Slide 1

ETH zürich

Grundlagen der Blockchain

Benno Luthiger (ID ETH Zürich), OBL /ch/open, 5. Okt. 2017

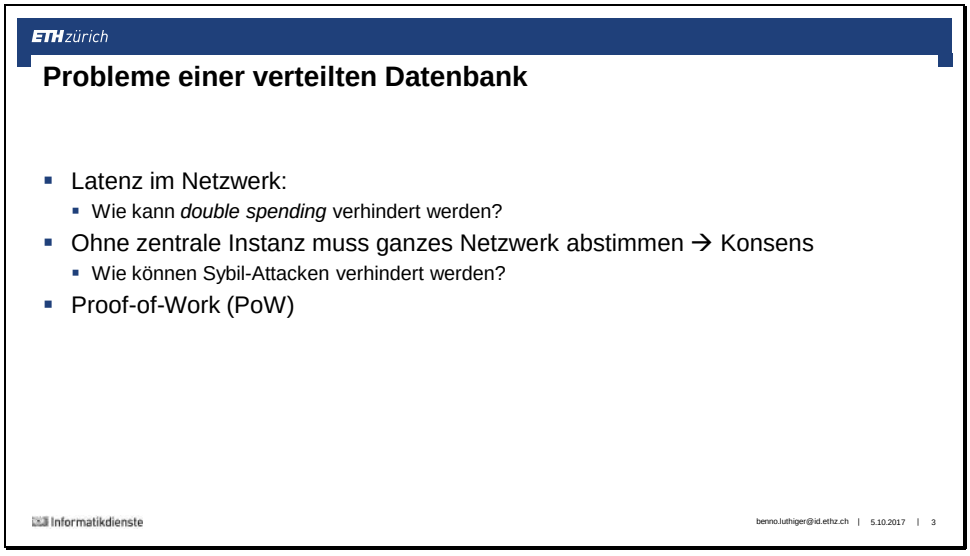
Slide 2

Was ist interessant an Bitcoin?
Bitcoin ist schnell und zuverlässig und funktioniert ohne zentrale Autorität. Die Infrastruktur von Bitcoin nutzt ein Peer-to-Peer-Netzwerk. Die Daten werden auf Tausenden von Peers gespeichert. Dadurch ist das Bitcoin-System maximal ausfallsicher.

Zusätzliche kann man die Bitcoin-Währung (vor allem im Internet) ohne zwischengeschaltete Instanz verschicken. Dadurch werden die Transaktionen viel billiger.

Bitcoin Core ist die Referenzimplementierung der Bitcoin-Blockchain. Bitcoin-Core ist Open Source (MIT-Lizenz)

Slide 3



Probleme einer verteilten Datenbank
In einem verteilten System muss jede Transaktion auf jedem Knoten des Systems registriert werden. Wenn die Datenübermittlung ohne zeitliche Verzögerung ablaufen würde, wäre eine konsistente zeitliche Abfolge aller Transaktionen gewährleistet. In einem solchen System wären alle Knoten in jedem Zeitpunkt synchron. In einem solchen System würden die Transaktionen auf allen Knoten in genau jener zeitlichen Abfolge registriert, in welcher sie vorgefallen sind. In einem solchen System ist kein *double spending* möglich.

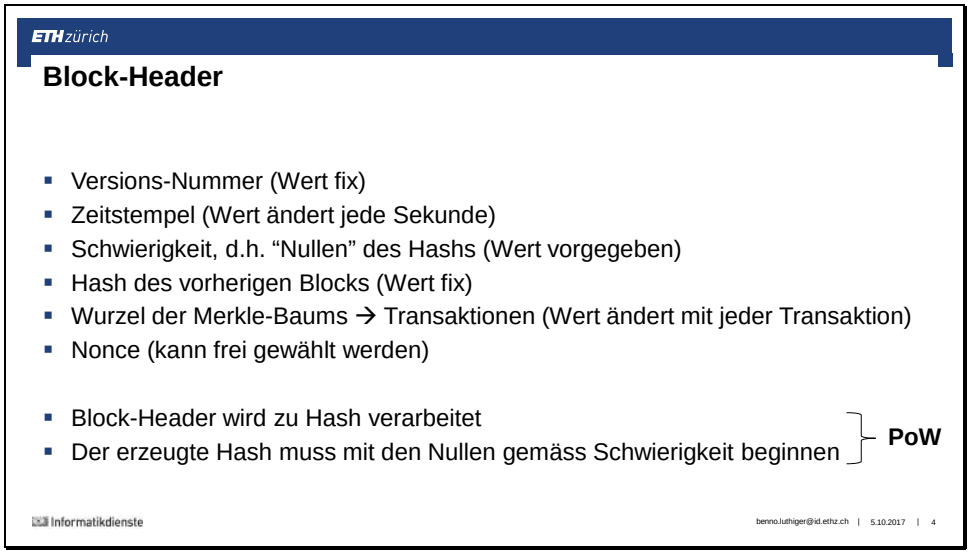
Ein solches System ist allerdings unmöglich. In der Realität müssen wir mit Netzwerklatenz rechnen. Das bedeutet, dass die einen Transaktionen auf den einen Knoten vor und auf anderen Knoten hinter bestimmten anderen Transaktionen registriert werden. In realen Netzwerken mit Latenz kann ich z.B. im Internet etwas kaufen und eine Sekunde später den gleichen Betrag mir überweisen (*double spending*) und habe gute Chancen, dass auf gewissen Konten die zweite, unrechtmässige Transaktion vor der ersten registriert wird.

Wie können wir in einem verteilten System Konsens darüber erreichen, welche zeitliche Reihenfolge der Transaktionen korrekt ist?
Der erste Teil der Antwort ist: wir lassen das Netzwerk entscheiden.

Gefälschte Identitäten («Sybil»-Attacken):
Wenn ich ein Teil des (anonymen) Netzwerks bin, welches über die richtige Reihenfolge der Transaktionen entscheidet, dann könnte ich versuchen, mich mit zusätzlichen Identitäten am Netzwerk anzumelden, um auf diese Weise eine Entscheidung zu meinen Gunsten zu erzwingen. Wie können solche Sybil-Attacken verhindert werden?
Das führt zum zweiten Teil der Antwort: wir müssen das Erzeugen falscher Identitäten aufwendig machen. Bevor eine Transaktion verifiziert und die entsprechenden

Information verbreitet wird, müssen die beteiligten Parteien eine Art von Arbeit leisten. Dadurch hängt die Fähigkeit, eine Transaktion zu verifizieren, von der Rechenleistung ab und nicht von der Kapazität, falsche Identitäten zu erzeugen. → Proof of Work.

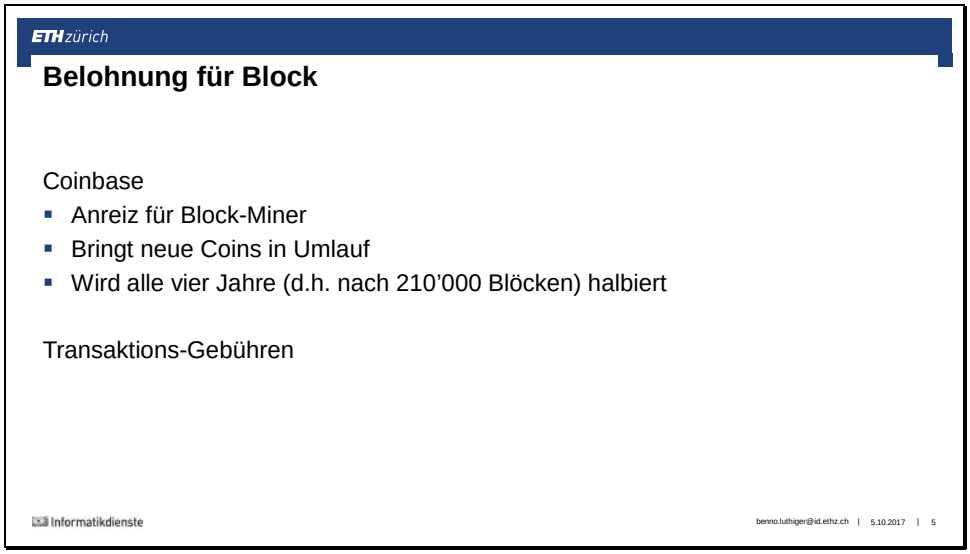
Slide 4



In der Bitcoin-Blockchain werden alle Transaktion in Blöcken gespeichert. Wie sieht so ein Block aus?
Der Block besteht aus einem Kopf und dem Körper. Im Körper sind die Transaktionen gespeichert. Der Block-Kopf enthält eine Referenz auf den vorgängigen Bock. Auf diese Weise formen die Blöcke eine Kette. Ein neuer Block wird durchschnittlich alle 10 Minuten erzeugt.
Der Block-Kopf besteht aus sechs Angaben: die *Versionsnummer* der Blockchain, einem *Zeitstempel* (in Sekunden ab 1970-01-01 UTC), der *Schwierigkeit*, dem *Nonce*, dem *Hash des vorhergehenden Blocks* sowie der *Wurzel des Merkle-Baums*, welcher durch die im Block gespeicherten Transaktionen geformt wird. Diese sechs Informationen werden zu einem Hash verarbeitet, welcher seinerseits in den Kopf des nachfolgenden Blocks eingeht.
Damit ein Block gültig ist, müssen folgende Bedingungen erfüllt sein: die im Block gespeicherten Transaktionen müssen verarbeitet und validiert sein, der Block muss den beschriebenen Kopf haben und der Hash aus dem Block-Kopf muss eine bestimmte Form haben.
Zwei Angaben sind wesentlich für die Berechnung des Hashs aus dem Block-Kopf: die *Schwierigkeit* und das *Nonce*. Die sogenannte Schwierigkeit bestimmt die Anzahl Nullen, mit welchen der berechnete Hash beginnen muss. Man mag sich jetzt wundern: wie kann ein Hash, welcher aus bestimmten Werten berechnet wird, eine vorgegebene Form aufweisen? Ist es nicht genau die Eigenschaft eines Hashs, dass sein Wert eindeutig von seinen Eingabewerten abhängig ist und es keine Freiheitsgrade gibt, was seine Form betrifft?
Doch mit dem Nonce wir haben einen Freiheitsgrad. Das ist genau der Zweck den Nonce. Dieses muss solange variiert werden, bis der Hash, welches das Nonce mit den anderen Block-Header-Informationen bildet, die gewünschte Form aufweist. Genau darin besteht die Arbeit des PoW, der Aufwand, den wir leisten müssen und der sicherstellt, dass wir mit der Rechenleistung und nicht mit möglicherweise falschen Identitäten abstimmen.

Die Schwierigkeit in der Bitcoin-Blockchain ist so eingestellt, dass im statistischen Mittel 10 Minuten benötigt werden, bis ein passender Hash gefunden und damit ein Block erzeugt wird. Diese Schwierigkeit wird alle zwei Wochen (jeweils nach 2016 Blöcken) angepasst. Warum das? Für eine stabile Bockchein ist es wesentlich, dass das PoW einen beachtlichen Aufwand bedeutet. Ist das PoW zu klein, besteht die Gefahr von Sybil-Attacken. Ein gutes Mass für die Stärke des PoW ist der zeitliche Aufwand, um dieses PoW zu leisten, d.h. einen Hash mit den geforderten Nullen am Anfang zu finden.
Wenn sich nun mehr Mining-Computer an der Blockchain betätigen oder wenn die Prozessoren stärker werden, muss die Schwierigkeit, einen gültigen Hash zu finden, erhöht werden. Ohne Anpassung würde das Intervall zwischen zwei Blöcken auf Millisekunden fallen. Es war eine der wesentlichen Erkenntnisse von Nakamotos Forschungspapier, dass er zeigen konnte, dass der Aufwand, einen gültigen Hash zu finden, exponentiell zur Anzahl der geforderten Nullen am Anfang steigt. Wenn das Netzwerk nun herausfinden, dass die Kapazität zur Berechnung der Hashe signifikant gestiegen ist, wird die Schwierigkeit erhöht. Dieser Automatismus stellt sicher, dass die Zeitspanne zwischen zwei Blöcken um 10 Minuten pendelt.
Es ist jedoch völlig unbestimmt, welcher Mining-Knoten im Netzwerk den nächsten Block finden wird. Es gibt nur eine Prognose: je mehr Rechenleistung ein Knoten hat im Vergleich zu den anderen Knoten, desto grösser ist die Wahrscheinlichkeit, dass dieser Knoten den nächsten Block finden wird.

Slide 5



Das PoW führt dazu, dass es kostspielig ist, einen neuen Block zu erzeugen. Warum soll jemand seinen Rechner mit seiner Rechenleistung zur Verfügung stellen, damit neue Blöcke für die Blockchain erzeugt werden können und diese somit am Leben erhalten wird? Das Bitcoin-Protokoll liefert einen starken Anreiz, dies zu tun. Jeder gefundene Block wird mit 12.5 Bitcoins belohnt (aktuell 55'000 $). Zusätzlich erhält der Miner, welcher den Block gefunden hat, die Transaktionsgebühren aller im Block gespeicherten Transaktionen.
Mit der Block-Belohnung sollen zwei Ziele erreicht werden: Zusätzlich zum Anreiz für Miner werden auf diese Weise neue Coins in Umlauf gebracht. Die neu erzeugten Coins werden *Coinbase* genannt. Die Block-Belohnung startete mit 50 Bitcoins und wird alle vier Jahre (exakt alle 210'000 Blöcke) halbiert. Am Ende, ca. im Jahr 2140, wird das Bitcoin-Währungssystem 21 Mio. Bitcoins im Umlauf haben.

Slide 6

ETH zürich

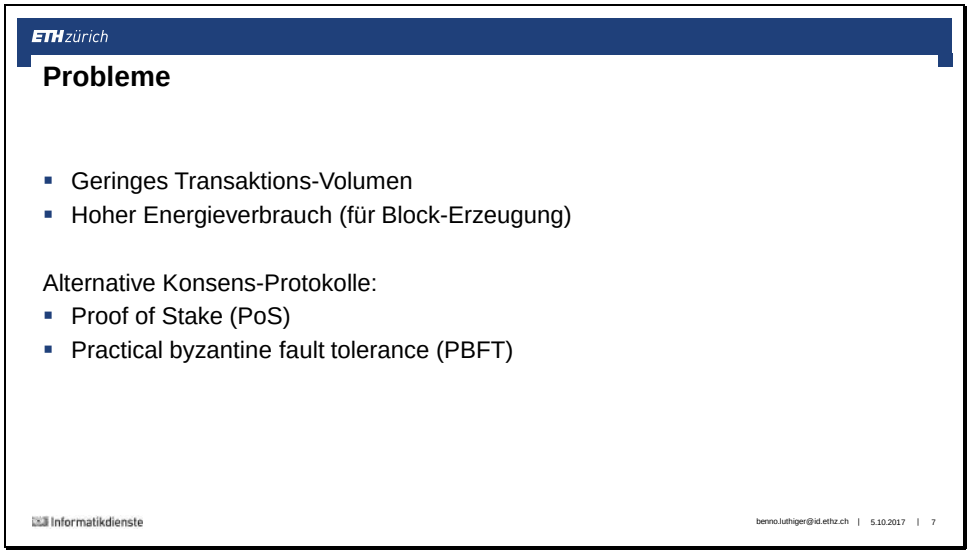
Rekapitulation

- Transaktionen werden in Blöcken registriert, welche die “Seiten” einer verteilten Buchhaltung darstellen.
- Die Blöcke werden in einer Kette angeordnet, um eine vollständige Ordnung der Transaktionsgeschichte sicherstellen zu können.
- Um einen Block zu erzeugen, muss ein kryptographisches Puzzle gelöst werden (PoW). Damit werden Attacken mit gefälschten Identitäten verhindert.
- Neue Blöcke werden auf der längsten Kette erzeugt, um Gabelungen zu verhindern.
- Der Erzeuger (miner) eines neuen Blocks wird mit einer Entschädigung (in Bitcoins) belohnt.

- Animation auf https://www.youtube.com/watch?v=rSL5eSv31ew

Wir verstehen nun die Blockchain-Architektur:
Mit diesen Prinzipien ist es möglich, dass die Bitcoin-Blockchain stabil bleibt ohne zentrale Autorität.

Slide 7

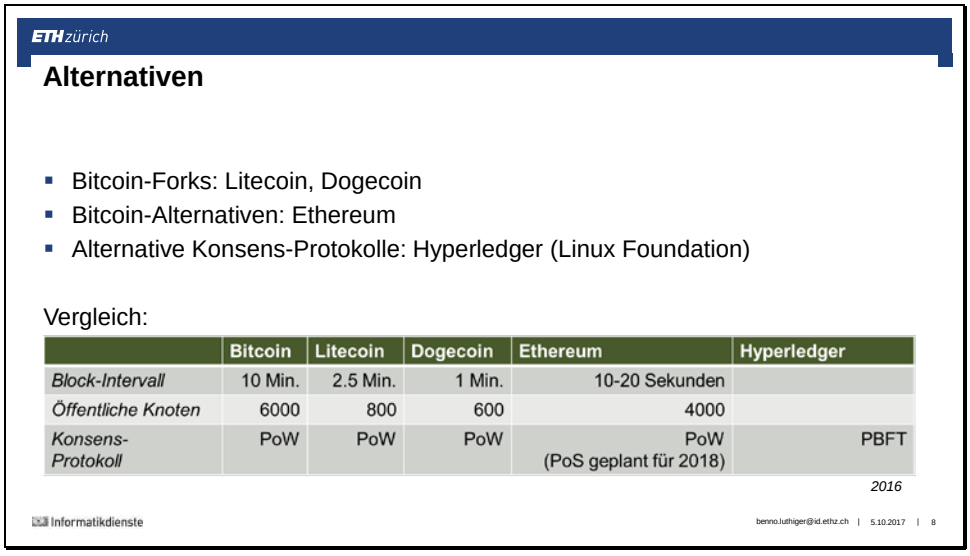


Das Bitcoin-Protokoll weist zwei Probleme auf.

Das eine Problem ist, dass das Transaktionsvolumen limitiert ist. Diese Beschränkung wird einerseits durch die Blockgrösse verursacht, welche 1MB beträgt. Andererseits beschränkt das Block-Erzeugungs-Rate von 10 Min. dieses Transaktionsvolumen. Gerade in diesen Wochen ist die Bitcoin-Blockchain in einer grossen Umbauphase, welche unter dem Namen SegWit2x läuft. Mit diesem Umbau soll das Transaktionsvolumen verdoppelt werden.

Wahrscheinlich das grössere Problem ist, dass das Erzeugen von neuen Blöcken heutzutage mit einem massiven Energieverbrauch verbunden ist. Bitcoin-Blöcke werden heutzutage mit hochspezialisierten CPUs erzeugt. Diese berechnen Millionen von Hashs pro Sekunde. Je mehr Hashs pro Zeiteinheit berechnet werden, desto grösser ist der Energieverbrauch. Bitcoin-Miner verbrauche also viel Energie für einen relativ stupiden Zweck. Die Ursache dieser Energieverschwendung liegt darin, dass die Bitcoin-Blockchain für das Konsens-Prinzip auf das PoW setzt. Wenn wir eine Blockchain mit weniger Energieverschwendung wollen, müssen wir ein anderes Konsens-Prinzip finden, welches das PoW ersetzen kann.
Die prominentesten Alternativen für das PoW ist das Proof-of-Stake (PoS) sowie das *Practical Bycantine fault tolerance* (PBFT).
Während das PoW und das PoS in echten Peer-to-Peer-Netzwerken funktionieren, setzt das PBFT ein Netzwerk voraus, in welchem alle Mining-Knoten bei allen anderen registriert sind. Ein solches Netzwerk ist also kein offenes Peer-to-Peer-Netzwerke mehr.

Slide 8



Einige Alternativen zur Bitcoin-Blockchain sind Bitcoin-Forks, welche das Blockerzeugungs-Intervall variieren, um ein höheres Transaktioinsvolumen zu erreichen. Die bekanntesten dieser Forks sind *Litecoin* und *Dodgecoin*. Der bekannteste Rivale von Bitcoin ist allerdings *Ethereum*. Ethereum hat ein eigenes Blockchain-Protokoll. Bei Ethereum werden die Transaktionen mit einer Skriptsprache validiert, welche sich deutlich von derjenigen bei Bitcoin unterscheidet. Die Etherum-Skriptsprache heisst Solidity und ähnelt entfernt JavaScript. Solidity ist Turing-komplett. Damit wird die Ehereum-Skriptsprache komplexer, ermöglicht es aber umgekehrt, auf der Ethereum-Blockchain sogenannte Smart-Contracts laufen zu lassen.
Eine neue Alternative zur Bitcoin-Blockchain ist *Hyperledger*. Hyperledger ist ein Projekt der Linux-Fundation und wird von einem Konsortium vorangetrieben. Ein wichtiger Treiber von Hyperledger ist IBM. Hyperledger nutzt PBFT als Konsens-Protokoll. Die Hyperledger-Blockchain stellt demnach kein offenes Peer-to-Peer-Netzwerk dar. Es gibt allerdings interessante Anwendungsfälle, für welche ein solches Peer-to-Peer-Netzwerk nicht notwendig ist. Für diese Fälle könnte Hyperledger eine gute Option darstellen.

Slide 9

ETH zürich

Blockchain: Anwendungsfälle

- Kryptowährung
- Smart Contracts
- Infrastruktur für Digitale IDs
- Verteilter Speicher für juristische Papiere
- Verteilte Datenbanken

Slide 10

ETH zürich

Blockchain: Anwendungsfall *Kryptowährung*

Zahlungen:
Rimessen von philippinischen Fremdarbeitern

Online-Handel:
- Lush Cosmetics UK
- Versandhaus Lehner
- Hochschule Luzern

Informatikdienste

Beispiel 1: Rimessen von philippinischen Fremdarbeitern:
http://biccur.com/partners/rebit-philippine-remittance/

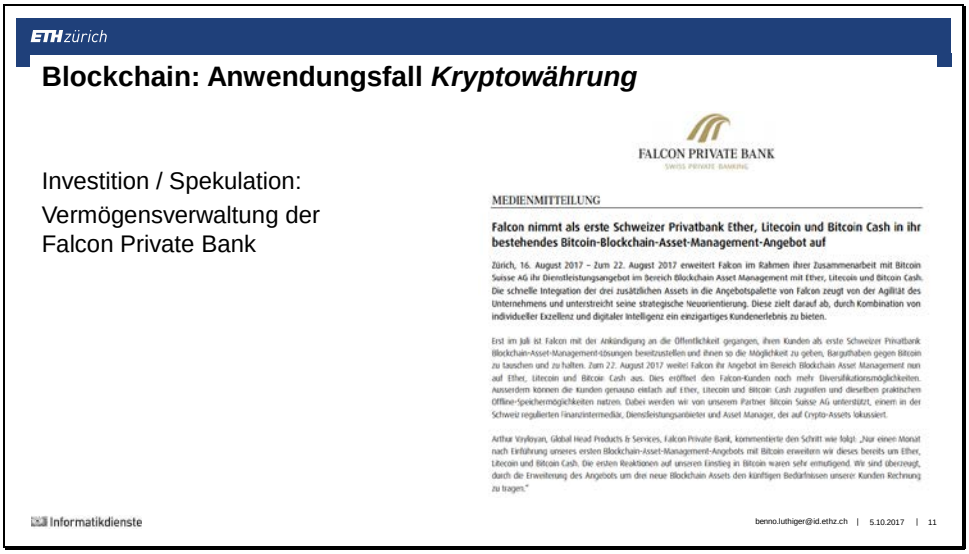
Lush Cosmetics UK (https://uk.lush.com/article/doing-our-bitcoin-lush-digital-accepts-cryptocurrency)
Versandhaus Lehner (https://www.lehner-versand.ch/)
Hochschule Luzern (https://www.hslu.ch/de-ch/hochschule-luzern/ueber-uns/medien/medienmitteilungen/2017/10/03/bitcoin/)

Slide 11

ETH zürich

Blockchain: Anwendungsfall *Kryptowährung*

Investition / Spekulation:
Vermögensverwaltung der Falcon Private Bank



FALCON PRIVATE BANK
SWISS PRIVATE BANKING

MEDIENMITTEILUNG

Falcon nimmt als erste Schweizer Privatbank Ether, Litecoin und Bitcoin Cash in ihr bestehendes Bitcoin-Blockchain-Asset-Management-Angebot auf

Zürich, 16. August 2017 – Zum 22. August 2017 erweitert Falcon im Rahmen ihrer Zusammenarbeit mit Bitcoin Suisse AG ihr Dienstleistungsangebot im Bereich Blockchain Asset Management mit Ether, Litecoin und Bitcoin Cash. Die schnelle Integration der drei zusätzlichen Assets in die Angebotspalette von Falcon zeugt von der Agilität des Unternehmens und unterstreicht seine strategische Neuorientierung. Diese zielt darauf ab, durch Kombination von individueller Exzellenz und digitaler Intelligenz ein einzigartiges Kundenerlebnis zu bieten.

Erst im Juli ist Falcon mit der Ankündigung an die Öffentlichkeit gegangen, ihren Kunden als erste Schweizer Privatbank Blockchain-Asset-Management-Lösungen bereitzustellen und ihnen so die Möglichkeit zu geben, Barguthaben gegen Bitcoin zu tauschen und zu halten. Zum 22. August 2017 weitet Falcon ihr Angebot im Bereich Blockchain Asset Management nun auf Ether, Litecoin und Bitcoin Cash aus. Dies eröffnet den Falcon-Kunden noch mehr Diversifikationsmöglichkeiten. Ausserdem können die Kunden genauso einfach auf Ether, Litecoin und Bitcoin Cash zugreifen und dieselben praktischen Offline-Speichermöglichkeiten nutzen. Dabei werden wir von unserem Partner Bitcoin Suisse AG unterstützt, einem in der Schweiz regulierten Finanzintermediär, Dienstleistungsanbieter und Asset Manager, der auf Crypto-Assets lokussiert.

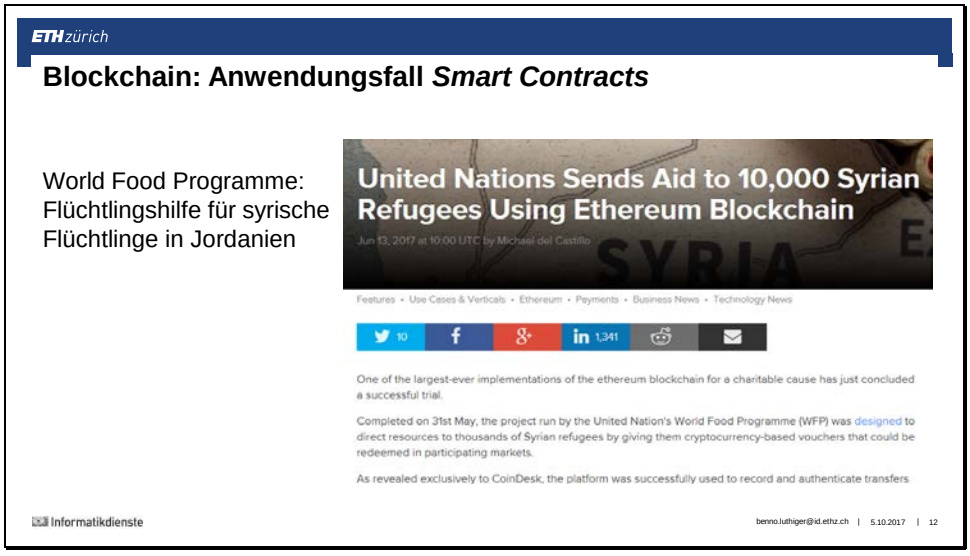
Arthur Vinyloyan, Global Head Products & Services, Falcon Private Bank, kommentierte den Schritt wie folgt: „Nur einen Monat nach Einführung unseres ersten Blockchain-Asset-Management-Angebots mit Bitcoin erweitern wir dieses bereits um Ether, Litecoin und Bitcoin Cash. Die ersten Reaktionen auf unseren Einstieg in Bitcoin waren sehr ermutigend. Wir sind überzeugt, durch die Erweiterung des Angebots um drei neue Blockchain Assets den künftigen Bedürfnissen unserer Kunden Rechnung zu tragen."

Informatikdienste

benno.luthiger@id.ethz.ch | 5.10.2017 | 11

Beispiel 2: Vermögensverwaltung der Falcon Private Bank: https://www.falconpb.com/tl_files/content/media_releases/150857-R-2127478-812417.pdf

Slide 12



World Food Programme: Flüchtlingshilfe für syrische Flüchtlinge in Jordanien auf der Ethereum-Blockchain: https://www.coindesk.com/united-nations-sends-aid-to-10000-syrian-refugees-using-ethereum-blockchain/

Slide 13

ETH zürich

Blockchain: Anwendungsfall *Infrastruktur für Digitale IDs*

Blockchainbasierte E-ID in der Stadt Zug

Zug startet Pilot mit E-ID auf Blockchain-Basis

Eine Stadt prescht bei der digitalen Identität vor.

Die Stadt Zug biete ab September als weltweit erste Gemeinde allen Einwohnern die Möglichkeit, eine digitale Identität zu bekommen, behauptet die Stadt in einer Mitteilung. Die Einwohner registrieren dabei ihre Identität selber in der Ethereum-Blockchain. "Wir überprüfen und bestätigen lediglich die Identität einer Person", lässt sich der Zuger Stadtpräsident Dolfi Müller in der Mitteilung zitieren.

Mathias Bucher, Dozent an der HSLU und am Projekt beteiligt, sagte zu inside-it.ch: "Es ist uns wichtig zu betonen, dass die Benutzer selber im Besitz ihrer Daten bleiben". Die Lösung speichert die persönlichen Informationen nicht zentral, sondern sichert sie durch die Verknüpfung mit einer Crypto-Adresse auf der Blockchain. Die persönlichen Daten befinden sich auf dem mobilen Gerät der User, aber im Falle des Verlusts des Devices, kann die Identität über die Blockchain neu verifiziert werden.

Blockchainbasierte E-ID für Zug:
http://www.inside-it.ch/articles/48044

Slide 14

ETH zürich

Blockchain: Anwendungsfall *verteilter Speicher*

Verteilter Speicher für juristische Papiere

IBM Forges Blockchain Collaboration With Nestlé & Walmart In Global Food Safety

Roger Aitken, CONTRIBUTOR
FULL BIO

A group of leading retailers and food companies including Nestlé and Walmart have signalled their commitment to "strengthen consumer confidence" in the foods they purchase by announcing a major blockchain collaboration with IBM. The consortium will work with 'Big Blue' to identify the "most urgent areas" across the global food supply chain that could benefit from the blockchain.

Highlighting matters, every year one-in-10 people fall ill (c.600 million) globally and around 420,000 die as a result of contaminated food, according to global estimates of foodborne diseases from the World

Verteilter Speicher für juristische Papiere auf Hyperledger: https://www.forbes.com/sites/rogeraitken/2017/08/22/ibm-forges-blockchain-collaboration-with-nestle-walmart-for-global-food-safety/