

# Vorlesung Nr. 2

Kryptologie II - Datum: 04.10.2018

- Digitales Geld

# Buch der Woche

**Titel:** Serious Cryptography (1. Auflage, 2018)

**Autor:** Jean-Philippe Aumasson

**Verlag:** no starch press

**Umfang:** ca. 280 Seiten

## **Hinweise zum Inhalt:**

- betrachtet auch theoretische Sicherheitsmodelle für Krypto
- unter anderem Kapitel zu Elliptischen Kurven und zu Quantum Crypto
- enthält diverse kleine Code-Schnipsel als Beispiele
- beschreibt manche Verfahren sehr gut, andere wiederum nur halbherzig und schlecht verständlich
- kleinere inhaltliche (Tipp-)Fehler, da erste Auflage
- insgesamt eines der empfehlenswerteren Bücher

# Status aktuelles Aufgabenblatt

Frage in die Runde:

- Hat jede(r) eine Arbeitsgruppe?
- Gibt es Fragen zur Abgabeprozedur in ILIAS?

Hinweis: die Situation alte versus neue Studien- und Prüfungsordnung wird gerade geklärt. Sollte jemand kein Praktikum mitmachen müssen, weil es die Studien- und Prüfungsordnung nicht vorschreibt, so kann er/sie die (Programmier-)aufgaben weglassen. Die Bearbeitung der sonstigen Aufgaben wird dringend empfohlen, unabhängig davon, ob dies verpflichtend ist oder nicht.

# Vorüberlegungen Digitales Geld

# Kryptowährungen im Aufschwung

- Seit über 30 Jahren verfügen wir über ausreichende kryptographische Protokolle und Algorithmen, um Kryptowährungen in Produkte umzusetzen. Bis vor wenigen Jahren hat das allerdings kaum jemanden interessiert, alle Versuche sind wirtschaftlich gescheitert. Dies hat sich erst geändert mit Bitcoin und Co.
- Frühe Vorschläge favorisierten einen zentralisierten Ansatz, erlaubten jedoch Anonymität, solange nicht betrogen wurde (Double Spending)
- Solche Verfahren kombinierten Methoden aus Blind Signatures, Bit Commitment Schemes, Secret Sharing, Public Key Crypto (RSA), etc.
- Aktuell erfolgreiche Ansätze verfolgen zumeist einen dezentralen Ansatz. Verwendete Komponenten sind unter anderem spezielle Hashfunktionen (resistent gegen Mining Pools mit Spezialhardware), Post-Quantum Public Key Crypto, Proof of Work Schemes, Proof of Stake Schemes, Blockchain, diverse Varianten von Hash Chains/Graphs, und vieles mehr.

# Was ist Digitales Geld?

Frage in die Runde: Meinungen, Vorschläge?

# Was ist Digitales Geld?

- Ist vielleicht ALLES digitales Geld außer Bargeld? Salden, Kontostände, Bankguthaben, Schulden, Targetsalden, etc.?
- Ist eine Online-Überweisung digitales Geld?
- Ist Guthaben auf dem Girokonto digitales Geld?
- Sind angesammelte Rentenansprüche digitales Geld?
- Ist Guthaben auf der Chipkarte digitales Geld?
- ...oder sind nur Cryptocurrencies wie Bitcoin oder Ethereum digitales Geld?
- Gibt es Unterschiede zwischen den Begriffen elektronisches / virtuelles / digitales Geld?

# Beispiele für Digitales Geld































- Ja, natürlich: Bitcoin

Frage in die Runde: weitere Beispiele?



## Top 100 Cryptocurrencies By Market Capitalization

Cryptocurrencies Exchanges Watchlist USD Next 100 View All

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	 Bitcoin	\$106,114,476,692	\$6,168.08	\$4,221,633,186	17,203,812 BTC	-4.27%	
2	 Ethereum	\$31,413,818,548	\$310.22	\$1,721,043,821	101,262,115 ETH	-13.77%	
3	 XRP	\$11,525,998,075	\$0.293283	\$290,104,395	39,299,874,590 XRP *	-12.46%	
4	 Bitcoin Cash	\$9,582,115,039	\$554.29	\$334,749,961	17,287,263 BCH	-6.95%	
5	 EOS	\$4,483,373,021	\$4.95	\$670,091,861	906,245,118 EOS *	-11.05%	
6	 Stellar	\$3,890,782,583	\$0.207272	\$110,949,940	18,771,403,505 XLM *	-8.76%	
7	 Litecoin	\$3,265,931,907	\$56.50	\$256,393,632	57,804,257 LTC	-9.55%	
8	 Cardano	\$2,859,008,736	\$0.110271	\$66,355,082	25,927,070,538 ADA *	-7.59%	
9	 Tether	\$2,413,352,310	\$1.00	\$2,793,709,693	2,407,140,346 USDT *	0.07%	
10	 TRON	\$1,469,401,899	\$0.022349	\$118,172,648	65,748,111,645 TRX *	-10.64%	
11	 Monero	\$1,452,508,157	\$89.29	\$28,983,809	16,266,706 XMR	-9.18%	
12	 IOTA	\$1,428,754,716	\$0.514027	\$48,305,506	2,779,530,283 MIOTA *	-14.76%	
13	 Dash	\$1,349,645,936	\$163.56	\$114,575,023	8,251,735 DASH	-11.02%	
14	 Ethereum Classic	\$1,320,518,292	\$12.73	\$258,706,332	103,707,744 ETC	-15.52%	
15	 NEO	\$1,166,794,998	\$17.95	\$77,073,354	65,000,000 NEO *	-15.31%	

Marktwert von  
Cryptowährungen in Dollar.  
Hier nur ein Ausschnitt, die  
Liste ist sehr viel länger.  
Info siehe [coinmarketcap.com](https://coinmarketcap.com)

# Anonym oder Identifizierbar?

- Es gibt kryptographische Lösungen und Protokolle sowohl für anonymes Bezahlen als auch für nichtanonymes Bezahlen. Ferner finden sich Lösungen für pseudonymes Bezahlen, d.h. der Bezahlvorgang ist zwar an eine Identität geknüpft, doch diese ist nicht ohne weiteres dem Namen einer Person zuzuordnen.
- Frage in die Runde: In welche Kategorie gehört Bitcoin?
- Frage in die Runde: Welche Vor- und Nachteile hat Anonymität?
- Wieviel Kriminalität sind wir bereit zu akzeptieren zugunsten anonymer Bezahlverfahren?
- Wieviel Freiheit sind wir bereit aufzugeben zugunsten nichtanonymer Bezahlverfahren?
- Geben wir überhaupt Freiheiten auf? Falls nicht, was sonst?
- Frage in die Runde: Glauben Sie, dass Bargeld in einigen Jahren komplett abgeschafft wird? Wollen wir das?

# Zentral oder Dezentral?

Digitales Geld kann, in Abhängigkeit von zugrundeliegenden Anforderungen und Philosophie ganz unterschiedlich realisiert werden. Eine grundsätzliche Unterscheidung besteht darin, ob das System dezentral sein soll (z.B. Bitcoin), oder ob es eine zentrale Instanz geben soll, die technisch/wirtschaftlich/rechtlich für das System zuständig ist.

- Frage in die Runde: welche Merkmale fallen Ihnen ein für zentrale / dezentrale Realisierungen?
- Frage in die Runde: ist Bargeld zentral oder dezentral?
- Frage in die Runde: welche Vorteile und Nachteile haben zentrale / dezentrale Ansätze?

# Nachteile von Bitcoin und Co.

- Zahlungen der organisierten Kriminalität und Geldwäsche sind nicht einzudämmen
- Erpressung wird erleichtert (z.B. Ransomware, aber als klassische Erpressung und/oder Entführung etc.)
- Falls ein Mitarbeiter absichtlich oder versehentlich eine Bitcoin-Überweisung an eine falsche oder unautorisierte Adresse sendet, so gibt es keinen Weg, das Geld zurück zu holen
- Im Fall von Phishing Attacken oder sonstigen breit angelegten Betrugsversuchen gibt es keine Instanz, die Beschwerden entgegen nehmen und den Betrug unterbinden könnte
- Falls ein Private Key verloren geht (z.B. Software- oder Hardwarefehler, oder im Rahmen einer Attacke), so ist das gesamte mit diesem Key / dieser Adresse verbundene Bitcoin-Vermögen verloren. Niemand kann jemals wieder auf dieses Geld zugreifen, es ist quasi aus dem Verkehr genommen
- Es gibt nichts vergleichbares wie eine Einlagensicherung bei Banken. Falls die Kryptowährung kollabiert, ist das Geld weg
- Falls irgendetwas nicht funktioniert, so gibt es keine zuständige Instanz (Service Hotline, Beschwerdestelle o.ä.), an die man sich wenden könnte
- Frage in die Runde: nach Kenntnis obengenannter Probleme – würden Sie noch immer Bitcoin und ähnliche Cryptocurrencies nutzen für Ihr eigenes Geld?

# Grundlagen und Einfache Beispiele für Digital Payment Protocols

# Elektronische Schecks

- Die elektronische Form eines gewöhnlichen Schecks läßt sich leicht mittels digitaler Signaturen erstellen. Mit „Scheckdaten“ bezeichnen wir die auf einem ausgefüllten Scheck befindlichen Informationen wie Bankname, Name von Aussteller und Empfänger, Geldbetrag, Datum etc. Ferner bezeichne  $\text{Sig}_A(X)$  eine digitale Signatur der Daten  $X$  durch Teilnehmer  $A$ . Die einfachste Form eines elektronischen Schecks besteht sodann aus

$\text{Sig}_{\text{Aussteller}}(\text{Scheckdaten})$

- Mehr Sicherheit für alle an der Transaktion beteiligten läßt sich dadurch erreichen, daß jeder das erhaltene elektronische Scheckformular digital signiert, bevor er es weiterreicht; ausführlich bedeutet dies:

$\text{Sig}_{\text{Bank des Ausstellers}}(\text{Sig}_{\text{Bank des Empfängers}}(\text{Sig}_{\text{Empfänger}}(\text{Sig}_{\text{Aussteller}}(\text{Scheckdaten})))$

- Zusätzlich ließe sich noch Verschlüsselung mit dem Public Key des Empfängers integrieren, so daß auch noch Vertraulichkeit gewährleistet wird. Ferner lassen sich Schecks generieren mit Auszahlungsgarantie seitens der Bank des Ausstellers, indem diese zunächst die betreffenden Scheckdaten „anerkennt“ und digital signiert mittels  $\text{Sig}_{\text{Bank des Ausstellers}}(\text{Scheckdaten})$ .

# Kann man blind signieren?

Frage in die Runde:

Angenommen wir haben ein Szenario, in dem wir von jemandem eine digitale Signatur auf einem Dokument benötigen, wobei wir den Inhalt des Dokumentes aber nicht offenlegen möchten.

Kann so etwas technisch möglich sein?

Gibt es solche Szenarien? Wo könnte dies sinnvoll sein?

# Blinde Signaturen und Cut and Choose

**Unser Ziel:** wir möchten unseren Kommunikationspartner (hier: die Bank) dazu bewegen ein Dokument zu signieren, das er zuvor nicht gesehen hat. Dennoch soll er uns vertrauen, daß der Inhalt des Dokumentes die vereinbarte Form (verabredeter Geldbetrag etc.) hat.

Dieses „blinde Signieren“ durch den Kommunikationspartner erlaubt uns, jene Teilinformationen des Dokumentinhaltes, aus welchen unsere Identität hervorgeht, vor unserem Gegenüber geheim zu halten.

Im folgenden werden wir sehen, wie Blinde Signaturen im Zusammenhang mit anonymen Zahlungsmitteln eingesetzt werden können.

**Anmerkung:** für unsere Zwecke wäre es noch keine Lösung, ein Dokument geheim zu halten und nur dessen Hashwert zum Signieren einzureichen, denn wir möchten auch die Kenntnis des Hashwerts geheim halten.

Zusätzlich möchte der Unterzeichner seinerseits gewisse Sicherheiten erhalten, dass er/sie nicht etwas Unerwünschtes signieren soll.



# Cut-and-Choose Protokoll

- Angenommen, zwei Personen haben ein großes Stück Kuchen und möchten dieses fair (d.h. gleich große Teilstücke) untereinander aufteilen. Eine Möglichkeit besteht darin, dass Person A die Aufteilung vornimmt und Person B sodann eines der beiden Teile auswählen darf. Dieses “Protokoll” nennt man Cut-and-Choose.
- Eine nicht-digitale Variante dieses Protokolls könnte beispielsweise so aussehen:  
Beispiel: Wir möchten einen Reisescheck von unserer Bank. Damit dieser gültig ist, muss ihn die Bank zuvor unterschreiben. Wir möchten jedoch nicht, dass die Bank die Seriennummer des unterschriebenen Reiseschecks sieht. Wie gehen wir vor?  
Wir legen unserer Bank 50 verschlossene Briefumschläge mit nummerierten Reiseschecks vor. Hiervon öffnet die Bank alle bis auf einen und verifiziert, daß die enthaltenen Schecks alle den zuvor vereinbarten Betrag enthalten. Ist dies der Fall, so wird die Bank nun bereit sein, den noch verbleibenden Scheck ungesehen (“abgedeckt”) zu unterschreiben in dem Vertrauen, daß auch dieser den vereinbarten Inhalt aufweist.
- In der Kryptographie verallgemeinert man dieses Prinzip so, dass eine Partei eine bestimmte Anzahl von Versionen (einen “Pool”) eines Parameters zur Verwendung in einem gemeinsamen Protokoll vorschlägt, die andere Partei sodann einen Teil der Parameter überprüft, ob diese die geforderten Eigenschaften erfüllen. Ist dies der Fall, so wird einer (oder mehrere) der verbleibenden Parameter ohne gesonderte Prüfung zur Verwendung im Protokoll übernommen.

# Blinde Signaturen

Wir haben folgende Ausgangssituation. Teilnehmer A hat ein Dokument, welches er von Teilnehmer B gerne digital signiert haben möchte. Hierbei soll B jedoch keine Kenntnis davon erhalten, was er für A signiert. Angenommen, B bildet digitale Signaturen mittels RSA. Dann können die beiden (vereinfacht dargestellt) wie folgt vorgehen:

Sei  $H(m)$  der zu signierende Wert (wobei  $m$  eine Nachricht und  $H(m)$  der zugehörige Hashwert sei),  $n$  bezeichne den RSA-Modul,  $e$  den öffentlichen Schlüssel und  $d$  den geheimen Schlüssel. Teilnehmer A wählt nun eine zufällig gewählte Zahl  $k$ ,  $1 \leq k \leq n$ , den sogenannten **Blinding Factor**. Danach sendet er an B den Wert

$$r := H(m)k^e \bmod n$$

B signiert nun den Wert  $r$  und sendet das Ergebnis zurück an A:

$$r^d = (H(m)k^e)^d \bmod n$$

Wie man sieht, gilt  $r^d = H(m)^d \bmod n$ , so daß A nun im Besitz einer gültigen Signatur für  $H(m)$  ist. Man kann sich überlegen, daß der Wert  $r$  keinerlei Information preisgibt über das zu signierende  $H(m)$ .

# Blinde Signatur und Cut & Choose (1)

## Beispiel:

- Der Kunde fordert eine Einheit anonymes elektronisches Geld über einen bestimmten Geldbetrag, z.B. 100 Euro, von seiner Bank. Hierzu erzeugt er seiner Bank  $k$  Beispiel-Einheiten; diese enthalten den Namen der auszahlenden Bank, den Geldbetrag, die zugehörige Währung etc., doch keinerlei Namensangaben über den Kunden.
- Jede der obigen Beispiel-Einheiten ist versehen mit einer eindeutigen, individuellen Seriennummer, deren Länge es praktisch nahezu ausschließt, daß jemals zwei dieser Seriennummern gleich sind; eine mögliche Länge dieser Seriennummer wäre 128 Bit.
- Die obigen Beispiel-Einheiten  $m_i$  sind in einem fest vereinbarten Standardformat kodiert, beispielsweise  $m_1 := (\text{Bank, Geldbetrag, Währung, 1. Seriennummer, ...})$ , ...,  $m_k := (\text{Bank, Geldbetrag, Währung, k-te Seriennummer, ...})$ .
- Der Kunde versieht die obigen  $k$  Datensätze mit verschiedenen Blinding factors  $b_i$ , d.h. er berechnet (mod  $n$ ):  $m_1 b_1^e$ ,  $m_2 b_2^e$ , ...,  $m_k b_k^e$ , wobei  $(e, n)$  der Public Key der Bank sei.

# Blinde Signatur und Cut & Choose (2)

- Der Kunde übergibt die so präparierten Datensätze an seine Bank.
- Die Bank wählt  $k-1$  dieser Datensätze und verlangt die zu diesen gehörigen  $k-1$  Blinding Factors. Der verbleibende Datensatz sei  $m_i b_i^e$ .
- Der Kunde übergibt die geforderten  $k-1$  Blinding Factors an seine Bank.
- Die Bank entfernt die Blinding Factors von den erhaltenen  $k-1$  Datensätzen und überprüft, ob alle resultierenden  $m_j$  die vereinbarte Form und den vom Kunden genannten Geldbetrag beinhalten. Ist dies nicht der Fall, so wird ein Verfahren wegen versuchten Betruges eingeleitet.
- Verliefe die Überprüfung ohne Beanstandungen, so signiert die Bank die noch mit einem Blinding factor versehene Geldeinheit  $m_i b_i^e$  mit ihrem Secret Key, bildet also  $(m_i b_i^e)^d = m_i^d b_i$ .
- Der Kunde entfernt den Blinding Factor  $b_i$  und verfügt nunmehr über die signierte, elektronische Geldeinheit  $m_i^d$ .

# Double Spending Problem

Frage in die Runde:

Angenommen wir haben anonymes digitales Geld. Was hindert uns daran, eine solche Geldeinheit einfach mehrmals zum Bezahlen zu verwenden?

Gibt es eine Möglichkeit, dies zu verhindern?

Falls ja, wie könnte das gehen und welche Voraussetzungen müssen hierzu erfüllt sein?

Oder geht das grundsätzlich nicht und wir lösen das Problem einfach so, dass der erste von mehreren Personen, der das Geld einlösen will, gewinnt?