BlockChain – vom Prinzip zu Kryptowährungen

Von Gilbert Brands

Einführung. Das Wort „Blockchain“ ist ähnlich wie „Künstliche Intelligenz“ ein Modebegriff geworden. Man kann mit Begriffen, mit denen kaum jemand etwas Konkretes verbinden kann, nicht nur ganz gut Geld verdienen, man kann auch die eine oder andere Gefahr, die mit bestimmten Anwendungen verbunden sind, recht gut verstecken. Hier sind insbesondere Kryptowährungen zu nennen, die aufgrund der geopolitischen Lage derzeit wieder als Alternative zu realen Währungen propagiert werden.

Wir stellen hier das Grundprinzip der Blockchain-Technologie und einige Einsatzmöglichkeiten vor, wobei auf Kryptowährungen wie beispielsweise BitCoin ausführlicher eingegangen wird. Vorab sei festgestellt, dass Kryptowährungen letztlich Schneeball- oder Ponzi-Systeme sind, deren spekulativer Einsatz nicht ungefährlich ist und die nur bedingt als Alternativen für Zahlungssysteme in Frage kommen.

Die zum Einsatz kommenden Algorithmen beschreiben wir lediglich verbal und verzichten auf eine Darstellung der Mathematik. Einige Datenstrukturen beschreiben wir in ASN.1-Notation, die mehr oder weniger intuitiv verständlich sein dürfte. Dies dient jedoch nur dem Verständnis und bezieht sich nicht auf konkrete Anwendungen, in denen die komplexen Abläufe weitere Steuerelemente notwendig machen.

Blockchain – das Grundprinzip

Eine Blockchain ist eine Methode, eine nicht fälschbare Verkettung von Datensätzen zu erzeugen. In solchen Ketten darf es weder möglich sein, unerkannt ein Kettenglied zu fälschen oder zu ersetzen noch die Reihenfolge der Glieder zu ändern.

Beim Einsatz einer Blockchain gibt es drei beteiligte Gruppen:

- Die Blockchain-Verwalter sind für die Führung und Erweiterung der Blockchain verantwortlich,
- die Signaturgeber fügen bei jeder Erweiterung bestimmte Elemente hinzu, die die Integrität sichern und
- die Teilnehmer können sich jederzeit davon überzeugen, dass die Integrität der Kette gewahrt ist.

Je nach Anwendung müssen die Gruppen nicht elementfremd sein.

Ein Datensatz einer Blockchain besitzt in Prinzip die folgende Form (die anwendungsbedingt sehr viel komplexer aussehen kann, aber immer diese Grundelemente enthält):

```
BlockChainEntry ::= SEQUENCE {
      blockData   BlockChainData,
      sig         Signature
}

BlackChainData ::= SEQUENCE {
      data        BitString,
      prevsig     Signature
}
```

Die Blockchain-Datensätze können fortlaufend nummeriert sein, müssen dies aber nicht. Die eigentlichen Daten (**blockData** und **data**) werden durch eine Signatur ergänzt (siehe folgenden Abschnitt). Eine Signatur ist ein Bitmuster, das aus den Daten erzeugt wird und nur zu diesen Daten passt. Es kann nur von einem Signaturgeber erzeugt, aber von allen anderen überprüft werden. Werden die Daten oder das Bitmuster verändert, schlägt diese Prüfung fehl und offenbart einen Betrug.

Die Signatur **sig** sichert die Integrität von **data.** Dieses Feld wiederum enthält neben den eigentlichen Daten die Signatur des vorhergehenden Datenblocks (die dort im Feld **sig** abgelegt ist). Ist der Satz korrekt signiert und entspricht **prevsig** der Signatur des vorhergehenden Satzes, kann man nun diesen auf die gleiche Weise auf Korrektheit prüfen und dies rekursiv bis zum Beginn der Kette fortsetzen.

> *Nehmen wir an, ein Datensatz im Blockchain-Datensatz N würde ausgetauscht und für diesen Datensatz eine neue Signatur berechnet. Alle Blockchain-Datensätze von 1 .. N wären dann weiterhin korrekt.*
>
> *Der Blockchain-Datensatz (N+1) wäre allerdings nicht mehr korrekt:* **prevsig** *stimmt nicht mit der Signatur von Satz N überein, da diese ja geändert wurde. Um das zu korrigieren, muss auch diese Signatur neu berechnet werden, wodurch aber nun Satz (N+2) nicht mehr in die Kette passt. Der Korrekturprozess muss bis zum Ende der Blockchain fortgeführt werden, um wieder eine vollständig integere Kette zu erhalten.*

Um die Integrität einer Kette nachzuweisen, ist sie komplett zu laden und von vorne bis hinten auf korrekte Daten und Signaturen (und ggf. weitere anwendungsbedingte Parameter) zu kontrollieren. Das kann bei größeren Ketten aufwändig werden, jedoch erfordert das keine speziellen Geräte oder Fähigkeiten und kann im Prinzip von jedem ausgeführt werden. Die beteiligten Gruppen können daher jederzeit durch neue Mitglieder erweitert werden.

Soll bei einer solchen Prüfung der tatsächliche Inhalt des Feldes **data** nicht bekannt werden, sind die Datensätze zu verschlüsseln. Dies ist allerdings eine Grundsatzentscheidung: ob ein Datensatz verschlüsselt wird oder nicht, ist vor der Erstellung der Signatur zu entscheiden. Einmal in der Kette befindliche Datensätze können werden ver- noch entschlüsselt werden, ohne die Signaturen ungültig werden zu lassen.

Eine Blockchain kann nur dann sinnvoll eingesetzt werden, wenn die Wahrscheinlichkeit einer nachträglichen Fälschung der Kette so klein gemacht werden kann, dass die Sicherheitsanforderungen aller Beteiligten erfüllt sind.

Die Formulierung ist deshalb so kompliziert, weil sich die Sicherheitsmaßnahmen natürlich auch an dem orientieren müssen, das abgesichert werden soll. Wer nur einen Bollerwagen in der Garage hat, wird möglicherweise schon zufrieden sein, wenn sich die Tür schließen lässt, wer einen Bugatti im Wert von 1,2 Mio € besitzt, wird sicher andere Vorstellungen haben.

Für eine Sicherheitsbewertung ist zu untersuchen, welcher Beteiligte ein Interesse an einer Fälschung haben könnte. Wie das Funktionsprinzip zeigt, ist eine Fälschung ohne Beteiligung der Signaturgeber nicht möglich. Im Wesentlichen ist bei der Gesamtkonstruktion der Anwendung darauf zu achten, dass

- der Signaturgeber nicht von anderen Beteiligten ausgenutzt werden kann, ohne das er dies erkennt.

Im Weiteren ist dafür zu sorgen, dass

- der Signaturgeber durch Ehrlichkeit einen größeren Profit erreicht als durch Betrug.

Alternativ kann dafür gesorgt werden, dass

- das Signaturverfahren (zeitlich) so aufwendig ist, dass neuere Versionen der korrekten Kette allen Beteiligten vor Abschluss der Fälschung vorliegen und diese deshalb nicht eingebaut werden kann.

Signaturen

Eine Signatur ist eine elektronische Unterschrift. Sie kann von jedem leicht überprüft, aber nur vom Signaturgeber erstellt werden. Jeder Versuch, die signierten Daten oder die Signatur zu fälschen, führt dazu, dass die Prüfung fehl schlägt.

Ein Signaturverfahren benötigt zwei Verschlüsselungsverfahren:

- Eine Hashfunktion oder Einwegverschlüsselungsfunktion, die aus einem Datensatz beliebiger Länge einen individuellen Datensatz fester Länge macht und die so gestaltet ist, dass
    - zwei beliebige Eingabewerte zwei unterschiedliche Ausgabewerte ergeben und keine Wiederholungen auftreten,
    - es nicht möglich ist, einen Eingabewert so zu konstruieren, dass ein bestimmter Hashwert resultiert und
    - es nicht möglich ist, vom Hashwert auf den Inhalt der ursprünglichen Nachricht zurück zu schließen.

Da der Eingabewert beliebig lang sein darf, die Länge des Hashwertes aber begrenzt ist, existieren natürlich Eingaben mit dem gleichen Hashwert, wenn die Eingabewerte länger sind als der Hashwert. Hashwerte haben allerdings Längen von 256 oder mehr Bit, was bedeutet, dass es

mehr als 10^{77} verschiedene Hashwerte gibt. Die Wahrscheinlichkeit, zwei Eingaben mit dem gleichen Hashwert zu finden, ist also extrem klein.

Gute Hashfunktionen haben die Eigenschaft, keine Abkürzungen zu besitzen, d.h. wenn man zwei Eingaben mit gleichem Hashwert sucht, bleibt nichts anderes übrig, als nach dem Zufallsprinzip alle Möglichkeiten durch zu probieren.

Ob eine Nachricht zu einem bestimmten Hashwert gehört, lässt sich nur feststellen, indem man den Hashwert neu berechnet. Wird vor der Berechnung ein geheimer Schlüssel zu der Nachricht hinzugefügt, kann ohne diesen Schlüssel nicht festgestellt werden, auf welche Nachricht ein sich so gebildeter Hashwert bezieht.

- Ein asymmetrisches Verschlüsselungsverfahren, das die Ver- und Entschlüsselung beliebig langer Nachrichten erlaubt und folgende Eigenschaften besitzt:
    - Für die Verschlüsselung wird ein anderer Schlüssel benötigt als für die Entschlüsselung. Ein Schlüssel wird als „öffentlicher Schlüssel“ bekannt gemacht, der andere als „geheimer Schlüssel“ vom Ersteller des Schlüsselpaars geheim gehalten.
    - Aus dem öffentlichen Schlüssel der geheime Schlüssel nicht abgeleitet werden.

Wie bei den Hashfunktionen muss man mehr oder weniger alle Optionen ausprobieren. Es existieren zwar einige mathematische Verfahren, die jedoch ebenfalls zu aufwendig sind, um schnellen Erfolg zu garantieren.

Mit einer asymmetrischen Verschlüsselungsfunktion bestehen somit die Möglichkeiten, dass

- jeder mit dem öffentlichen Schlüssel eine Nachricht verschlüsseln kann, die nur der Inhaber des Geheimschlüssel entschlüsseln kann;
- mit dem Geheimschlüssel eine Nachricht verschlüsselt werden kann, die jeder mit dem öffentlichen Schlüssel entschlüsseln und damit sicher sein kann, dass sie vom Inhaber des Geheimschlüssels verschlüsselt wurde.

Eine Signatur besteht aus dem Hashwert einer Nachricht, der mit dem privaten Schlüssel verschlüsselt wird. Der öffentliche Schlüssel wird durch ein Zertifikat bekannt gemacht, das den Schlüssel mit der Identität des Inhabers des Geheimschlüssels verknüpft und ebenfalls durch eine Signatur gegen Fälschung gesichert wird. Man kann sich mit verschiedenen Methoden davon überzeugen, dass das Zertifikat von einem bestimmten Inhaber ausgestellt wurde und dem Zertifikat anschließend ohne erneute Prüfung vertrauen.

Der Umweg über den Hashwert hat zeitliche Gründe. Den Hashwert etlicher Megabyte zu berechnen geht sehr schnell, die komplette Nachricht zu verschlüsseln, dauert ziemlich lange.

Eine Signatur besteht somit aus dem Datenpaket

```
Signature ::= SEQUENCE {
      cert        Certificate
      sig         IA5String,
}

Certificate ::= SEQUENCE {
      SEQUENCE {
            pk          PubKey,
            par         CertParameter,
      }
      sig         IA5String
}
```

Die Berechnung erfolgt durch

```
hash = hasf_func(data | parameter)
sig = encrypt( private_key , hash)
```

Die Prüfung ist erfolgreich, wenn

```
hasf_func(data | parameter) = decrypt(public_key , sig)
```

gilt. Sowohl die Ausstellung als auch die Prüfung solcher Signaturen erfordert keinen nennenswerten Aufwand.

Signaturen in Verbindung mit einer Blockchain

Der Signaturersteller ist der Verwalter der Blockchain

Liegt alles – Verwaltung der Blockchain und Signatur – in einer Hand, kann jederzeit eine Fälschung durchgeführt werden, wobei ein Richter bei Vorlage beider Ketten nicht entscheiden kann, welche das Original und welche die Fälschung ist. Trotzdem existieren auch unter solchen Umständen sinnvolle Einsatzmöglichkeiten der Blockchain, wenn der Inhaber ein Interesse daran hat, dass die übrigen Teilnehmer ihm vertrauen.

Das ist beispielsweise der Fall, wenn Zertifikate für bestimmte Zwecke ausgestellt werden oder nur eine bestimmte Zeit gelten und dann durch neue ersetzt werden. Um zu vermeiden, dass bei jedem neuen Zertifikat ein Empfänger umständlich prüfen muss, ob der Inhaber tatsächlich derjenige ist, der er vorgibt zu sein, wird im Feld **CertParameter** das Vorgängerzertifikat oder ein spezielles Master-Zertifikat untergebracht und das neue Zertifikat mit diesem Zertifikat signiert und nicht mit dem eigenen privaten Schlüssel. Das neue Zertifikat kann daher nur von jemandem stammen, dem man schon vertraut, und ist daher ebenfalls vertrauenswürdig.

Die Blockchain

- bildet Ketten von einander ablösenden Zerifikaten, wenn der Vorgänger den Nachfolger signiert, oder

- spaltet sternförmig auf, wenn Zertifikate für unterschiedliche Zwecke in Verbindung mit einem Masterzertifikat verwendet werden.

Notarfunktion

Sind Verwalter und Signaturgeber der Blockchain voneinander verschieden, müssen beide zusammen arbeiten, um eine Fälschung zu produzieren. Dazu muss sich der Signaturgeber allerdings Kontrollinformationen merken und darf nichts blind signieren.

Dazu genügt es bereits, wenn der Signaturgeber als Notar fortlaufende Nummern vergibt, die öffentlich bekannt sind und eindeutig einem Satz in der Blockchain zugeordnet werden (beispielsweise im Datenteil der Blockchain notiert werden). Die Signatur eines neuen Datensatzes besteht aus der Verkettung

```
sig = encrypt(private_key , hash( [N-1] | [N] | data) )
```

wobei [N-1] die vom Notar vergebene Nummer des letzten Blockchainsatzes ist, [N] die Nummer des neuen. Es genügt, wenn der Verwalter dem Notar anstelle von **data** nur den Hashwert liefert. Da andere Teilnehmer aufgrund der Regeln auf die Nummern [N-1] und [N] schließen und einen Hashwert berechnen können, fällt ein Betrugsversuch auf.

Laut Buchführung des Notars käme bei einem neuen Datensatz das Paar (4711 , 4712) zum Einsatz. Kappt der Verwalter die Kette bei Glied 1211 und fälscht Glied 1212, so würde ein Teilnehmer

```
hash(1211 | 1212 |  data) ≠ decrypt(public_key , sig)
```

feststellen, da der Notar seine Zahlen verwendet hat, die zu einer anderen Signatur führen.

Der Signaturgeber wird als vertrauenswürdige Instanz betrachtet (Notar) und erzeugt die Signatur gegen Vergütung. Die Einsatzfelder hängen natürlich davon ab, dass Verwalter und Teilnehmer das notwendige Vertrauen in die Ehrlichkeit des Notars aufbringen.

Wechselnde Signaturgeber

Sind an der Bildung und Verwaltung der Blockchain K Parteien beteiligt, kann der Signaturgeber aus diesem Kreis nach einem festgelegten Verfahren für jeden Verkettungsschritt nach dem Zufallsprinzip neu ermittelt werden. Bekommt jeder Signaturgeber eine fortlaufende Nummer, so kann der nächste zufällig durch die Berechnung des Indexwertes anhand des aktuellen Hashwertes

$$k \equiv \text{hash}(\ldots) \bmod K$$

berechnet werden. Der so berechnete Teilnehmer signiert das neue Datenpaket, das alle anderen an ihre Blockchain anfügen. Eine Veränderung eines älteren Datensatzes ist nur möglich, wenn der die Veränderung signierende Teilnehmer und alle Signaturgeber der darauf folgenden Sätze betrügen. Da die Reihenfolge zufällig ist und vom signierenden Hashwert abhängt, müssen zwangsweise alle betrügen.

Dieses Signaturprinzip wird in einigen Kryptowährungsmodellen eingesetzt. Die Signaturerstellung ist in solchen Modellen stets mit einer Prämie verbunden (s.u.). Die Ermittlung des nächsten Signaturgebers kann aufwendig werden, wenn aus technischen Gründen nicht alle Teilnehmer als Signaturgeber in Frage kommen, jedoch verhindert werden soll, dass einige Teilnehmer zu stark von der Prämienausschüttung profitieren.

Das Signaturmodell wird beispielsweise bei der Aufbewahrung und dem Nachweis von Gesundheitsdaten diskutiert. Eine zentrale Verwaltung aller Patientendaten ist aus verschiedenen Gründen zu aufwendig und kostenintensiv, so dass die Daten auf von den Patienten selbst verwalteten Chipkarten gespeichert werden. Ein neuer Befund kann nach Vorlage der Karte beim Arzt von diesem als neuer Satz an die Blockchain angehängt und signiert werden.

Die Rolle des Zufalls übernimmt gewissermaßen die Erkrankung des Patienten.

Ärzte könnten versucht sein, einen für sie peinlichen Befund zu fälschen, müssten dann aber alle Kollegen danach überreden, ihre Signaturen zu ändern, was vermutlich schwierig wird. Sie könnten natürlich auch, wie die Patienten ebenfalls, die Kette irgendwo kappen, was aber irgendwann vermutlich auffallen würde (z.B. bei der Kontrolle der Abrechnungsdaten). Patienten als technisch unbedarfte Teilnehmer könnte die Karte aber auch einfach „verlieren“.

In der Kritik steht die „Gesundheitskarte“ aber weniger wegen der verwendeten Technik als vielmehr aufgrund des befürchteten Missbrauchs der Daten, der teilweise bereits absehbar ist.

Signatur durch Arbeitsaufwand

Durch Veränderung der Berechnungsvorschrift für die Hashfunktion kann die Erzeugung der Signatur in einen länger dauernden Vorgang verwandelt werden. Bei einer gut konstruierten Hashfunktion ist es in der Praxis zwar nicht möglich, einen bestimmten Hashwert zu erzeugen, mit höherem Arbeitsaufwand ist es aber ohne Weiteres möglich, zu erreichen, dass zumindest Teile des Hashwertes bestimmte Muster aufweisen. Beispielsweise kann man fordern, dass durch Ergänzung der Daten durch einen zusätzlichen Wert namens **nonce** eine bestimmte Anzahl Führungsbits den Wert 0 aufweisen

```
hash( data | nonce ) = 000..0xxx...xx
```

Hierbei wird die Zufallzahl **nonce** zufällig so lange verändert, bis ein Hashwert mit den gewünschten Eigenschaften erzeugt wird.

Hat eine Hashfunktion beispielsweise 32 Bit, was 4.294.967.296 verschiedenen Hashwerten entspricht, müsste man im im ungünstigsten Fall alle 4.294.967.296 dieser Möglichkeiten an verschiedenen Eingabedaten ausprobieren, um einen bestimmten Hashwert zu erhalten. Sollen die vorderen 8 Bit den Wert 0 aufweisen, hat man bis auf Ausnahmen nach 256 Versuchen oder früher Erfolg.

Hashfunktionen weisen in der Praxis 256 oder 512 Bit auf, d.h. man kann den notwendigen Rechenaufwand durch Vorgabe entsprechender Muster beliebig steuern.

nonce wird als zusätzlicher Parameter im Blockchain-Satz notiert und eine normale Signatur generiert. Die Kontrolle ist mit keinem zusätzlichen Aufwand verbunden.

Dieses Verfahren bietet sich an, wenn die Blockchain mehr oder weniger regelmäßigen Erweiterungen unterliegt. Entspricht die Taktzeit der Blockchainerweiterung der notwendigen Rechenzeit für die Berechnung von **nonce**, sind unerkannte Fälschungen im Prinzip nicht möglich.

Blinde Signaturen

Bei Artikeln zur Blockchain-Technologie taucht fallweise der Begriff „blinde Signatur“ auf, weshalb wir ihn hier berücksichtigen. Bei blinden Signaturen erstellt der Signaturgeber eine gültige Signatur, ohne Kenntnis des Hashwertes zu erlangen, den er verschlüsselt.

Hierzu wird der Hashwert vor Übergabe an den Signaturbeger durch eine Verknüpfung mit einer Zufallzahl unkenntlich gemacht:

```
blend = f(hash , decrypt(public_key , rand)) = f(hash , rand_blend)
```

Der Signaturgeber erstellt nun auf normale Weise eine Signatur **sig_blend,** wodurch der Hashwert verschlüsselt und die zuvor verschlüsselte Zufallzahl entschlüsselt wird:

```
sig_blend = encrypt(private_key , blend)
          = encrypt(private_key , f(hash , rand_blend)
          = f(sig , rand)
```

hash wird so in **sig** überführt, **rand_blend** in **rand**. Der Blockchain-Verwalter kann die Zufallzahl mit Hilfe einer Umkehrfunktion wieder herausrechnen:

```
sig = f⁻¹(sig_blend , rand)
```

Voraussetzung für den Einsatz ist natürlich, dass für ein asymmetrisches Verschlüsselungsverfahren ein Funktionspaar **(f , f⁻¹)** mit diesen Eigenschaften funktioniert. Das sieht zwar mathematisch recht exotisch aus, ist aber in Verfahrensvorschlägen für elektronische Wahlen über das Internet realisiert.

Im Notarverfahren ist durch den Austausch

```
hash( [N-1] | [N] | data)  ->  f( [N-1] , [N] , data)
```

eine Signatur blind erzeugbar, in Signaturen durch Arbeitsaufwand nicht, da ohne Kenntnis des Hashwertes **nonce** nicht berechnet werden kann.

Kryptowährungen

Am bekanntesten dürften Anwendungen der Blockchain-Technologie im Bereich der Kryptowährungen sein. Hier wiederum dürfte Bitcoin am bekanntesten sein, obwohl sich inzwischen die Anzahl der verschiedenen Varianten im höheren 2-stelligen Bereich bewegen dürfte. Alle Modelle ba-

sieren auf einer Blockchain, in der die Transaktionen verwaltet werden. Alle Modelle sind dezentralisiert und werden nicht von einer zentralen Instanz kontrolliert. Die Regeln sind so konstruiert, dass Unstimmigkeiten zwar nicht ausgeschlossen sind, aber bereinigt werden können, bevor irreparabler Schaden eintritt.

Beteiligte Parteien sind

a) die Teilnehmer, die in die Kryptowährung investieren oder über sie Tansaktionen mit anderen Teilnehmern abwickeln,

b) Broker, die die Blockchain verwalten und damit verbundene weitere Aufgaben abwickeln und

c) Signaturgeber, die gegen Lohn neue Signaturen zur Verlängerung der Blockchain erstellen.

Als Signaturverfahren kommen die Modelle „wechselnde Signaturgeber“ und „Signatur durch Arbeitsaufwand“ zum Einsatz. Wir beschränken uns hier auf das Modell „Signatur durch Arbeitsaufwand“, auf dem beispielsweise Bitcoin basiert.

Die Signaturfindung oder der Schürfprozess

Die Signaturermittlung wird „schürfen“ oder „mining“ genannt, die Signaturgeber „Miner“. Der Name Miner rührt daher, dass alle Mitglieder der Gruppe „Signaturgeber“ rechenintensiv nach einem passenden **nonce** suchen, aber nur der eine Prämie erhält, der als erster ein **nonce** findet. Das Durchsuchen eines großen Zahlenraums ähnelt gewissermaßen dem schürfen (mining) nach Gold, wobei der Schürfer (Miner) nur mit einer entsprechenden Portion Glück auch einmal ein Nugget findet.

Die Schürfmethode wird als die beste mögliche Prävention gegen Betrugsversuche betrachtet, da die Zykluszeit, in der neue Blockchainsätze erzeugt werden, mit der Zeit korrespondiert, die benötigt wird, das **nonce** der Signatur zu finden. Die Blockchain läuft daher einem Fälschungsversuch davon.

Prinzipiell kann jeder mitmachen: man muss sich nur bei den Koordinatoren (den Brokern oder Genossenschaften von Minern, die bei den Brokern registriert sind) registrieren, um die zu signierenden Sätze zu erhalten und, sofern man etwas findet, eine fertige Signatur zur Prüfung einzureichen zu können. Um allerdings Aussichten auf Erfolg zu haben, ist die Investition in spezielle Hardware notwendig, die in den kleineren Versionen auch für den privaten Miner erschwinglich ist. Die Miner-Community teilt sich in folgende Gruppen auf:

(a) Investoren mit größeren Serverfarmen, die auf professioneller Basis operieren.

(b) Genossenschaften privater Miner, in denen die Suchparameter aufeinander abgestimmt werden und deren individuelle Hardware virtuell zu Serverfarmen verbunden wird. Bei Erfolg kann je nach Geschäftsmodell die Prämie dem erfolgreichen Genossenschafter gut geschrieben werden (was die Erfolgschancen auf (c) begrenzt) oder sie wird auf alle aufgeteilt.

(c) Kleine, alleine operierende Miner mit entsprechend geringen Aussichten auf Erfolg.

(d) Miner ohne eigene Hardware, aber mit der Möglichkeit, auf Rechnern anderer Internetnutzern zu „parasitieren“. Auf diesen werden mit verschiedenen Methoden Mining-Scripte installiert, die positive Ergebnisse zurück senden.

    Die Effizienz ist natürlich sehr gering, d.h. es müssen schon recht viele Systeme „infiziert“ werden, um eine nennenswerte Rechenpower zusammen zu bekommen. Allerdings entstehen auch fast keine Kosten, so dass sich auch seltene Treffer auszahlen können. Die betroffenen Internetnutzer wissen in der Regel nichts vom Missbrauch ihrer Systeme und sind natürlich auch nicht an einem eventuellen Gewinn beteiligt.

Es wird zwar dafür geworben, sich am Mining zu beteiligen und dadurch Einnahmen zu generieren, was aber von einer Reihe von Parametern abhängt. Die Prämie besteht aus einer festgelegten Anzahl an Münzen (Coins, Einheiten der Krypowährung), die an den Finder des **nonce** ausgezahlt werden. Die Risiken bestehen in:

- Der reale Wert der Prämie richtet sich nach dem Zeitwert der Kryptowährung und kann stark schwanken. Unter Umständen erreicht man die Gewinnzone in Zeiten schwacher Kurse nicht.

- Die Wahrscheinlichkeit, die Prämie zu gewinnen, sinkt mit der Anzahl der Miner und deren Hardwarefähigkeiten und kann zu gering werden, um noch Profit zu generieren.

- Wechselnde Energiekosten beeinflussen das Betriebsergebnis. Steigen die Energiekosten, kann eine Teilnahme trotz akzeptabler Wahrscheinlichkeiten, die Prämie zu erhalten, zum Verlustgeschäft werden.

- Für den Einstieg sind (auch von privaten Minern) Investitionen in Hardware zu tätigen. Diese Investitionen müssen durch erhaltene Prämien erst einmal erwirtschaftet werden.

- Werden die Einnahmen aufgrund der Randbedingungen zu gering, können institutionelle Teilnehmer ihre Hardware mit einiger Wahrscheinlichkeit auch auf anderen Gebieten vermarkten (Server, KI, usw.). Betriebsergebnisse bewegen sich daher in der Regel in kalkulierbaren Grenzen.

  Für private Teilnehmer gibt es allerdings in der Regel keine sinnvollen anderen Einsatzgebiete der Spezialhardware im Privatbereich, da der Betrieb viel zu kostspielig ist. Investitionen sind daher mit der spekulativen Erwartungshaltung verbunden, dass man lange genug erfolgreich im System bleiben kann, um die Kosten zu erwirtschaften.

Einige Kryptowährungen wie Bitcoin sehen außerdem vor, die Regeln für die Miner zyklisch anzupassen (bei Bitcoin alle 4 Jahre). Dabei wird deren Aufgabe schwerer, indem das zu generierende Bitmuster komplizierter wird (z.B. mehr Nullbits) und noch mehr Rechenleistung erfordert, oder die Belohnung geringer, d.h. die Prämie in Form von Münzen sinkt (oder eine Kombination aus beidem).

Das kann zur Folge haben, dass einige Miner aussteigen (müssen), weil die Gruppe unter den neuen Bedingungen zu groß ist, um noch eine Kostendeckung zu erreichen. Zudem wird das Angebot an neuen Münzen kleiner, wenn die Prämie sinkt. Je nach Marktbedingungen kann das zu starken Kurssprüngen nach oben oder unten führen.

Die Münze oder Coin

Grundlage des Kryptowährungen ist eine elektronische Münze. Die Zahl der im Umlauf befindlichen Münzen ist begrenzt, steigt aber im Laufe der Zeit, da die Prämie für die Miner in neuen Münzen besteht. Die einzelnen Münzen können jedoch in so kleine Einheiten zerlegt werden, dass beliebige Beträge auch mit großen Teilnehmerzahlen abgewickelt werden können. Eine einzelne Münze kann sich dadurch auf sehr viele Inhaber verteilen. Im Weiteren werden wir der Einfachheit halber immer von Münzen sprechen, auch wenn wir nur Teile meinen.

Münzen haben ausschließlich einen positiven Wert und alle Münzen sind jeweils im Besitz eines bestimmten Teilnehmers, d.h. es existieren weder Kreditgeschäfte auf der Basis der Münzen noch existieren „herrenlose“ Münzen. Will man eine Münze erwerben, erfordert das, dass ein anderer Teilnehmer bereit ist, den gewünschten Anteil gegen einen ausgehandelten Betrag in realer Währung zu verkaufen; umgekehrt erfordert der Umtausch eine Münze in eine reale Währung einen interessierten Käufer. Der Wert einer Münze in einer realen Währung hängt daher wie bei Börsengeschäften ausschließlich von Angebot und Nachfrage ab.

> *Kreditgeschäfte sind somit nur in Verbindung mit einer realen Währung möglich. Man kann Münzen erwerben, wenn der vorherige Inhaber bereit ist, einen entsprechenden Kredit zu gewähren. In der Blockchain sind die wahren Eigentumsverhältnisse nicht erkennbar.*

Eine Kryptowährung kann in zwei Weisen genutzt werden:

(1) Vornahme von Zahlungen an andere Teilnehmer durch Übertragen des Besitzes einer entsprechenden Anzahl von Münzen.

(2) Kauf und Verkauf zu Spekulationswecken, ohne an andere etwas zu überweisen.

Dabei ist zu berücksichtigen, das die Miner ihre als Prämie erhaltenen Münzen zwangsläufig verkaufen müssen, da die Hardwarekosten und Kosten des Minings in realen Währungen zu bezahlen sind. Die Miner sind dabei den anderen Teilnehmern gleich gestellt: für die Konvertierung in reguläres Geld sind Interessenten für die Münzen notwendig. Ähnliches gilt für die Broker, da auch diese nicht unerhebliche Kosten haben.

> *Man kann natürlich annehmen, dass auch der Stromlieferant Münzen als Bezahlung akzeptiert. Der muss aber wiederum seine Lieferanten und seine Mitarbeiter bezahlen. Wie man es auch dreht oder wendet, irgendwann kommt man in der Kette nicht um eine Konvertierung der Münzen in reale Währungen herum.*

Die Broker

Die Korrektheit aller Transaktionsvorgänge wird durch die Blockchain gewährleistet, die bei Bitcoin derzeit eine Größe von ca. 600 GByte besitzt. Im Prinzip müsste jeder Teilnehmer diese Blockchain herunterladen, prüfen und nach jeder Transaktion weiterführen, sobald eine Signatur für den neuen Datenblock vorliegt. Bei Unstimmigkeiten (zwei Miner liefern mehr oder weniger gleichzeitig eine Signatur ab) ist ein demokratisches Abstimmungssystem vorgesehen, das bei sehr vielen Teilnehmern natürlich in der Praxis nicht machbar ist, zumal ja auch keine zentrale Instanz vorhanden ist, die die Kommunikation organisieren könnte.

Aus diesem Grund wird eine Gruppe von Brokern als Bindeglied zwischen den Nutzern und den Minern eingerichtet. Prinzipiell kann jeder Broker werden. Dazu ist nur eine Abstimmung mit den anderen Brokern notwendig. Die Broker stellen das eigentliche zentrale demokratische Entscheidungsgremium dar. Da die Aufgaben der Broker aber recht umfangreich sind und sie zur Deckung ihrer Kosten über eine genügend große Kundschaft (Nutzer oder Teilnehmer) und damit auch über entsprechende und wirtschaftliche Ressourcen verfügen müssen, bleibt die Zahl der Broker eines Kryptowährungssystems überschaubar.

Eine Transaktion gleich welcher Art erfordert zwei Zyklen der Blockchain. Der erste Zyklus beginnt mit der Arbeit der Miner an einer neuen Signatur und umfasst das Sammeln der Transaktionwünsche der Teilnehmer und deren Kontrolle. Liegt eine neue Signatur vor, die von allen Brokern akzeptiert wird, beginnt der zweite Zyklus mit der erneuten Arbeit der Miner am abgestimmten nächsten Satz der Blockchain und endet mit der neuen Signatur und der Aufnahme des signierten Satzes in die Blockchain, mit der die Transaktionen ausgeführt sind. Die Aufgabe der Broker besteht

(a) in einer Kontrolle der Korrektheit der Transaktionsmeldungen im ersten Zyklus (die notwendige Anzahl von Münzen muss im Besitz des Teilnehmers sein und dieser darf nicht versuchen, die gleiche Münze mehrfach einzusetzen),

(b) in der Kontrolle, dass im ersten Zyklus eingesetzte Münzen nicht erneut verwendet werden, bevor die Transaktion mit dem Ende des zweiten Zyklus abgeschlossen ist.

Vorgesehen ist bei Bitcoin eine Zykluszeit von ca. 10 Min., d.h. nach spätestens 20 Min. sollte eine Transaktion bestätigt abgewickelt sein. Bei hohem Transaktionsaufkommen kann aber auch schon einmal 1 h oder mehr dabei herauskommen. Der notwendige Kontroll- und Abstimmungsaufwand der Broker und einige andere Regeln begrenzen die Anzahl der Transaktionen, die in einem Zyklus bearbeitet werden können oder dürfen.

Um als privater Teilnehmer die Kryptowährung benutzen zu können benötigt man ein Konto bei einem Broker, eine so genannte Wallet. Die Einrichtung kann anonym oder zumindest anonymisiert erfolgen. Die Wallet besteht aus einem Zertifikat mit öffentlichem Schlüssel und alle Transaktionen werden mit dem privaten Schlüssel des Zertifikats, den nur der Teilnehmer kennt, signiert. Geht dieser Schlüssel verloren, kommt der Teilnehmer nicht mehr an seine Guthaben heran. Umgekehrt kann jeder, der in den Besitz des privaten Schlüssels gelangt, den Wert der Wallet auslesen und über Guthaben verfügen, ohne sich anders ausweisen zu müssen. Die Wallet wird darüber hinaus vom Broker signiert und kann daher nur über ihn verwendet werden. Eine Nutzung bei einem anderen Broker ist aus Sicherheitsgründen (Mehrfachnutzung einer Münze) nicht möglich.

Der Erwerb von Münzen erfolgt über den Broker. Dazu überweist der Teilnehmer einen entsprechenden Betrag in einer realen Währung auf ein Bankkonto des Brokers, der zu einem zwischen allen Brokern festgelegten Kurs, der auf der Auswertung von Angebot und Nachfrage beruht, eine Transaktion von einem oder mehreren Verkaufswilligen in den nächsten Datenblock aufnimmt und nach Aufnahme in die Blockchain den Betrag abzüglich seiner Gebühren ebenfalls auf dem Bankweg an die Verkäufer auszahlt.

> *Der Broker geht dabei keine Risiken ein, da keine Kreditgeschäfte auf Blockchainebene möglich sind. Er kann natürlich auf eigene Rechnung Münzen kaufen und bevorraten und daraus Verkäufe auch auf Kredit tätigen und trägt dann Kurs- und andere Risiken selbst. Möglich ist natürlich auch, dass die Kaufwünsche bei einem Broker nur durch Verkaufswünsche bei einem anderen befriedigt werden können. Wie die Broker dies untereinander abwickeln, ist aber deren Sache.*

Die Anonymität der Wallet war (und ist) ein Argument von Leuten, die auf ihre Privatsphäre wert legen, für die Nutzung von Kryptowährungen. Unter Berücksichtigung der Kosten aber eine recht kostspielige Absicherung der Privatsphäre.

> *Tatsächlich ist die Anonymität nur bedingt gegeben: Staaten können die Broker verpflichten, Wallets nur gegen einen Identitätsnachweis einzurichten. Und selbst wenn sie darauf verzichten, ist über Ein- und Auszahlungen bei den Brokern der Zahlungsfluss und die dabei Beteiligten rekonstruierbar.*

Das vom Broker geführte Wallet-Konto ist eine nutzerspezifische Bilanz der Blockchain. Eingetragen werden alle Münzen, deren Inhaber der Nutzer in einer Transaktion geworden ist. Nur diese Münzen kann er in einer eigenen Transaktion verwenden. Inhaber einer Münze wird er, indem seine Wallet in einer vom vorhergehenden Inhaber signierten Transaktion als Empfänger eingetragen ist. Setzt er diese Münze in einer Transaktion mit seiner Wallet als Absender ein und signiert die Transaktion, geht der Besitz auf einen anderen Empfänger über und die Münze wird aus dem Wallet-Konto gelöscht. Eine Münze kann also nur in der Form in einer Transaktion eingesetzt werden, in der sie eingenommen wurde.

Diese Vorgehensweise ist notwendig, um innerhalb der Blockchain auf einfache Weise die Kontrolle zu behalten, dass jeder Teilnehmer nur die Münzen ausgeben kann, die er auch bekommen hat. Da der Wert aber selten demjenigen entsprechen dürfte, der in einer Transaktion überwiesen werden soll, sind weitere Mechanismen notwendig, die von den Brokern abgewickelt werden müssen.

Das Transaktionsschema

Das hier vorgestellte Schema hat Modellcharakter; wie die Einzelheiten in verschiedenen Kryptowährungen konkret gelöst sind, ist der jeweiligen Dokumentation zu entnehmen.

Ein Blockchain-Satz besteht aus einer zwischen den Brokern abgestimmten Menge von Transaktionssätzen. Er wird von einem Miner signiert wird, wobei die Prämie für eine gültige Signatur ebenfalls in Form einer Transaktion erfasst ist.

```
BlockChainSet ::= SEQUENCE {
      SEQUENCE {
            transactionSets   SEQUENCE OF TansactionSet,
            reward            Transaction,
            nonce             IA5string
      }
      sig               Signature         // des Miners
}
```

Die Transaktion ist eine Überweisung der festgelegten Anzahl von Münzen des Miners an sich selbst, signiert mit seiner Wallet. Mit der Aufnahme des Datensatzes in die Blockchain durch die Broker geht sie in seinen Besitz über und kann von ihm verwendet werden.

Liegen mehrere konkurrierende Signaturen vor, müssen sich die Broker auf eine einigen, bevor ein Miner versucht, seine Münze in eine Realwährung zu konvertieren.

Da eine Münze nur in der Form eingesetzt werden kann, in der sie erhalten wurde, ist eine Transaktion eine komplexe Angelegenheit. Der Wert einer Münze eines Absenders dürfte in den seltensten Fällen dem Wert entsprechen, den der Empfänger bekommen soll, außerdem stehen dem Broker für seine Tätigkeit Gebühren zu, die er ebenfalls in Form einer Transaktion erhält. Das erfordert einen ganzen Satz an Einzeltransaktionen. Der Transaktionssatz eines Teilnehmers besteht daher aus zwei Mengen von Transaktionen, die der Broker signiert, nachdem er alles auf Korrektheit kontrolliert hat.

```
TransactionSet ::= SEQUENCE {
      SEQUENCE {
            credit  SEQUENCE OF Transaction,
            debit   SEQUENCE OF Transaction
      }
      sig     Signature              // des Brokers
}
```

Die Einzeltransaktionen haben die Struktur

```
Transaction  ::= SEQUENCE
      SEQUENCE {
            coin        Coin,
            recipient   Certificate // „Wallet“
      }
      sig         Signature         // des Absenders
}
```

Ein Teilnehmer wird Inhaber einer Münze, wenn seine Wallet im **recipient**-Feld eines gültigen **debi**t-Transaktionssatzes steht. und der vorherige Inhaber (Wallet **payer**) die Transaktion signiert hat. Genau diese Münze kann er in einen **credit**-Satz eintragen und mit seiner Wallet signieren.

Block	Sequence	Coin	Signatur	Recipient
105 (alt)	debit	4711.0040	Wallet old	Wallet
Neu	credit	4711.0040	Wallet	----
- Signaturzyklus -				

126	**credit**	**4711.0040**	**Wallet**	**-----**

Im Beispiel hat der Teilnehmer in Blockchain-Satz 105 die Münze 4711.0040 übertragen bekommen und setzt sie nun in einem neuen Transaktionssatz ein. Wird dieser signiert, ist sie „verbraucht“, d.h. in einer weiteren Transaktion wird der Broker die Münze nicht akzeptieren, wenn der Teilnehmer versuchen sollte, sie noch einmal zu verwenden.

Formal sieht es kompliziert aus, in einer großen Blockchain mit vielen Transaktionsätzen zu überprüfen ob ein Teilnehmer eine bestimmte Münze besitzt und sie auch noch nicht wieder eingesetzt hat. Das ist aber nur im Notfall oder wenn neuer Broker hinzukommt zu prüfen. Münze und Wallet bilden einen eindeutigen Datenbankschlüssel, so dass bei Besitzübergabe lediglich ein Schlüssel gelöscht und ein anderer eingetragen wird. Ist kein Schlüssel vorhanden, gehört dem Teilnehmer die Münze auch nicht.

In der **credit**-Menge werden alle Münzen erfasst, die in der Gesamttransaktion verwendet werden. Sie werden vollständig auf die **debit**-Sätze aufgeteilt, wobei nun neue Stückelungen auftreten können. Das lässt sich am Einfachsten an einem Beispiel erläutern:

*Nehmen wir an, der Inhaber von Wallet A möchte 0060 Teileinheiten ganzer Münzen an den Inhaber von Wallet B übverweisen. Zuzüglich fällt eine Gebühr von 0001 Einheiten für den Broker an. Um diese Einheiten abzudecken, muss er aus seinem Besitz Münzen im Wert von 107 Einheiten einsetzen, die im **credit**-Satz enthalten sind.*

Credit	**4711.0040**	
	4711.0017	
	4813.0050	
Debit	**4711.0057**	**Wallet B**
	4813.0003	**Wallet B**
	4813.0001	**Broker**
	4813.0046	**Wallet A**

*Im **debit**-Satz kann er 0057 Einheiten der vorher in die Teile 0040 und 0017 gestückelten Münze mit der Seriennummer 4711 wieder zusammen setzen und an B übertragen. Weitere 0003 Einheiten muss er durch Stückelung von Münze 4813 zusätzlich bereit stellen, um den vereinbarten Gesamtbetrag von 0060 Einheiten zu erhalten. Eine weitere Stückelung von 0001 Einheiten gehen als Gebühr an den Broker und die restlichen 0046 Einheiten erhält er schließlich als „Wechselgeld“ durch eine Überweisung an sich selbst wieder zurüc, so dass die Gesamtbilanz ausgeglichen ist.*

Diese Verteilungen vorzunehmen ist Aufgabe des Brokers, der prüfen muss, ob es sich um unverbrauchte Münzen handelt und diese in einem weiteren Transaktionssatz nicht nochmals auftauchen. Das so gebildeten **TransactionSet** wird an alle anderen Broker verteilt, die ebenfalls die Prüfungen vornehmen.

Nach vereinbarten Regeln wird aus den Transaktionssätzen aller Broker der neue Blockchainsatz von allen gebildet (für die Berechnung des Hashwertes ist notwendig, dass bei allen Brokern alle Sätze in der gleichen Reihenfolge auftreten) und in einem Zustimmungsverfahren sicher gestellt, dass alle über den gleichen Satz verfügen. Dieser wird dann den Minern zum Signieren überlassen.

Aus dem beschriebenen Verfahren wird auch verständlich, dass eine Wallet an einen Broker gebunden ist und nur dieser die Münzen in neuen Transaktionen einsetzen darf, weil der gleichzeitige Einsatz einer Münze bei verschiedenen Brokern kaum kontrollierbar ist. Das schließt aber nicht aus, dass auch Verfahren existieren, deren Regeln das Problem nicht auftreten lassen.

Teilnehmer oder Kontoinhaber?

Jede Kryptowährung besitzt natürlich ihre eigenen Varianten der Strukturen und Buchführung, die möglicherweise nicht unerheblich von den beschriebenen Mechanismen abweichen können. Broker können abweichend vom beschriebenen Schema die Teilnehmer-Wallet auch als reines Teilnehmerkonto führen, d..h. der private Schlüssel fungiert lediglich als Identitätsnachweis des Teilnehmers und die Transaktionen in der Blockchain werden ausschließlich vom Broker signiert. Für den Broker ist eine solche Kontenführung einfacher, hat aber Konsequenzen im Falle einer Insolvenz des Brokers, was in der Praxis auch schon aufgetreten ist:

- Wird in der Blockchain die Wallet-Signatur des Teilnehmers verwendet, ist er der Inhaber der Münzen und vom Konkurs nicht betroffen. Ein anderer Broker kann die Münzen auf eine neue Wallet transferieren, ohne dass es zu Verlusten außer kleineren Gebühren kommt.

- Enthält die Blockchain die Signatur des Brokers, ist er Inhaber der Münzen und bei einer Insolvenz können sich die Gläubiger bedienen. Der eigentliche Inhaber geht möglicherweise leer aus.

Blockaufspaltungen

Unter bestimmten Umständen kann sich die Einigung der Broker auf den neuen obersten Satz der Blockchain verzögern, so dass es zu einer Aufspaltung kommt, wenn bereits ein weiterer Datensatz an die Miner übergeben wurde. In Bitcoin ist dieser Fall letztmalig 2019 aufgetreten.

Block A , Signatur 0	
Block B , Signatur 1	Block B , Signatur 2
Block C , Signatur X	Block D , Signatur Y

Ein Teil der Broker hält den linken Zweig für den korrekten, ein anderer den rechten, und je nachdem, von wem die Miner ihre Informationen erhalten, erzeugen sie die Signaturen X oder Y für den Folgesatz. In solchen Fällen ist ein Mehrheitsentscheid der Broker vorgesehen. Stimmen mehr Broker für den linken Zweig, ist dieser für alle verbindlich. Die Abstimmung sollte abgeschlossen sein, bevor die Signaturen X und Y vorliegen.

Die Aufspaltung ist völlig unkritisch, wenn

Block C = Block D

gilt. Einigt man sich auf Signatur 1, so ist auch Signatur X gültig und alle Transaktionen sind korrekt erfasst. Der zweite Zweig wird gelöscht und lediglich Miner 2 und Miner Y gehen leer aus und sind sauer.

Ist hingegen auch

Block C ≠ Block D

gehen zwar wieder Miner 2 und Miner Y leer aus, das Aufräumen ist aber wesentlich aufwendiger, da nun überprüft werden muss, welche Transaktionen aus Block D bereits in Block C vorhanden sind und welche wiederholt werden müssen.

Kritisch wird es allerdings, wenn keine Einigung erzielt und auch Signatur X und Signatur Y von jeweils einer Brokergruppe anerkannt wird. Enthalten die Blöcke C und D Konvertierungen von Münzen in reales Geld, das mit Anerkennung der Signatur ausgezahlt wird, lässt sich das kaum noch reparieren. Solche Fälle sind aufgrund fehlender Regeln, die Blockchainbildung unter bestimmten Bedingungen anzuhalten, in der Anfangszeit der Kryptowährungen auch aufgetreten und haben zur dauerhaften Aufspaltung in mehrere Teilketten geführt – und wegen des daraus resultierenden Vertrauensverlustes zu einem baldigen Ende.

Eine Aufspaltung ist bei Einhaltung bestimmter Regeln formal unkritisch, kann aber aufgrund der auftretenden Kosten für alle Teilnehmer trotzdem unangenehm werden.

Kryptowährungen ./. reale Währungen

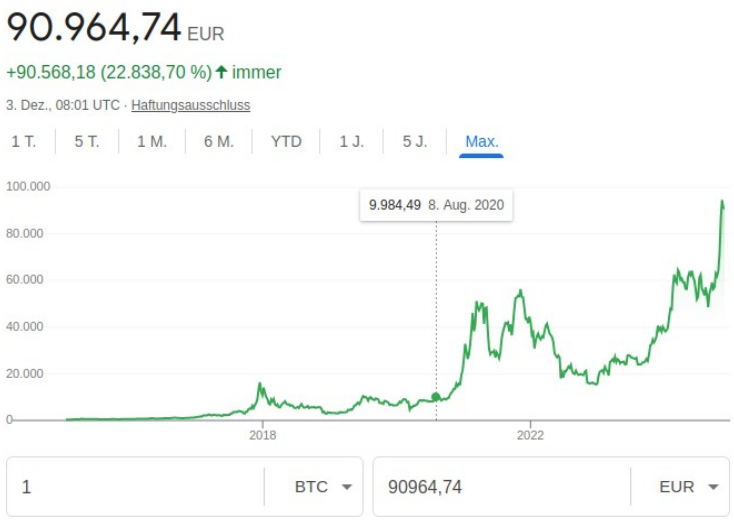
Beginnen wir mit ein paar Zahlen zu Bitcoin. Im Jahr 2024 wurden ca. 1,3 Mrd. Transaktionen abgewickelt. Im Umlauf sind ca. 18,4 Mio. ganze Münzen, die jeweils in 100.000.000 kleinere Einheiten (Satoshis) zerlegt werden können, um beliebigen Beträge abbilden zu können. Bei einem aktuellen Kurs von ca. 91.000 € / Coin sind ca. 1,7 Billionen € im Jackpot.

Der Aufwand, der beim Mining getrieben wird, ist immens: die derzeit weltweit aufgewandte Menge an elektrischer Arbeit für den Schürfvorgang bei Bitcoin liegt mit geschätzt 90 TWh höher als der Gesamtbedarf eines Landes wie der Schweiz mit 57 TWh. Die weltweit günstigsten Stromkosten liegen bei ca. 9 ct / kWh, was zu Kosten von ca. 5 Mrd. € führt; bei einem mittleren Welt-Strompreis von 14 ct / kWh macht das 7,8 Mrd. € aus, beim landesüblichen Preis von 23 ct /kWh in Deutschland 12,8 Mrd. €. Da die großen gewerblichen Miner in Ländern mit niedrigen Strompreisen ansiedeln, dürften Kosten von ca. 6 Mrd. € oder ca. 3,5 ‰ des aktuellen Gesamtwertes realistisch sein.

Durch das Mining wurden im Jahr 2024 ca. 200.000 neue Münzen geschaffen, was nach aktuellem Kurs ca. 18 Mrd. € entspricht. Das Mining lohnt sich folglich: pro eingesetztem Euro können bis zu 3 € Einnahmen erzielt werden. Aufgrund der im Abschnitt „Die Signaturfindung oder der Schürfprozess“ erwähnten Regeln sinkt die Quote allerdings. Allerdings hat die Sache einen Pferdefuss: der Kurs einer Münze hängt ausschließlich von Angebot und Nachfrage ab und die 18 Mrd. € sind –

als reales Geld betrachtet – nur realisierbar, wenn sich Teilnehmer finden, die ihrerseits 18 Mrd. € in Bitcoin investieren und das Geld dort lassen. Finden die sich nicht, sinkt der Kurs.

Schaut man sich die Kursentwicklung an, finden sich derzeit genügend „Investoren“ und der Kurs steigt. Zwischendurch gibt es aber auch stärkere Abstürze. Solches Kursverhalten führt speziell bei stark steigenden Kursen zu Spekulationen: die Bitcoins werden gehalten und weitere Teilnehmer stoßen hinzu, weil sie sich Gewinn versprechen. Von den im Umlauf befindlichen Münzen haben



nach Auswertung der Blockchain ca. 63% innerhalb eines Jahres nicht mehr an Transaktionen teilgenommen, was auf die Größe des spekulativ gehaltenen Anteils hinweist.

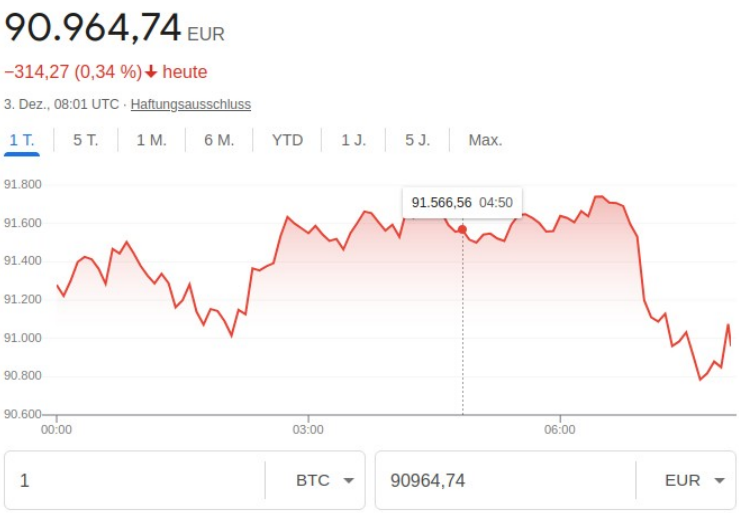
Bereits eine Werterhaltung der Bitcoins setzt somit voraus, dass neue Teilnehmer auf Dauer hinzugewonnen werden, eine „Rendite“ zusätzliche Teilnehmer, die auf einen anscheinend Erfolg versprechenden Zug aufspringen. Schaut man sich die Kurve an, so hat die Überzeichnung der neuen Münzen zu einem 2,5-fach höherem Kurs geführt. Mitte 2024, als Angebot und Nachfrage nach neuen Münzen etwa ausgeglichen war, blieb der Kurs konstant. Eine Rendite durch Erhöhung der Anzahl der Teilnehmer ist aber ein charakteristisches Merkmal eines Ponzi-Schemas oder Schneeballsystems, was „Investmentberater“ aber vehement abstreiten, weil die Betrugsabsicht fehlt. Fehlt die wirklich?

Drehen wir die Sicht einmal um: die neuen Münzen machen ca. 1% aller Münzen aus, führen aber zu Kursschwankungen von 250% bei Überzeichnung. Umgekehrt muss man also davon ausgehen, dass schon wenige Teilnehmer genügen, den Kurs massiv abstürzen zu lassen, wenn sie versuchen, ihre „Rendite“ zu realisieren, d.h. den Gewinn in realer Währung abzuziehen. Wenn dann noch Panikverkäufe hinzukommen … Da Bitcoin nicht reguliert ist, besteht für Spekulanten durchaus die Möglichkeit, mit relativ kleinem Einsatz den Kurs in irgendeiner Richtung zu manipulieren und große Gewinnen einzufahren. Fehlen Betrugsmöglichkeiten wirklich?

Halten wir fest: Investitionen in Bitcoin und verwandte Kryptowährungen sind hochspekulativ und Gewinne davon abhängig, dass weitere Teilnehmer rekrutiert werden können, während echte Werte in Form von Waren nicht generiert werden.

Zudem kann das System auch bei relativ hohen Kursen zusammen brechen. Können die Miner ihre Kosten nicht mehr erwirtschaften, weil ihre Münzen nicht mehr zu den notwendigen Preisen verkauft werden können, werden viele Miner aussteigen, was dazu führen kann, dass die Transaktionszeiten sehr viel länger werden oder die Blockchain komplett zum Stillstand kommt, was den Totalverlust für die Teilnehmer bedeutet.

Die Kryptowährungen wurden ursprünglich nicht zu spekulativen Zwecken, sondern als Möglichkeit angepriesen, weltweit anonym Geschäfte nach dem Muster von Bargeldgeschäften abzuwickeln. Für den normalen Teilnehmer kommen dabei Gebühren von ca. 30 ct / Transaktionssatz und je nach Marktlage 0,5% - 3% für die Konvertierung in reale Währungen hinzu.



Als weiteres Risiko kommen die Kursschwankungen hinzu, die selbst auf Tagesbasis schon 1% - 2% betragen können. Im Graubereich spielt dies für die Abwicklung von Erpressungszahlungen, Schutzgeldern oder Geldwäsche keine Rolle. Und eine international aufgestellte Kryptowährung bietet auch genügend Möglichkeiten, solche Geschäfte anonym abwickeln zu können. Für Teilnehmer, die Geldtransfers in Länder vornehmen wollen, die mit der Hausbank nicht möglich sind, sind die Risiken eher auch kein Problem, da es sich um Rein-Raus-Geschäfte handelt, d.h. das was eingezahlt wird, wird auf der anderen Seite abgehoben, sobald es da ist. Unter welchen Rahmenbedingungen so etwas für den Geschäftsverkehr in Frage kommt, ist aber gut abzuwägen.

Diese Diskussion wurde am Beispiel Bitcoin geführt, die immer noch der Marktführer der Kryptowährungen ist. Vieles hier gesagte trifft auch auf andere Kryptosysteme zu. Wer sich für eine bestimmte interessiert, kann sich anhand der hier genannten Kriterien kritisch in sie einarbeiten. Manche versprechen, für bestimmte Schwächen weniger anfällig zu sein, was aber überprüft werden sollte. Verkaufstechnisch wird oft etwas anderes angeboten, als in der Packung drin ist, denn der Verkäufer will ja auch Geld verdienen.

Abschließend sei auf den Widersinn verwiesen, einerseits das Mining als sicherste Methoden anzupreisen, eine Blockchain und damit auch den Besitz der Teilnehmer gegen Fälschungen und Unfälle abzusichern, andererseits bereits vorschreiben zu wollen, was aufgrund des angeblichen Klimawandels und der damit verbundenen CO_2 – Einsparung um jeden Preis noch auf den Mittagstisch gebracht werden darf. Denn Mining ist letztlich nichts anderes als das Verbraten extremer Energiemengen im wahrsten Sinne des Wortes für Nichts, und so lange der Strom nicht durchgehend aus Kernenergie kommt …

Kryptowährungen und gestörte Finanzflüsse

Auch wenn das letzte Kapitel mit der Warnung endet, man solle sich genau überlegen, ob und für was man in eine Kryptowährung einsteigt, könnte es Gründe geben, ihren Einsatz zu verbreitern, auch geschäftlich.

Das globale reguläre Finanzsystem ist in einem hohen Maße vom US-$ abhängig und die USA vom weiteren Bestand dieser Abhängigkeit. Im Grunde sind die USA hoffnungslos überschuldet und andere Länder haben technisch aufgeholt und werden weniger abhängig. Um trotzdem ihre bisherige Hegemonie zu wahren, setzen die USA zunehmend auf offene Erpressung, angeführt vom weiter zunehmenden Abschneiden Russlands und anderer Länder von internationalen Finanzströmen. Das geht so weit, dass die Volkswirtschaften der engsten Verbündeten, den EU-Ländern, brutal stranguliert werden, was die aber leider fast mit Begeisterung über sich ergehen lassen.

Derzeit ist es nicht möglich, reales Geld offiziell nach Russland zu transferieren. International aufgestellte Kryptowährungen wie etwas Bitcoin schon, denn dass sich russische Miner und Broker an der Sache beteiligen, können selbst die USA anscheinend nicht verhindern. Grundsätzlich besteht also die Möglichkeit, dass Teilnehmer A in einem EU-Land beim ortsansässigen Broker Münzen kauft, diese nach Russland transferiert und Teilnehmer B sie bei seinem Broker, der natürlich in Russland residieren muss, wieder in Rubel umtauscht.

Das könnte zu Problemen führen, wenn es bei diesem einseitigen Fluss von West nach Ost bleibt. Der Käufer könnte nach einiger Zeit feststellen, dass auf seiner Seite des Vorhangs zu wenig Münzen zum Verkauf angeboten werden, der Verkäufer wiederum, dass auf seiner Seite kein Geld für seine Münzen angeboten wird und er sie nicht mehr los wird, denn die Broker sind ja auch nicht mehr in der Lage, Käufe und Verkäufe untereinander in realen Währungen abzuwickeln. Verbergen sich hinter den Teilnehmern Unternehmen und größere Beträge, geht das noch schneller.

Trotzdem sieht die russische Regierung hier anscheinend eine Möglichkeit, die USA auszutricksen. Der Grundgedanke dabei ist vermutlich, dass Wirtschaftsunternehmen mehr an profitablen Geschäften interessiert sind als an der Befolgung ideologischer Verbote und so auch Möglichkeiten finden, den ebenfalls sanktionierten Warenverkehr auf vielerlei Umwegen aufrecht zu erhalten, wenn auch auf vielleicht auf einem niedrigeren Niveau.

Hier könnte der Staat eine aktive Rolle übernehmen, auch den parallelen Kapitalfluss in Gang zu halten. Liefert Unternehmen A etwas in die EU und erhält dafür in Russland nicht konvertierbare Bitcoins, können damit auch Lieferungen aus China für Unternehmen B bezahlt werden, während B seinerseits A in Rubel auszahlt. In China wiederum gibt es keine Probleme, die Bitcoins wieder zu konvertieren, da dort keine Sanktionen bestehen. Das ein wenig weiter ausgewalzt mit ein paar weiteren Transfers, um den Geld- vom Warenfluss zu trennen, dürfte auch das US-Finanzministerium wenig Möglichkeiten habe, etwas zu sanktionieren.

Die Rolle des Staates (oder der Staaten, wenn das funktioniert und Schule macht) dürfte darin bestehen,

- Geschäfte auf Geld- und Kryptoebene zu koordinieren,
- durch eigene Systembeteiligung an der Kryptowährung extreme Kursschwankungen abzufangen und
- durch Diversifizierung in einem Mix verschiedener Kryptowährungen die Risiken weiter zu senken.

Man kann zwar davon ausgehen, dass die Sache ein paar Milliarden an Kosten verursachen wird, was aber im Vergleich zum Brechen der US-Epressungen eine gute Investition ist, zumal sich viele Staaten anschließen werden, wenn es funktioniert.