Fragenstellungen:

Dezentralisierung:   
a) dezentrales Bezahlen  
Wie könnte ein dezentraler Bezahlmechanismus zB für Straßenmaut oder Stromtanken funktionieren, also in dem zB eine gewisser Geldbetrag im Auto verfügbar ist, von dem an verschiedenen Stationen ein entsprechender Teilbetrag automatisch abgebucht wird, ohne dass der Fahrer jedesmal zahlen muss (Internet of Things Bezahlung, wo die Maschinen also zB Auto und Mautsensor, die Bezahlung automatisch untereinander machen). Das sollte auch funktionieren, wenn es verschiedene Betreiber der Mautstellen oder der Stromtankstellen gibt, ohne dass man für jeden eine eigene Abrechnungskarte benötigt: IOTA ist darauf ausgelegt.

b) Was ist das Web of Trusts? Könnte man sowas auch für den dezentralen Austausch von Informationen verwenden

## IOTA

IOTA ist ein Konzept für den Austausch von Werten (der Wert wird als „Währung“ IOTA genannt) zwischen Teilnehmern im Internet of Things.

Ein Austausch ist eine Transaktion (Teilnehmer x gibt an Teilnehmer y den Wert z)  
Wobei eine Transaktion bestätigt oder nicht bestätigt (tips) sein kann. Eine neue Transaktion enthält aber nicht nur Info darüber wer wem wieviel gibt, sie muss auch 2 andere Tips bestätigen. Dadurch entstehen jeweils 2 Graphen, die eine Transaktion mit 2 vorhergehenden verbindet. Die Graphen bilden ein Netz, das in der IOTA Terminologie Tangle (=Wirrwarr oder so) genannt wird. Ganz links ist der Ursprung (genesis), also die erste Transaktion des ganzen Tangles.

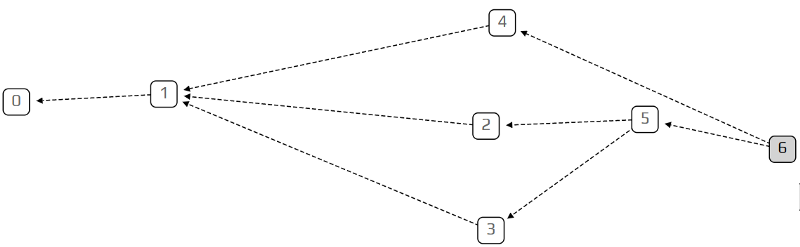


Abbildung: IOTA Tangle,   
Quelle https://blog.iota.org/the-tangle-an-illustrated-introduction-4d5eae6fe8d4

Welche tips für die Bestätigung ausgewählt werden, ist Teil des Konzeptes von IOTA, Statt zufällige Tips zu nehmen, werden schlaue Algorithmen aus der Graphenthoerie gewählt um passende Tips auszuwählen. Dadurch wird das System zuverlässiger und perofrmanter.

Als Spamschutz wird, bevor eine Transaktion in den Tangle gesendet wird, eine Proof of Work Rechenaufgabe gelöst, die eine bestimmte Zeit benötigt. Das wird gemacht, damit Hacker den Tangle nicht mit sinnlosen Transaktionen fluten können, um das auszunutzen.

Transaktionen werden aber nicht unbedingt vom Beutzer selber erledigt, sondern an sogenannte nodes übergeben, die dazu eine passende Software installiert haben.

Beim Bestätigen wird die Plausibilität der Transaktion geprüft (zB ob es wohl kein double spending gibt) und der Hash der Transaktionsinformationen mit dem private key eines Benutzers signiert. Das private-public Schlüsselpaar wird beim Erzeugen der wallet (also der digitalen Brieftasche) erzeugt und gehört somit genau zum Besitzer der Brieftasche.

Eigenheiten von IOTA:

Skaliert angeblich unendlich und wird sogar schneller je mehr Teilnehmer den Tangle benutzen.

Ist Quantencomputer sicher, weil es einen speziellen Hash-Algorithmus verwendet, den auch Quantencomputer nicht in vernünftier Zeit knacken können.

Es fallen keine Transaktionsgebühren an, weil es kein minen wie beim Bitcoin, gibt

Speichert Daten in einem ternären Zahlenysystem (nicht Binär)

Kann schlank bleiben, weil bestätigte vollständige Transaktionen, bei denen das ganze Geld verbraucht wurde, entfernt werden können.

Teil-Tangles können unabhängig (also ohne Netzwerkanbindung zum Haupttangle) arbeiten und dann wieder eingebunden werden.

Fortsetzung folgt…

# Zusatzfrage Web of Trusts

Das Web of Trust (WOT) ist in der Kryptologie die Idee, die Echtheit von digitalen Schlüsseln durch ein Netz von gegenseitigen Bestätigungen (Signaturen), kombiniert mit dem individuell zugewiesenen Vertrauen in die Bestätigungen der anderen („Owner Trust“), zu sichern. Es stellt eine dezentrale Alternative zum hierarchischen System dar, bei dem Zertifizierungsauthorities die Echtheit von Zertifikaten bestätigen (wie es zB bei https derzeit üblich ist)

Warum braucht man das überhaupt:  
Weil bei dem public-private-key Verfahren sichergestellt sein muss, dass der public key, den man verwendet, um Daten verschlüsselt an den zugehörigen Empfänger zu senden, auch wirklich dem Empfänger gehört. Sonst könnte sich ja jemand als Empfänger ausgeben und einen falschen public key veröffentlichen (zB beim man in the middle und certficate spoofing). Bei https kann man das Zertifikat überprüfen, in dem man es mit dem public key der Zertifizierungsauthorität (CA) testet. Der CA muss man also bedingungslos vertrauen.

## Vorgang beim web of trusts

1. Es gibt key-Server auf denen die public keys der Teilnehmer abgelegt werden
2. Ein Teilnehmer A kann einen public key eines anderen Teilnehmers B, den er vertraut, signieren. Signieren heißt, dass er eine Klartextinfo der Art  
   *Ich A vertraue dem key von B, der so lautet:   
   hier steht dann der public key von B*  
   mit seinem private key verschlüsselt, das Ergebnis der Verschlüsselung an die Klartextnachricht dazuhängt (signiert) und Ganze wieder am key-Server veröffentlicht.  
   Jeder kann testen, ob das passt, in dem er die Nachricht mit dem public key von A entschlüsselt und mit der Klartextnachricht vergleicht. Wenn es passt, weiß er zumindest, dass A B vertraut und dass der publick key von B (aus Sicht von A) richtig ist.
3. Sollte B also irgendwo einem anderen Teilnehmer C vertrauen, würde er seinerseits den public key von C signieren und somit sagen: ich vertraue C
4. Daraus ergibt sich aber, dass A auch den public key von C als gültig ansieht (A vertraut ja den Signaturen von B) es heißt aber nicht, dass A C vertraut, nur der Schlüssel von am Keyserver ist ok. Wenn A C vertraut, muss er den Schlüssel von signieren, so wie er es bei B gemacht hat.

Im Endeffekt ergibt sich, dass ein Teilnehmer alle Schlüssel als gültig ansieht, die von jemanden signiert wurden, dem er vertraut. So gesehen gibt es nicht mehr eine CA sondern viele, mit gegenseitigen Vertrauensstellungen, eben ein Web of Trusts (WoT).  
Wie das jeweilige Vertrauen zustande kommt, ist egal (zB persönlicher Kontakt, auf alternativem Weg verfizierte emails, oder was auch immer), aber man vertraut darauf, dass der Besitzer eines Schlüssels seinerseits nur sorgfältige Schlüsselsignaturen vornimmt, dass also die mit der Signatur zum Ausdruck gebrachte Behauptung desjenigen, dass ein bestimmter Schlüssel zu einer bestimmten Person gehört, verlässlich ist. Dieses Vertrauen wird „Owner Trust“ genannt.

Man kann natürlich jeden Schlüssel am key-Server als gültig ansehen, auch wenn er von Teilnehmern signeirt wurde, denen ich nicht vertraue oder die man nicht kennt. Ein Kriterium wäre zB, dass er von genügend Teilnehmern signiert wurde.