die von unserem Angriff gefundenen Adressen tatsächlich zu Händlern auf Cryptonia Market oder Cannazon gehören, nicht mit absoluter Sicherheit möglich. Ein einfacher Weg zur teilweisen Validierung wäre es, Testkäufe bei einem Händler zu tätigen und zu überprüfen, ob die Zahlung tatsächlich auf der erwarteten Adresse eingeht — Dieses Vorgehen wurde jedoch durch die Rechtsabteilung unserer Einrichtung untersagt. Aus diesem Grund beschränkt sich die Validierung der Resultate darauf, ein zufälliges Zustandekommen der Ergebnisse weitestgehend auszuschließen. Wie in Abb. 10 und 11 im Anhang zu sehen, gibt es eine sehr große Korrelation zwischen den Bewertungen eines Anbieters und den eingehenden Transaktionen der identifizierten Händleradresse. Dies betrifft nicht nur die transferierten Beträge und die Zeitpunkte der Transaktionen, sondern sogar die Reihenfolge der Transaktionen innerhalb des gleichen Tages.

Zum Zeitpunkt unseres Experiments gab es insgesamt 33 Cannazon-Händler, deren öffentliche Pretty Good Privacy (PGP) Schlüssel auch in Händlerprofilen auf Cryptonia Market hinterlegt waren. Vermutlich handelt es sich hierbei also um die gleichen Personen. 16 dieser Anbieter wurden erfolgreich mit Bitcoin-Adressen verknüpft. Nach dem Clustern der gefundenen Adressen zu Wallets mithilfe der Multi-Input-Heuristik fanden sich auf sechs dieser Wallets tatsächlich eingehende Transaktionen von beiden Marktplätzen.

Schließlich war auch zu beobachten, dass die Locking-Skripte der von Cannazon verwendeten Multisig-Treuhand-Adressen regelmäßig denselben öffentlichen Schlüssel enthielten, welcher vermutlich dem Marktplatz zuzuordnen ist.

In der Gesamtschau halten wir es daher für äußerst unwahrscheinlich, dass all diese Beobachtungen zufällig aufgetreten sind.

Davon abgesehen bedeuten die Erfolgsraten von 55.1% und 19.1% allerdings auch, dass unser Verfahren nicht unbedingt für gezielte Angriffe auf einzelne Anbieter geeignet ist. Dennoch stellt der Angriff einen erheblichen Eingriff in die Privatsphäre derjenigen dar, die von ihm betroffen sind. Darüber hinaus können die erfolgreich zugeordneten Adressen

als Ausgangspunkt dienen, um zusätzliche Händleradressen zu identifizieren: Durch eine Analyse von Querverbindungen innerhalb des Zahlungssystems lassen sich beispielsweise unbekannte Händleradressen finden, deren Zuordnung zu Händlern durch eine umgekehrte Anwendung unseres Verfahrens möglich ist. Darüber hinaus wird selbst in den Fällen, in denen unser Angriff nicht erfolgreich ist, die Anonymität der Nutzer verringert: Selbst fehlgeschlagene Versuche grenzten die Zahl der Kandidatenadressen im Durchschnitt auf etwa 15 ein. In 48 Fällen lag die Größe des Kandidatensets sogar bei fünf oder weniger.

Die niedrige Erfolgsrate auf Cannazon war zu erwarten, da die Unsicherheit hinsichtlich des tatsächlichen Werts der Bestellungen erheblich höher war als auf Cryptonia Market. Es ist auch sehr wahrscheinlich, dass zumindest einige der Cannazon Bewertungen, die wir zuordnen wollten, auf Bestellungen verweisen, die in Monero bezahlt wurden.

6 Fazit

In dieser Arbeit wurde ein neuer Angriff vorgestellt, mit dessen Hilfe Bitcoin-Adressen von Darknet Verkäufern anhand öffentlich zugänglicher Informationen, insbesondere positiver Kundenbewertungen, identifiziert werden können. Experimente haben die Anwendbarkeit der Angriffe auf echte Darknet Marktplätze bestätigt.

Als Konsequenz davon sind Händler auf Darknet Marktplätzen mit zwei widersprüchlichen Zielen konfrontiert. Einerseits sind sie daran interessiert, so viele positive Bewertungen wie möglich anzusammeln. Andererseits erlauben es aber gerade diese Bewertungen, Informationen über getätigte Käufe abzuleiten und schließlich auch die Verkäuferadressen zu identifizieren.

Unabhängig von den in dieser Arbeit vorgestellten Angriffen betrachten wir dies als einen interessanten Konflikt, der eine Reihe wichtiger Fragen für zukünftige Forschung aufwirft. Vor allem die Frage, ob es möglich ist, diesen Konflikt ohne die Verwendung von Drittanbietern wie beispielsweise Bitcoin-Mixern zu lösen. Darüber hinaus können die in den Angriffen verwendeten Techniken auch dazu verwendet werden, Benutzer- und Markplatzadressen zu identifizieren, was weiter untersucht werden sollte. Das Gleiche gilt für die Frage, ob ein Angriff immer noch möglich ist, wenn Zeitstempel, Auftragsvolumen oder Beides in den Bewertungen fehlen.

Zusammenfassend hoffen wir, dass diese Arbeit eine Grundlage für weitere Forschungen über die Datenschutzimplikationen von Kryptowährungen sein kann, besonders mit Blick auf deren stark gestiegene Beliebtheit.

Literatur

[Ch19] Chen, X.; Hasan, M. A.; Wu, X.; Skums, P.; Feizollahi, M. J.; Ouellet, M.; Sevigny, E. L.; Maimon, D.; Wu, Y.: Characteristics of Bitcoin Transactions on Cryptomarkets. In (Wang, G.; Feng, J.; Bhuiyan, M. Z. A.; Lu, R., Hrsg.): Security, Privacy, and Anonymity in Computation, Communication, and Storage. Springer International Publishing, Cham, S. 261–276, 2019, ISBN: 978-3-030-24907-6.

[Go17a] Goldfeder, S.; Bonneau, J.; Gennaro, R.; Narayanan, A.: Escrow Protocols for Cryptocurrencies: How to Buy Physical Goods Using Bitcoin. In (Kiayias, A., Hrsg.): Financial Cryptography and Data Security. Springer International Publishing, Cham, S. 321–339, 2017, ISBN: 978-3-319-70972-7.

[Go17b] Goldfeder, S.; Kalodner, H. A.; Reisman, D.; Narayanan, A.: When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. Proceedings on Privacy Enhancing Technologies 2018/, S. 179–199, 2017.

[Ja19] Jawaheri, H.; Sabah, M.; Boshmaf, Y.; Erbad, A.: Deanonymizing Tor Hidden Service Users Through Bitcoin Transactions Analysis. Computers & Security 89/, S. 101684, Dez. 2019.

[Jo18] Jourdan, M.; Blandin, S.; Wynter, L.; Deshpande, P.: Characterizing entities in the Bitcoin Blockchain. In: Data Mining Workshop (ICDMW), 2018 IEEE International Conference on. IEEE, 2018.

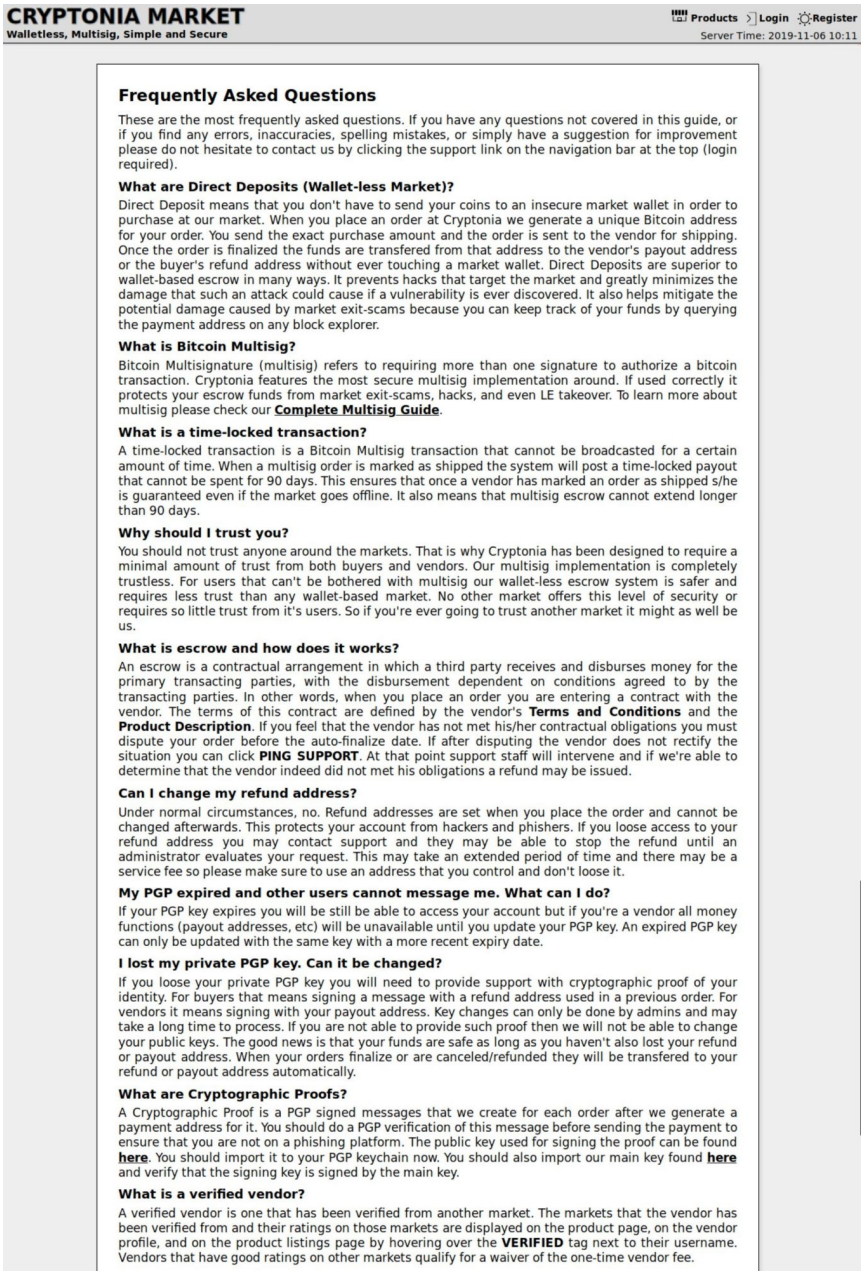
[Le71] Levandowsky, M.: Distance between Sets. Nature 234/5323, S. 34–35, Nov. 1971.

[MMG18] McGinn, D.; McIlwraith, D.; Guo, Y.: Toward Open Data Blockchain Analytics: A Bitcoin Perspective. Royal Society Open Science 5/, Feb. 2018.

[Sa19] Sabry, F.; Labda, W.; Erbad, A.; Al Jawaheri, H.; Malluhi, Q.: Anonymity and privacy in bitcoin escrow trades. In: Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society. S. 211–220, 2019.

[So19] Sommer, D.: Processing Bitcoin Blockchain Data using a Big Data-specific Framework, Bachelor's Thesis, University of Zurich. https://www.merlin.uzh.ch/contributionDocument/download/11801, Mai 2019.

A Appendix



CRYPTONIA MARKET
Walletless, Multisig, Simple and Secure

Products Login Register
Server Time: 2019-11-06 10:11

Frequently Asked Questions

These are the most frequently asked questions. If you have any questions not covered in this guide, or if you find any errors, inaccuracies, spelling mistakes, or simply have a suggestion for improvement please do not hesitate to contact us by clicking the support link on the navigation bar at the top (login required).

What are Direct Deposits (Wallet-less Market)?

Direct Deposit means that you don't have to send your coins to an insecure market wallet in order to purchase at our market. When you place an order at Cryptonia we generate a unique Bitcoin address for your order. You send the exact purchase amount and the order is sent to the vendor for shipping. Once the order is finalized the funds are transfered from that address to the vendor's payout address or the buyer's refund address without ever touching a market wallet. Direct Deposits are superior to wallet-based escrow in many ways. It prevents hacks that target the market and greatly minimizes the damage that such an attack could cause if a vulnerability is ever discovered. It also helps mitigate the potential damage caused by market exit-scams because you can keep track of your funds by querying the payment address on any block explorer.

What is Bitcoin Multisig?

Bitcoin Multisignature (multisig) refers to requiring more than one signature to authorize a bitcoin transaction. Cryptonia features the most secure multisig implementation around. If used correctly it protects your escrow funds from market exit-scams, hacks, and even LE takeover. To learn more about multisig please check our **Complete Multisig Guide**.

What is a time-locked transaction?

A time-locked transaction is a Bitcoin Multisig transaction that cannot be broadcasted for a certain amount of time. When a multisig order is marked as shipped the system will post a time-locked payout that cannot be spent for 90 days. This ensures that once a vendor has marked an order as shipped s/he is guaranteed even if the market goes offline. It also means that multisig escrow cannot extend longer than 90 days.

Why should I trust you?

You should not trust anyone around the markets. That is why Cryptonia has been designed to require a minimal amount of trust from both buyers and vendors. Our multisig implementation is completely trustless. For users that can't be bothered with multisig our wallet-less escrow system is safer and requires less trust than any wallet-based market. No other market offers this level of security or requires so little trust from it's users. So if you're ever going to trust another market it might as well be us.

What is escrow and how does it works?

An escrow is a contractual arrangement in which a third party receives and disburses money for the primary transacting parties, with the disbursement dependent on conditions agreed to by the transacting parties. In other words, when you place an order you are entering a contract with the vendor. The terms of this contract are defined by the vendor's **Terms and Conditions** and the **Product Description**. If you feel that the vendor has not met his/her contractual obligations you must dispute your order before the auto-finalize date. If after disputing the vendor does not rectify the situation you can click **PING SUPPORT**. At that point support staff will intervene and if we're able to determine that the vendor indeed did not met his obligations a refund may be issued.

Can I change my refund address?

Under normal circumstances, no. Refund addresses are set when you place the order and cannot be changed afterwards. This protects your account from hackers and phishers. If you loose access to your refund address you may contact support and they may be able to stop the refund until an administrator evaluates your request. This may take an extended period of time and there may be a service fee so please make sure to use an address that you control and don't loose it.

My PGP expired and other users cannot message me. What can I do?

If your PGP key expires you will be still be able to access your account but if you're a vendor all money functions (payout addresses, etc) will be unavailable until you update your PGP key. An expired PGP key can only be updated with the same key with a more recent expiry date.

I lost my private PGP key. Can it be changed?

If you loose your private PGP key you will need to provide support with cryptographic proof of your identity. For buyers that means signing a message with a refund address used in a previous order. For vendors it means signing with your payout address. Key changes can only be done by admins and may take a long time to process. If you are not able to provide such proof then we will not be able to change your public keys. The good news is that your funds are safe as long as you haven't also lost your refund or payout address. When your orders finalize or are canceled/refunded they will be transfered to your refund or payout address automatically.

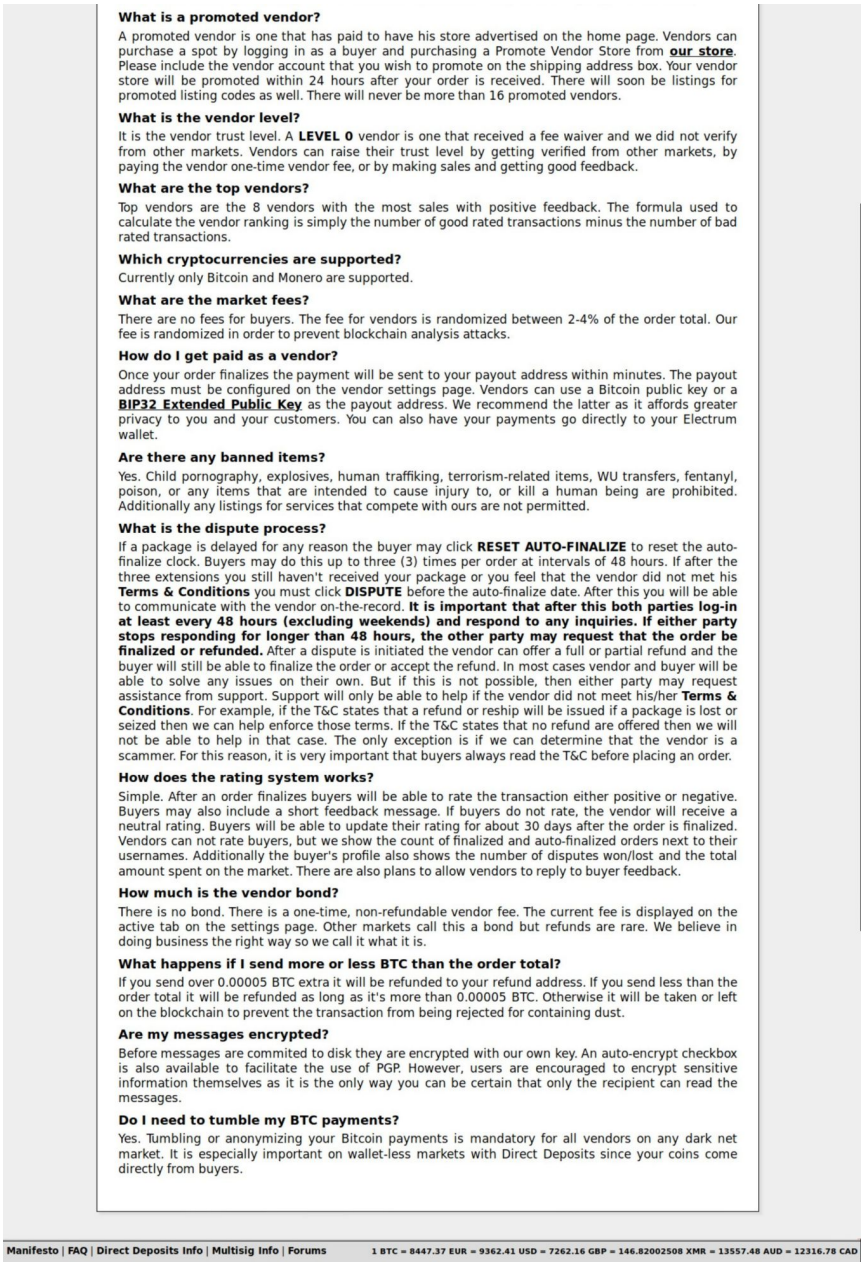
What are Cryptographic Proofs?

A Cryptographic Proof is a PGP signed messages that we create for each order after we generate a payment address for it. You should do a PGP verification of this message before sending the payment to ensure that you are not on a phishing platform. The public key used for signing the proof can be found **here**. You should import it to your PGP keychain now. You should also import our main key found **here** and verify that the signing key is signed by the main key.

What is a verified vendor?

A verified vendor is one that has been verified from another market. The markets that the vendor has been verified from and their ratings on those markets are displayed on the product page, on the vendor profile, and on the product listings page by hovering over the **VERIFIED** tag next to their username. Vendors that have good ratings on other markets qualify for a waiver of the one-time vendor fee.

Abb. 6: Seite „Payment Info“ auf Cryptonia Market 1/2.



What is a promoted vendor?

A promoted vendor is one that has paid to have his store advertised on the home page. Vendors can purchase a spot by logging in as a buyer and purchasing a Promote Vendor Store from **our store**. Please include the vendor account that you wish to promote on the shipping address box. Your vendor store will be promoted within 24 hours after your order is received. There will soon be listings for promoted listing codes as well. There will never be more than 16 promoted vendors.

What is the vendor level?

It is the vendor trust level. A **LEVEL 0** vendor is one that received a fee waiver and we did not verify from other markets. Vendors can raise their trust level by getting verified from other markets, by paying the vendor one-time vendor fee, or by making sales and getting good feedback.

What are the top vendors?

Top vendors are the 8 vendors with the most sales with positive feedback. The formula used to calculate the vendor ranking is simply the number of good rated transactions minus the number of bad rated transactions.

Which cryptocurrencies are supported?

Currently only Bitcoin and Monero are supported.

What are the market fees?

There are no fees for buyers. The fee for vendors is randomized between 2-4% of the order total. Our fee is randomized in order to prevent blockchain analysis attacks.

How do I get paid as a vendor?

Once your order finalizes the payment will be sent to your payout address within minutes. The payout address must be configured on the vendor settings page. Vendors can use a Bitcoin public key or a **BIP32 Extended Public Key** as the payout address. We recommend the latter as it affords greater privacy to you and your customers. You can also have your payments go directly to your Electrum wallet.

Are there any banned items?

Yes. Child pornography, explosives, human traffiking, terrorism-related items, WU transfers, fentanyl, poison, or any items that are intended to cause injury to, or kill a human being are prohibited. Additionally any listings for services that compete with ours are not permitted.

What is the dispute process?

If a package is delayed for any reason the buyer may click **RESET AUTO-FINALIZE** to reset the auto-finalize clock. Buyers may do this up to three (3) times per order at intervals of 48 hours. If after the three extensions you still haven't received your package or you feel that the vendor did not met his **Terms & Conditions** you must click **DISPUTE** before the auto-finalize date. After this you will be able to communicate with the vendor on-the-record. **It is important that after this both parties log-in at least every 48 hours (excluding weekends) and respond to any inquiries. If either party stops responding for longer than 48 hours, the other party may request that the order be finalized or refunded.** After a dispute is initiated the vendor can offer a full or partial refund and the buyer will still be able to finalize the order or accept the refund. In most cases vendor and buyer will be able to solve any issues on their own. But if this is not possible, then either party may request assistance from support. Support will only be able to help if the vendor did not meet his/her **Terms & Conditions**. For example, if the T&C states that a refund or reship will be issued if a package is lost or seized then we can help enforce those terms. If the T&C states that no refund are offered then we will not be able to help in that case. The only exception is if we can determine that the vendor is a scammer. For this reason, it is very important that buyers always read the T&C before placing an order.

How does the rating system works?

Simple. After an order finalizes buyers will be able to rate the transaction either positive or negative. Buyers may also include a short feedback message. If buyers do not rate, the vendor will receive a neutral rating. Buyers will be able to update their rating for about 30 days after the order is finalized. Vendors can not rate buyers, but we show the count of finalized and auto-finalized orders next to their usernames. Additionally the buyer's profile also shows the number of disputes won/lost and the total amount spent on the market. There are also plans to allow vendors to reply to buyer feedback.

How much is the vendor bond?

There is no bond. There is a one-time, non-refundable vendor fee. The current fee is displayed on the active tab on the settings page. Other markets call this a bond but refunds are rare. We believe in doing business the right way so we call it what it is.

What happens if I send more or less BTC than the order total?

If you send over 0.00005 BTC extra it will be refunded to your refund address. If you send less than the order total it will be refunded as long as it's more than 0.00005 BTC. Otherwise it will be taken or left on the blockchain to prevent the transaction from being rejected for containing dust.

Are my messages encrypted?

Before messages are commited to disk they are encrypted with our own key. An auto-encrypt checkbox is also available to facilitate the use of PGP. However, users are encouraged to encrypt sensitive information themselves as it is the only way you can be certain that only the recipient can read the messages.

Do I need to tumble my BTC payments?

Yes. Tumbling or anonymizing your Bitcoin payments is mandatory for all vendors on any dark net market. It is especially important on wallet-less markets with Direct Deposits since your coins come directly from buyers.

Abb. 7: Seite „Payment Info“ auf Cryptonia Market 2/2.

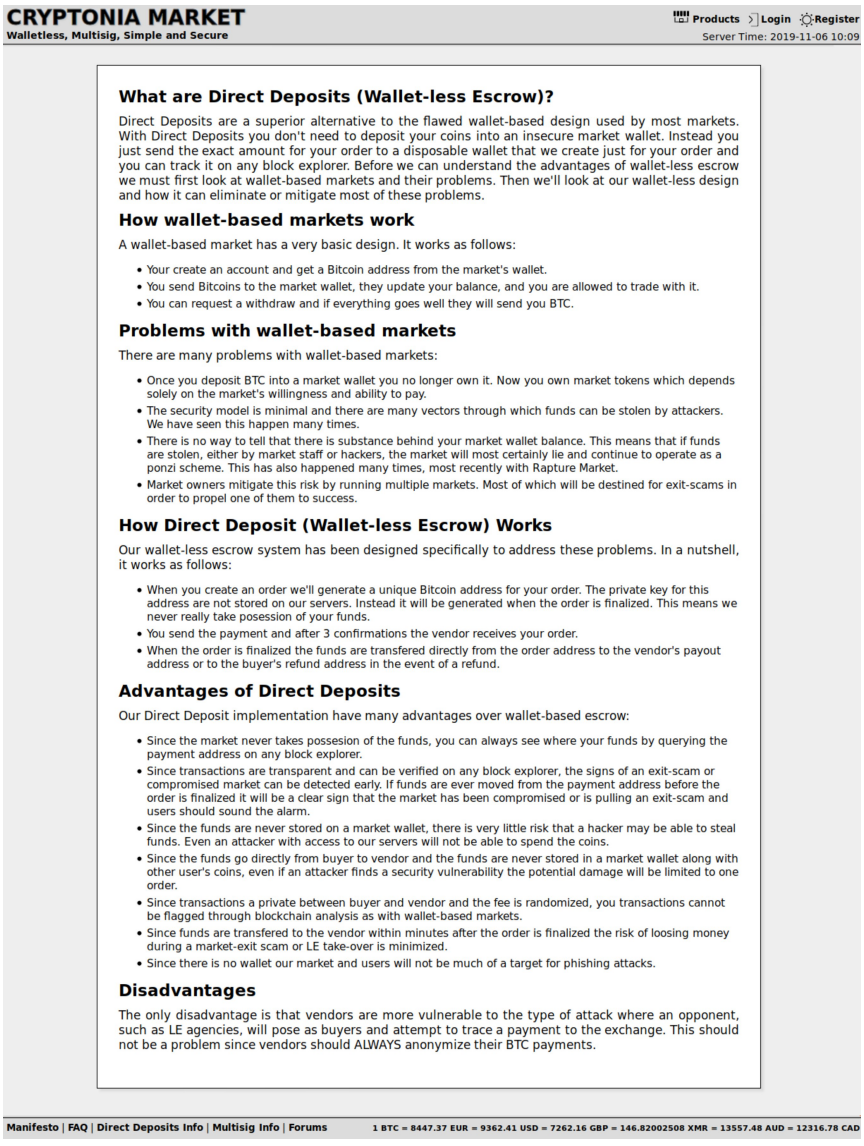


Abb. 8: Seite „FAQ“ auf Cryptonia Market.

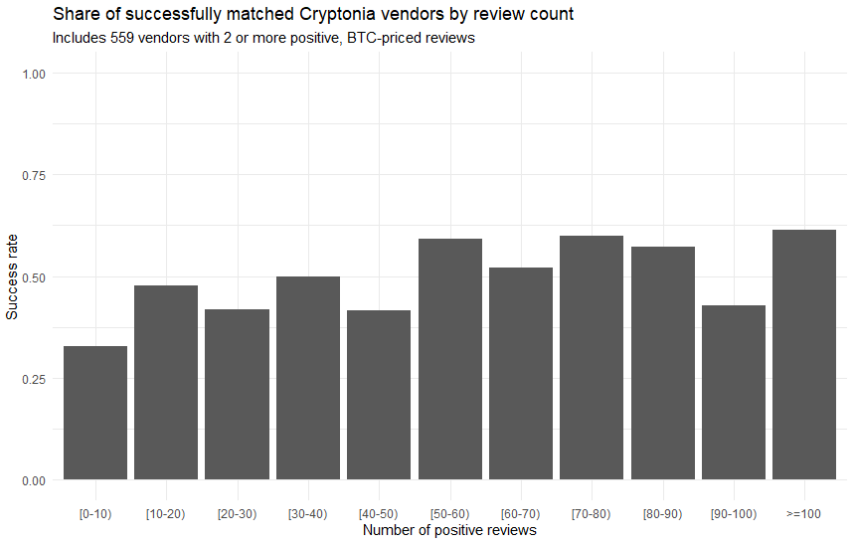


Abb. 9: Erfolgsrate nach Anzahl der Bewertungen auf Cryptonia Market.

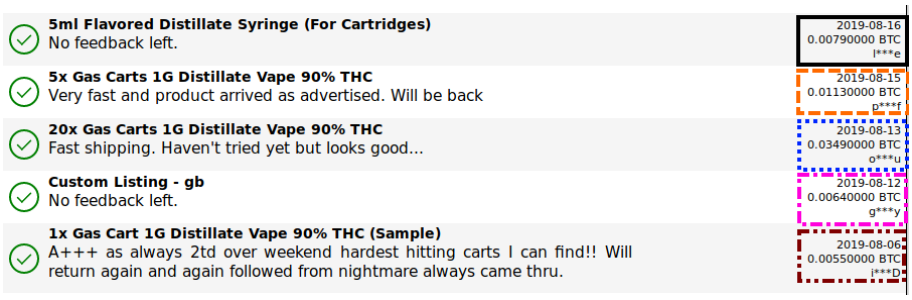


Abb. 10: Bewertungsseite eines Cryptonia Market-Händlers.

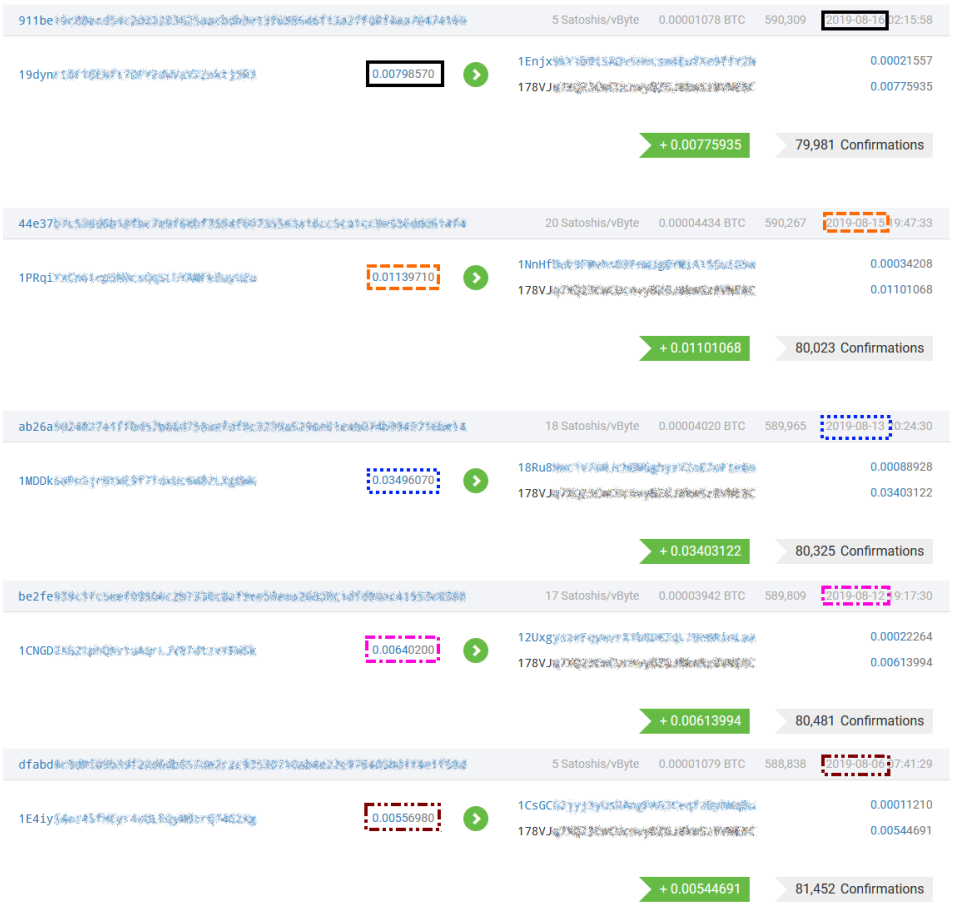
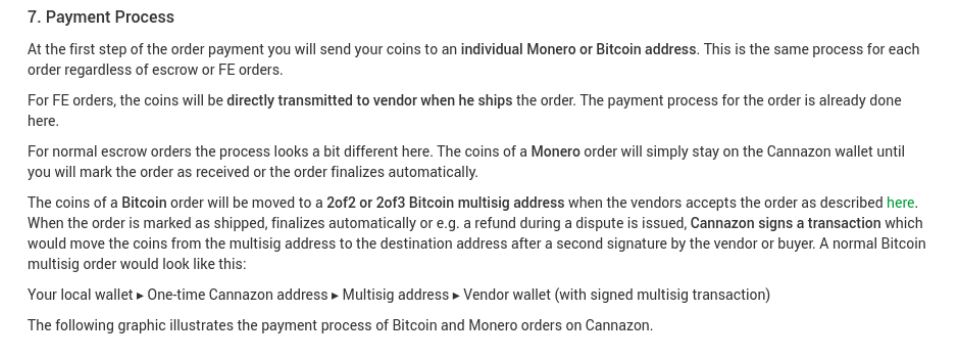


Abb. 11: Identifizierte Auszahlungsadresse des gleichen Händlers auf btc.com (Bearbeitet).



7. Payment Process

At the first step of the order payment you will send your coins to an **individual Monero or Bitcoin address**. This is the same process for each order regardless of escrow or FE orders.

For FE orders, the coins will be **directly transmitted to vendor when he ships** the order. The payment process for the order is already done here.

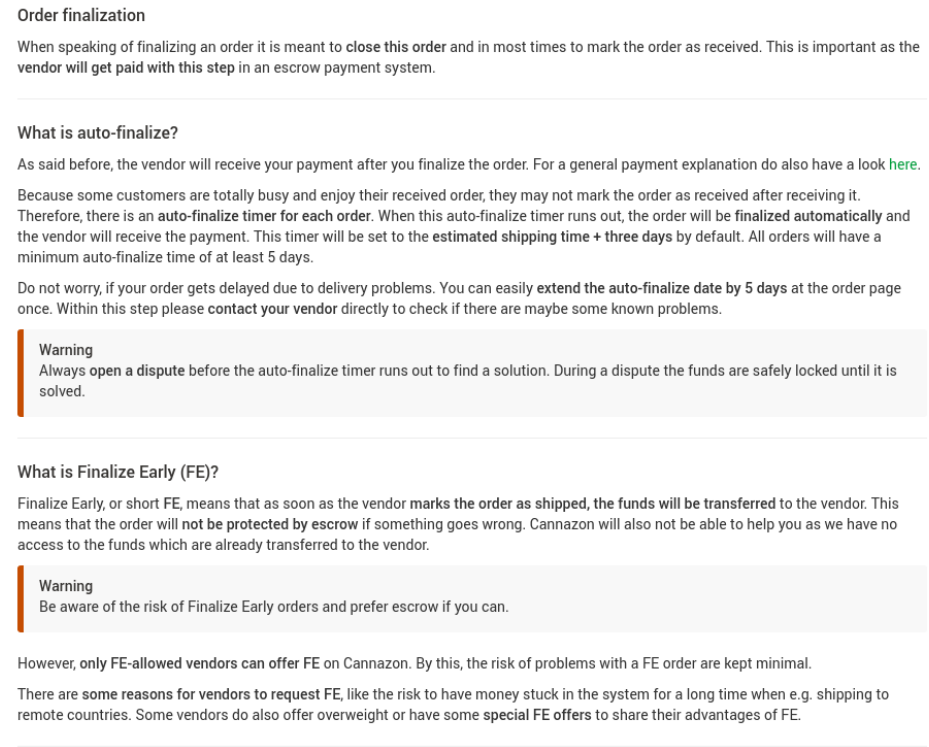
For normal escrow orders the process looks a bit different here. The coins of a **Monero** order will simply stay on the Cannazon wallet until you will mark the order as received or the order finalizes automatically.

The coins of a **Bitcoin** order will be moved to a **2of2 or 2of3 Bitcoin multisig address** when the vendors accepts the order as described here. When the order is marked as shipped, finalizes automatically or e.g. a refund during a dispute is issued, **Cannazon signs a transaction** which would move the coins from the multisig address to the destination address after a second signature by the vendor or buyer. A normal Bitcoin multisig order would look like this:

Your local wallet ▸ One-time Cannazon address ▸ Multisig address ▸ Vendor wallet (with signed multisig transaction)

The following graphic illustrates the payment process of Bitcoin and Monero orders on Cannazon.

Abb. 12: Beschreibung der Zahlungsabwicklung auf Cannazon.



Order finalization

When speaking of finalizing an order it is meant to **close this order** and in most times to mark the order as received. This is important as the **vendor will get paid with this step** in an escrow payment system.

What is auto-finalize?

As said before, the vendor will receive your payment after you finalize the order. For a general payment explanation do also have a look here.

Because some customers are totally busy and enjoy their received order, they may not mark the order as received after receiving it. Therefore, there is an **auto-finalize timer for each order**. When this auto-finalize timer runs out, the order will be **finalized automatically** and the vendor will receive the payment. This timer will be set to the **estimated shipping time + three days** by default. All orders will have a minimum auto-finalize time of at least 5 days.

Do not worry, if your order gets delayed due to delivery problems. You can easily **extend the auto-finalize date by 5 days** at the order page once. Within this step please **contact your vendor** directly to check if there are maybe some known problems.

> **Warning**
> Always **open a dispute** before the auto-finalize timer runs out to find a solution. During a dispute the funds are safely locked until it is solved.

What is Finalize Early (FE)?

Finalize Early, or short **FE**, means that as soon as the vendor **marks the order as shipped, the funds will be transferred** to the vendor. This means that the order will **not be protected by escrow** if something goes wrong. Cannazon will also not be able to help you as we have no access to the funds which are already transferred to the vendor.

> **Warning**
> Be aware of the risk of Finalize Early orders and prefer escrow if you can.

However, **only FE-allowed vendors can offer FE** on Cannazon. By this, the risk of problems with a FE order are kept minimal.

There are **some reasons for vendors to request FE**, like the risk to have money stuck in the system for a long time when e.g. shipping to remote countries. Some vendors do also offer overweight or have some **special FE offers** to share their advantages of FE.

Abb. 13: Beschreibung des Treuhandsystems auf Cannazon.

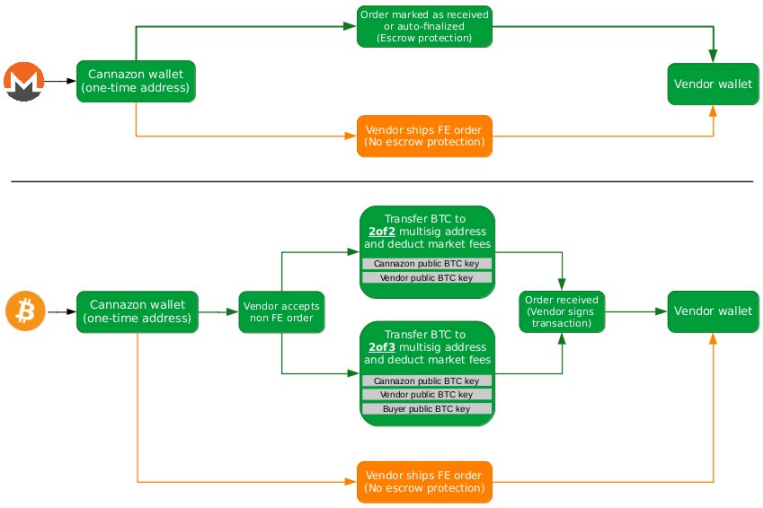


Abb. 14: Visualisierung der Zahlungsabwicklung auf Cannazon (Screenshot der Hilfe-Seite).

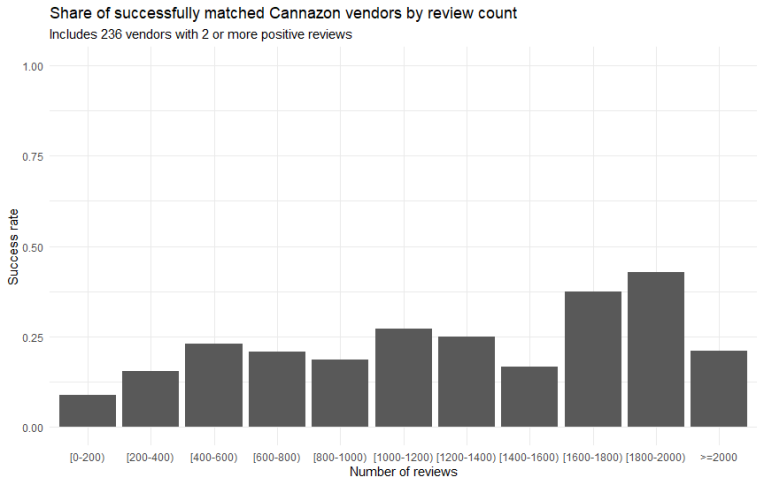


Abb. 15: Erfolgsrate nach Anzahl der Bewertungen auf Cannazon.