Christoph Sorge / Artus Krohn-Grimberghe

Die **Zukunft** des Bezahlens

Für das elektronische Bezahlen – insbesondere im Online-Handel über das Internet – hat sich eine ganze Reihe von Verfahren etabliert. Als Beispiel seien Kreditkartenzahlungen, Lastschriften, aber auch neuartige Angebote wie Skrill, Click-and-Buy oder Paysafecard erwähnt. Gemein ist den Verfahren, das jeweils ein oder mehrere herausgehobene und vertrauenswürdige Instanzen (Banken beziehungsweise Zahlungsdienstleister) zur Abwicklung der Bezahlung herangezogen werden.

Vor- oder nachschüssige Zahlung

Abstrakt betrachtet zahlt der Nutzer in der Regel vorschüssig oder nachschüssig an den Zahlungsdienst, welcher dann wiederum die Forderungen gegenüber dem Händler begleicht. Der Zahlungsdienst führt dazu letztlich Konten für die Nutzer und wickelt Transaktionen ab. Gegebenenfalls können auch mehrere Zahlungsdienste bei der Abwicklung einer Zahlung involviert sein.

Die Nutzung von Chipkarten (Smartcards) stellt einen Sonderfall dar. Meist wird die Smartcard als vertrauenswürdiges Gerät betrachtet, das ein Konto für den Nutzer verwalten und unter anderem sicherstellen kann, dass kein höherer Betrag ausgegeben werden kann, als auf die Karte „aufgeladen" wurde. Die Smartcard übernimmt somit also einen Teil der Aufgaben des vertrauenswürdigen Zahlungsdienstes.

Das beschriebene Prinzip der Abwicklung von Transaktionen kommt auch beim „mobilen Bezahlen" mit Smartphones zum Tragen. Beispielsweise wird bei Google Wallet die sogenannte Near Field Communication (NFC) für kontaktlose Datenübertragung zwischen Mobiltelefon und Terminal eingesetzt. So kann das Smartphone für drahtloses Bezahlen im Einzelhandel genutzt werden. Eine Online-Nutzung ist über das gleiche System ebenso möglich.

Basis-Techniken bereits gut verstanden

Aus Sicht der Informatik sind die Basis-Techniken, die zur Realisierung sicherer Transaktionen nach dem dargestellten Prinzip benötigt werden, bereits gut verstanden. So bietet die Kryptographie seit langem Verfahren, um sicherzustellen, dass nur berechtigte Nutzer eine Transaktion auslösen können – beispielsweise können dazu digitale Signaturverfahren eingesetzt werden. Die Umsetzung in die Praxis stellt aber nach wie vor eine Herausforderung dar. Wird eine Bezahlung über eine Website abgewickelt, können bereits dem Zahlungsdienstleister zahllose Fehler unterlaufen, die zu Sicherheitslücken führen.

Aber auch die Webbrowser, die auf Seiten der Nutzer eingesetzt werden, haben eine Komplexität erreicht, bei der Sicherheitslücken kaum vermeidbar sind – betrachtet man das PC-System des Nutzers als Ganzes, gilt dies in noch stärkerem Ausmaß. Für aktuelle Smartphones gilt bereits das Gleiche, sodass auch in diesem Fall das sichere Bezahlen nicht einfach zu erreichen ist. Die Einbindung als vertrauenswürdig bekannter (und weniger komplexer) Komponenten kann zur Lösung der bestehenden Probleme beitragen. In Mobilfunkgeräten wie Telefonen sind solche Komponenten in Form von SIM-Karten ohnehin enthalten und können einen Baustein eines sicheren Bezahlverfahrens darstellen.

In der Kryptographie werden aber seit langer Zeit Bezahlverfahren diskutiert, die weitergehende Anforderungen erfüllen können.

Anforderungen an elektronische Bezahlverfahren aus Datenschutz-Sicht

Aus Sicht des Datenschutzes ist zu bemängeln, dass der Zahlungsdienst beziehungsweise die Bank alle Zahlungsvorgänge des Kunden sieht. Aus Kundensicht gibt es jedoch einen Wunsch nach Anonymität der Zahlungen: Der Zahlungsdienst soll ähnlich wie bei Bargeld einzelne Zahlungen nicht einzelnen Kunden zuordnen können. Auch der Händler sieht einen Teil der Zahlungsvorgänge des Kunden. Zumindest, soweit digitale Güter verkauft werden, für die der Händler nicht ohnehin eine Lieferadresse braucht, wäre es aus Datenschutzsicht wünschenswert, die Er-

Prof. Dr. Christoph Sorge, Institut für Informatik, und Prof. Dr. Artus Krohn-Grimberghe, Juniorprofessur „Analytische Informationssysteme und Business Intelligence", beide Universität Paderborn

Lassen sich aus Sicht der Informatik verlässliche Aussagen zur Zukunft des Bezahlens treffen? Die Autoren verneinen das, unabhängig davon, ob nur Verfahren für das Bezahlen im Online-Handel betrachtet werden oder auch andere. Als spannendes Konzept mit einer interessanten Umsetzung stufen sie Bitcoin ein, das einen Verzicht auf einen Zahlungsdienstleister vorsieht. Nach einer Würdigung der praktischen Umsetzung aus verschiedenen Blickwinkeln, angefangen von der juristischen Betrachtung über die IT-Sicherheit bis hin zu einigen Zwischenfällen auf Seiten der Dienstleister, sprechen sie auch diesem Ansatz in seiner jetzigen Form das Prädikat „Zukunft des Bezahlens" ab. Für die nahe Zukunft erwarten sie eine weitere Verbreitung von Bezahlverfahren auf Basis von Smartphone-Anwendungen, ohne sich aber auf ein konkretes Konzept festzulegen, das sich durchsetzen wird. (Red.)

stellung von Nutzerprofilen durch Händler zu verhindern.

Ein Händler sollte also nicht feststellen können, ob verschiedene Bezahlvorgänge durch den gleichen Kunden durchgeführt wurden; erst recht sollte dies händlerübergreifend gelten – also, wenn verschiedene Händler ihre Daten zusammenführen, um gemeinsam Nutzerprofile zu erstellen. Möglichst wenige personenbezogene Daten anfallen zu lassen – selbst bei eigentlich vertrauenswürdigen Organisationen – entspricht auch dem in § 3 a des Bundesdatenschutzgesetzes verankerten Grundsatz der Datenvermeidung und Datensparsamkeit.

Chaum et al.[1] entwickelten bereits in den achtziger Jahren ein Verfahren, das die genannten Anforderungen erfüllen kann. Dazu wird das Konzept elektronischer „Münzen" eingeführt, die jeweils einen festen Wert haben. Wird eine Münze nur einmal ausgegeben, bleibt der jeweilige Nutzer anonym; versucht er, sie ein zweites Mal auszugeben, wird dabei mit sehr hoher Wahrscheinlichkeit seine Identität offengelegt. Neuere Verfahren betrachten darüber hinaus auch die Möglichkeit, elektronische Münzen zwischen verschiedenen Nutzern weitergeben zu können, bis sie letztlich wieder beim Zahlungsdienst eingelöst werden.

Das Unternehmen Digi Cash Inc., das das Verfahren von Chaum in die Praxis umsetzte, konnte aber am Markt nicht bestehen; noch existierende Zahlungsdienstleister verwenden deutlich einfachere Verfahren, bei denen Anonymität nicht mit Mitteln der Kryptographie erreicht wird. Regelungen zur Geldwäsche (in Deutschland im Geldwäschegesetz sowie für E-Geld in § 25i des Kreditwesengesetzes) erlauben es auch nicht mehr in allen Fällen, mit Bezahlverfahren vollständige Anonymität zu erreichen – Teilziele[2] ließen sich mit Hilfe der Kryptographie durchaus noch umsetzen, was aber in der Praxis nicht verfolgt wird. Das anonyme Bezahlen von Kleinbeträgen lässt sich allerdings mit Verfahren realisieren, bei denen eine Karte (de facto in der Regel nur eine einmalige Nummer) gegen Bargeld erworben werden kann, die beim Zahlungsdienstleister mit einem Konto verknüpft ist. Mehrere Zahlungen mit der gleichen Karte lassen sich bei diesen Verfahren aber einander zuordnen, womit sie nicht die theoretischen Eigenschaften kryptographischer Bezahlverfahren erreichen.

Bitcoin

Ende 2008 ergab sich eine wesentliche Neuerung im Bereich elektronischer Bezahlverfahren: „Satoshi Nakamoto"[3] veröffentlichte in einem Artikel auf einer Kryptographie-Mailingliste das Konzept von Bitcoin[4]. Anfang 2009 erfolgt die praktische Umsetzung und die Bereitstellung einer Referenzimplementierung. Das Konzept sieht den Verzicht auf einen herausgehobenen Zahlungsdienstleister vor. Vielmehr sind alle Teilnehmer in diesem „Peer-to-Peer-Verfahren" gleichberechtigt. Sie können ohne Mittelsmänner Überweisungen tätigen und sogar selbst Bitcoins schöpfen.

Bitcoin verzichtet auf das Konzept elektronischer Münzen und beruht im Kern auf asymmetrischer Kryptographie[5]: Schlüsselpaare aus öffentlichem und privatem Schlüssel sind die Basis für Überweisungen. Der öffentliche Schlüssel (strenggenommen: ein aus dem öffentlichen Schlüssel abgeleiteter Wert) stellt die Bitcoin-Adresse, eine „Kontonummer", dar. Der zugehörige private Schlüssel wird zur Autorisierung von Überweisungen verwendet. Auf diese Weise sind Überweisungen unproblematisch und sicher – ohne Kenntnis des privaten Schlüssels kann keine Überweisung getätigt werden. Ein Nutzer kann beliebig viele Bitcoin-Adressen (Konten) erzeugen. In der aktuellen Implementierung werden Überweisungen etwa alle zehn Minuten en bloc festgeschrieben; es fallen nur geringe oder gar keine Gebühren an.

Um aus dem beschriebenen Ansatz ein sicheres Bezahlverfahren zu machen, müssen aber noch diverse Probleme gelöst werden. Beispielsweise muss sichergestellt werden, dass die Ausgangskonten gedeckt sind, denn Bitcoin hängt dazu einen Verweis auf die eingehenden Transaktionen an und legt fest, dass nur die erste Referenz auf eine Eingangstransaktion gültig ist, um das doppelte Ausgeben von Beträgen zu verhindern.

Die Reihenfolge der Transaktionen selbst wird in einer öffentlichen Transaktionshistorie, der sogenannten Blockchain, festgehalten. Da eine zentrale Instanz explizit nicht vorgesehen ist, ist noch zu klären, wie die Echtheit einer Transaktionshistorie (von der ansonsten beliebige gefälschte Versionen erzeugt werden können) garantiert werden kann. Ein Quorum an Teilnehmern ist für diese Entscheidung ungeeignet, da Bitcoin ein offenes System ist und Scheinidentitäten möglich sind; daher wurde bei Bitcoin die Mehrheit an Rechenleistung im System als maßgebliches Kriterium ausgewählt. Anders gesagt: Stehen mehrere Möglichkeiten zur Auswahl, gilt die Transaktionshistorie als echt, in die die meiste Rechenleistung geflossen ist. Bitcoin enthält einen Belohnungsmechanismus, der Teilnehmern, die Rechenleistung investieren, die Schaffung neuer Bitcoins ermöglicht.

Eine juristische Betrachtung

Aus juristischer Sicht ist vor allem hervorzuheben, dass es sich bei Bitcoin nicht um elektronisches Geld/E-Geld im Sinne des Zahlungsdiensteaufsichtsgesetzes (§ 1 a Abs. 3) handelt. Es fehlt bei Bitcoin unter anderem an der „Forderung gegenüber dem Emittenten", auch wird Bitcoin nicht „gegen Entgegennahme eines Geldbetrags ausgegeben". Weiterhin ist Bitcoin wohl auch nicht als Geld anzusehen. Strafrechtlich fehlt Bitcoin dazu die staatliche Beglaubigung, ökonomisch die notwendige Verbreitung.

Bitcoin fungiert jedoch als Rechnungseinheit, da der Wert von Gütern und Dienstleistungen in Bitcoin ausgedrückt werden kann und diese Nutzung ausdrücklich auch ein wesentlicher Zweck von Bitcoin ist. Mit der Einordnung als Rechnungseinheit ist Bitcoin jedoch ein Finanzinstrument gemäß § 1 Abs. 11 Satz 1–3 des Gesetzes über das Kreditwesen. Dies wiederum hat zur Folge, dass einige Dienstleistungen auf Bitcoin-Basis erlaubnispflichtig sind.[6]

IT-Sicherheit und Datenschutz

Insgesamt kann Bitcoin als sehr durchdachtes und gut umgesetztes Konzept bezeichnet werden. Jedoch gibt es einige prinzipielle Probleme. Aus Sicht des Datenschutzes ist zu bemängeln, dass die vollständige Transaktionshistorie öffentlich ist. Die Anonymität der Nutzer wird nur ansatzweise dadurch unterstützt, dass die Zuordnung von einem „Konto" zu einem Nutzer beziehungsweise von einer Transaktion zu einem Nutzer schwierig ist. Teilweise ist es jedoch möglich, einer Transaktion die IP-Adresse eines Nutzers zuzuordnen. Auch ist es Forschern in vielen

Fällen gelungen, jeweils mehrere Konten einem Nutzer zuzuordnen.[7)]

Aus Sicht der IT-Sicherheit ist darauf hinzuweisen, dass ein Angreifer mit Kontrolle über genügend Rechenleistung (mehr, als alle korrekt arbeitenden Teilnehmer zusammengenommen investieren) das gesamte System zerstören kann, indem er gefälschte Versionen der Transaktionshistorie erzeugt. Ein weiterer Knackpunkt für die Zukunft wird die Skalierbarkeit sein: mit steigendem Transaktionsvolumen steigt auch die Netzwerklast in Hinblick auf Speicherplatzbedarf und Netzwerkbandbreite. Dies ist insbesondere für den mobilen Einsatz auf langsam angebundenen Geräten mit beschränkter Datenübertragungs- und Speicherkapazität kritisch. Hier zeigt sich schon jetzt über die Verwendung von Whitelists und Zahlungsdienstleister eine Tendenz weg von einer gleichberechtigten Peer-to-Peer-Architektur zur Zentralisierung hin.

Bitcoin in der Praxis

Da Bitcoin maßgeblich von der aufgewendeten Rechenleistung abhängt, darf der Energiebedarf des Bitcoin-Netzwerks nicht vernachlässigt werden – da die Transaktionshistorie als gültig gilt, in die die meiste Rechenleistung geflossen ist, ist es für das Funktionieren des Systems auch nötig, dass korrekt arbeitende Teilnehmer viel Rechenleistung investieren. Schätzungen[8)] zufolge kostet der Rechenaufwand von Bitcoin täglich etwa 1,7 GWh elektrischer Energie, was bei einem Preis von 20 ct je KWh zirka 340 000 Euro pro Betriebstag entspräche. Diese Schätzung ist zwar mit Vorsicht zu genießen, da der genaue Wert von der konkret eingesetzten Hardware abhängt; sie kann aber eine Größenordnung aufzeigen.

Der Wechselkurs von Bitcoin in die maßgeblichen Fiat-Währungen ist aufgrund des geringen Volumens der Märkte starken Schwankungen unterworfen. Zwei bis fünf Prozent pro Tag sind normal, bis zu 15 Prozent pro Tag keine Seltenheit. Dies behindert den Einsatz von Bitcoin zwar nicht als Medium für Zahlungen, ist jedoch für Anleger und Spekulanten sehr riskant.

Zwischenfälle

Bei einer Betrachtung des Bitcoin-Ökosystems darf die Seite der Dienstleister rund um Bitcoin nicht unberücksichtigt bleiben. Dazu gehören die beliebten Online-Wallets, bei denen die privaten Schlüssel für Bitcoin-Konten durch den Dienstleister verwaltet werden, Wechselstuben, komplexe Handelsplattformen und Zahlungsdienste. Viele dieser Unternehmen sind Startups mit keiner bis geringer Erfahrung in den Bereichen der IT-Sicherheit und der Finanzen. Zwischenfälle größeren Ausmaßes (gemessen am Bitcoin-Handelsvolumen) sind dementsprechend keine Seltenheit.

So verlor im Juli 2011 die seinerzeit zweitgrößte Handelsplattform bitomat.pl sämtliche der 17 000 Bitcoins ihrer Kunden bei einer Datenpanne, da kein Backup der privaten Schlüssel vorlag. Nur wenige Tage später unterschlug die Online-Wallet mybitcoin.com vermutlich 79 000 Bitcoins, von denen anschließend angeblich 49 Prozent wieder zurückgezahlt wurden.

In einer Serie von Diebstählen zwischen Februar und Juli 2012 verlor die wiederum zu ihrer Zeit zweitgrößte Bitcoin-Börse (gleichzeitig auch der größter Anbieter von fortgeschrittenen Handelsoptionen) bitcoinica.com sämtliche der von ihr gehaltenen rund 100 000 Bitcoins. Im September 2012 wurden dem Handelsplatz bitfloor.com 17 000 Bitcoins gestohlen, und es wird berichtet, dass der Nutzer „PirateAt40" sich mit einem Schneeballsystem rund 100 000 weitere Bitcoins erschlich. Im Dezember 2012 musste die Bitcoin-Börse bitmarket.eu schließen, da der Betreiber die Bitcoins der Kunden durch eine Spekulation verloren hatte.

Bitcoin stellt zweifelsohne ein spannendes Konzept mit einer technisch interessanten Umsetzung dar. Jedoch sollte man sich gewahr sein, dass Bitcoin keine vollständige Anonymität beim Bezahlen erlaubt – es bleibt in dieser Hinsicht hinter schon lange bekannten kryptographischen Verfahren zurück. Weiterhin gibt es – vor allem hinsichtlich der Natur als Peer-to-Peer-System, also das Funktionieren ohne zentralen Server – große Fragezeichen bezüglich der Umsetzung bei steigendem Volumen.

Echt anonyme kryptografische Bezahlverfahren sind theoretisch spannend. Durch Digi Cash Inc. wurde ein solches Verfahren auch bereits 1990 in der Praxis überführt. Jedoch zeigen nicht zuletzt die Insolvenz von Digi Cash im Jahre 1998 sowie die Marktanteile von Pay-Pal und neuer Dienstleister wie sofortüberweisung.de, dass der Erfolg von Bezahlverfahren nicht allein von deren technischer Eleganz abhängt. Daher lässt sich aus Sicht der Informatik die Frage nach der Zukunft des Bezahlens (auch, wenn es nur den Online-Handel betrifft) nicht beantworten. Es scheint aber wahrscheinlich, dass Bitcoin in seiner jetzigen Form nicht die Zukunft des Bezahlens darstellen wird – und dies allgemein für Verfahren gilt, die ohne vertrauenswürdige Instanzen auszukommen versuchen.

Für die nahe Zukunft ist eine weitere Verbreitung von Bezahlverfahren auf Basis von Smartphone-Anwendungen zu erwarten – welches konkrete Verfahren sich dabei durchsetzen wird, steht aber ebenfalls noch in den Sternen.

Fußnoten

1) David Chaum, Amos Fiat, Moni Naor: Untraceable Electronic Cash. In Advances in Cryptology — CRYPTO' 88, Lecture Notes in Computer Science, Band 403, S. 319–327. Springer, Berlin/Heidelberg, 1990.

2) Beispielsweise Anonymität gegenüber den Händlern oder auch nur ein Schutz gegen das Erstellen händlerübergreifender Nutzerprofile.

3) Es handelt sich hierbei vermutlich um ein Pseudonym; die Person (oder Gruppe), die sich dahinter verbirgt, ist unbekannt.

4) Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System.Online veröffentlicht: http://bitcoin.org/bitcoin.pdf

5) Asymmetrische Kryptographie ermöglicht (neben anderen Anwendungen) die digitale Signatur: Nutzer haben statt eines einzelnen kryptographischen Schlüssels ein Schlüsselpaar. Ein Schlüssel bleibt privat und kann verwendet werden, um Dokumente zu signieren; der korrespondierende öffentliche Schlüssel kann durch beliebige Dritte verwendet werden, um die Signatur zu prüfen.

6) Zur rechtlichen Einordnung auch ausführlich: Christoph Sorge, Artus Krohn-Grimberghe: Bitcoin: Eine erste Einordnung. In Datenschutz und Datensicherheit 36(7), S. 479–484, 2012.

7) Fergal Reid, Martin Harrigan: An Analysis of Anonymity in the Bitcoin System. In Security and Privacy in Social Networks, S. 197–223. Springer, New York 2013; Dorit Ron, Adi Shamir: Quantitative Analysis of the Full Bitcoin Transaction Graph. Online veröffentlicht: Cryptology e-Print Archive: Report 2012/584, http://eprint.iacr.org/2012/584

8) http://blockchain.info/stats mit Stand vom 27. Mai 2013.

Der Beitrag basiert auf einer Rede von Prof. Dr. Christoph Sorge anlässlich des „Zahlungsverkehrssymposiums 2013" der Deutschen Bundesbank.

Die Zwischenüberschriften sind teilweise von der Redaktion eingefügt.