

readme

Das Bulletin der
UZH Alumni Informatik

Blockchain, X-coins und Smart Contracts – Was machen wir daraus?

Blockchains, Bitcoins und Smart Contracts – Eine Evolution oder Revolution in der Informatik? 3

Worum geht's, welche Aspekte sind zu berücksichtigen und worin liegen die Potentiale
Burkhard Stiller

Abenteuer Crypto-Trading-Bot 8

Wie man trotz hoher Volatilität und Gewinnerwartungen doch noch
einen kühlen Kopf bewahrt
Amancio Bouza

Entwicklung von Customized Indizes am Beispiel des Crypto Market Index 10

Entstehung und Umsetzung einer Krypto-Index-Lösung und deren Herausforderungen
Christian Bahr

Sind ICOs Stolperstein oder Chance? 14

Neues Finanzierungs-Instrument, aber nur gepaart mit bewährten Grundsätzen
Ralph Morigato und Roger Darin

Gaming oder Mining? 20

Kampf der Anwendungs-Domänen um rechenstarke Graphikkarten
Marc Stampfli

Let's talk security: Tod dem Passwort 22

Wie man das Passwortmanagement sicher in den Griff bekommt
Adrian Bachmann

Tokeneconomy – Wieso macht das Sinn? 24

Tokenisierung der eigenen Freizeit
Moritz Baggenstos

editorial

readme

Liebe Alumni-Mitglieder,
liebe Leserin,
lieber Leser

Bei einigen unter uns liegen wohl schon die Nerven blank aufgrund dem Anfangs Jahr hingelegten Kurssturz der Bitcoin. Andere stehen noch an der Seitenlinie und warten weiter ab, wohin denn die Reise gehen mag. Blockchain als Basistechnologie scheint wohl gesetzt zu sein... oder etwa auch noch nicht? Jedenfalls tun sich mit diesen sagen wir mal «Konzepten» zigfache Möglichkeiten auf, wie wir in Zukunft Waren und Dienstleistungen austauschen sowie Handel treiben können und werden. Bestehende Prozessketten werden damit kompromittiert, ganz neue werden sich auftun und können als Chancen wahrgenommen werden. Und dies global. Spannend, oder?

Gerne möchten wir nun in diesem readme 39/18 ebenfalls diese Konzepte und Entwicklungen aufnehmen und behandeln. Fragen wie «welcher Bitcoin wird denn das Rennen machen» oder «wo soll ich investieren – in Geld oder applikatorische Anbindung» sind nur einige Fragen, die sich einem in diesem Kontext stellen. In diesem Sinne haben ich unsere Alumni-Community aufgerufen, über ihre eigenen Erfahrungen, Aktivitäten oder Projekte zu berichten. Der Feedback, einen Artikel schreiben zu wollen, war diesmal auch erstaunlich höher als bei vergangenen readmes. Das Topic scheint wohl auch in unserer Alumni-Community heiss zu sein.

Glücklicherweise haben wir unter unseren IfI-Professoren einen ausgewiesenen Experten, was Blockchain, Bitcoin,

Smart Contracts und damit verbundene Technologien oder Aspekte betrifft. Burkhard Stiller gibt uns dementsprechend auch eine Intro in das Themenfeld und regt mit seinen Ausführungen zu weiteren Reflektionen an.

Andri Färber berichtet uns über die letzte Generalversammlung im November 2017 und gibt einen kurzen Ausblick auf die für dieses Jahr aufgelegten Alumni-Events.

Amancio Bouza, unser Ex-IfI-Vertreter im Vorstand, gibt uns einen Einblick über seine hands-on Erfahrungen mit Ether Trading und diesbezügliche Begleitung mit Informatik-Mitteln.

Christian Bahr von der SIX legt uns dar, wie er und sein Team den Crypto Market Index 10 realisiert und die verschiedenen Herausforderungen gemeistert haben.

Ralph Mogenicato und Roger Darin beleuchten mit ihrem Artikel das Thema Initial Coin Offerings (ICO) und zeigen auf, welche speziellen Aspekte es da zu beachten gilt und dass Best-Practice-Prinzipien sowie haarscharfe Analysen beim Investieren durchaus immer noch ihre Daseinsberechtigung haben.

Wir dachten, dass es wieder mal an der Zeit wäre, sich über Security Gedanken zu machen. In unserer Rubrik «Let's talk security» behandelt unser IT-Security-Experte Adrian Bachmann das Topic Passwortmanagement. Ich glaube, diese Reflektionen tun uns wieder mal gut.

Auch am IfI gab es wieder professoralen Zuwachs, worüber uns Avi Bernstein ausführlich berichtet.



Ferner wurden auch im Blockchain-Umfeld unter der Ägide der Professoren Stiller und Schwabe hochinteressante Projekte lanciert.

Marc Stampfli zeigt auf, in welchem Luxus-Dilemma sich das GPU-Business befindet. 3D-Grafik, Crypto-Mining sowie Deep Learning benötigen alle rechenstarke Hardware, weshalb es zu Lieferengpässen und Bezugslimiten kommt.

Moritz Baggenstos legt uns dar, wie er in einem persönlichen Feldversuch seine eigene Freizeit als MoCoin implementiert respektive tokenisiert und dabei auch gleich einen kleinen Marktplatz im Bekanntenkreis lanciert hat.

Zum Schluss danke ich allen, die an diesem readme 39/18 mitgearbeitet haben, sowie unseren Sponsoren und Partnern für deren Unterstützung und wünsche viel Vergnügen bei der Lektüre.

Herzlich, Euer
Kornél Szabó

Chefredaktor readme

Kontakt:
Dr. Kornél Szabó, szabo@alpnet.ch

Blockchains, Bitcoins und Smart Contracts – Eine Evolution oder Revolution in der Informatik?

Burkhard Stiller

Blockchains, Bitcoins und Smart Contracts werden einer kurzen Analyse unterzogen, um auf der Basis einer Definition dieser Begriffe, dem Ausführen wesentlicher Eigenschaften dieser Komponenten und der Einbettung dieser in die Technologiediskussion heutiger Tage aufzeigen zu können, dass die Informatik sich in diesem Bereich einer Evolution gegenüber sieht, welche im täglichen Umfeld unserer Gesellschaft allerhöchstens revolutionäre Anzeichen für verschiedene Anwendungsfelder aufweist, da diese bis heute mit komplementären Lösungsansätzen versehen wurden, aber zumindest bis anhin keine traditionellen Systeme hinweggefegt haben.

Blockchains werden gerne als Technologie bezeichnet, obwohl sie im Kern nichts weiter als eine Datenstruktur – eine verkettete Liste von Datenelementen, welche einzeln als «Block» referenziert werden – sind und welche über kryptografisch definierte Verkettungsregeln verbunden werden. Aber wie in der Informatik relativ regelmässig üblich, wird eine prospektiv mit Potential versehene Idee schnell mit dem Begriff einer «Technologie» versehen. Während ursprünglich im Griechischen *τεχνολογία* (technologia) «Kunst» oder «Handwerk» bezeichnete, wird Technologie heute eher in der Bedeutung der «Wissenschaft von der Technik» oder gar eines «einsatzfähigen Systems mit dezidierter Funktionalität» verwendet. Diese gewisse Form der Schönfärberei findet sich deswegen immer häufiger in der Verwendung des Technologiebegriffes, welcher eben auch in Form der «Blockchain-Technologie» im Sprachgebrauch sowohl der Medien als auch der Wissenschaft Einzug gehalten hat. Sprich, worum handelt es sich nun wirklich bei Blockchains oder gar einer Blockchain-Technologie? Gleicht diese besondere, verkettete Liste einer Evolution der bekannten dynamischen Datenstruktur von Verkettungen, die mehr als nur eine reihenfolgegebundene Anordnung der Datenelemente erlaubt? Oder ist die Tatsache, dass die Anzahl der Objekte

im Vorhinein nicht festgelegt sein muss und damit für die gesamte Lebenszeit der verketteten Liste nach oben offen, aber durch die Verwendung kryptografischer Verkettungsregeln nicht mehr auflösbar bzw. lösbar (sondern nur noch erweiterbar) und damit fälschungssicher (unter klar definierten Annahmen) ist, eine Revolution?

Definition

Um diese Fragen zu beantworten und damit auch dem Problem ansatzweise Herr zu werden, wo denn überhaupt eine Blockchain sinnvollerweise eingesetzt werden kann, folgt als Startpunkt eine grundlegende Definition: *Eine Blockchain ist eine verkettete Liste von Datenelementen, den «Blöcken», welche über kryptografische Hashes (Streuwerte) des vorhergehenden Datenelementes, einen Zeitstempel und die sogenannten Transaktionsdaten (dem zwischen Teilnehmern ausgetauschten Inhalt des Datenelementes, als Byte-String betrachtet und damit unterschiedlichen semantischen Nutzungen offenstehend) verfügen und verkettet sind.* Das Berechnen des Hashes und das damit verbundene Eintragen in die Blockchain wird als «Mining» bezeichnet, welches vom Verteilen dieser persistierten Datenelemente auf der Basis eines Peer-to-Peer-Netzes gefolgt wird, um



Prof. Dr. Burkhard Stiller leitet die Communication Systems Group (CSG) des Instituts für Informatik an der Universität Zürich seit ihrer Gründung im Jahr 2004 und beschäftigt sich in Zusammenarbeit mit seinem Team von Doktoranden und Oberassistenten u.a. mit den Themen Systeme mit vollständig verteilter Kontrolle (Blockchains, Peer-to-Peer), Netzwerk Management, Internet-of-Things (IoT, Sicherheit, LoRa) und Telecommunication Economics.

Kontaktadresse:
Prof. Dr. Burkhard Stiller
Communication Systems Group (CSG)
Institut für Informatik
Universität Zürich
Binzmühlestrasse 14
CH-8050 Zürich
Tel: +41 44 635 67 10
E-Mail: stiller@ifi.uzh.ch
<http://www.ifi.uzh.ch>

Fortsetzung auf Seite 4

sicherzustellen, dass alle Teilnehmer (welche sich freiwillig dieser Blockchain angeschlossen haben) den aktuellen Stand der Transaktionen mitgeteilt bekommen.

Der Begriff der Blockchain – hier nun als Konzept interpretiert – erweitert diese erste Definition um die Tatsache, dass diese verketteten Listen nun nicht notwendigerweise nur auf einem Rechner geführt werden müssen, sondern verteilt über beliebige Systemgrenzen hinweg auf vielen Rechnern dezentral gespeichert werden können. Gerne spricht die Literatur dann von einem «Distributed Ledger» (verteiltes Hauptbuch) und unter Beachtung der obigen Diskussion lieber gleich von einer «Distributed Ledger Technology (DLT)», welche im Kern ein Buchführungssystem kennzeichnet, das dezentral Datenelemente in dieser verketteten Liste speichern kann. Dabei ist aber sicherzustellen, dass ein Konsens der (vielen) Beteiligten über den korrekten Zustand dieses Systems erreicht wird und ein neu zu schreibendes Datenelement in Form einer Transaktion auf der bereits im Konsens gespeicherten und damit korrekten, früheren Transaktion aufzubauen ist – eben unter der Anwendung der kryptografischen Verkettung der Datenelemente. Offensichtlich besteht auch im verteilten Fall keine obere Grenze, welche in irgendeiner Form die Anzahl der Datenelemente limitieren würde. Die Blockchain wächst mit jeder neu hinzugefügten Transaktion um eben genau diese als in einer maximalen Blockgrösse definierten Byte-Anzahl an, welche in einem einzelnen Konsensfindungsschritt zugelassen ist.

Dieses Vorgehen stellt sicher, dass spätere Transaktionen auf früheren Transaktionen aufgebaut sind. Damit kann eine neue Transaktion als richtig bestätigt werden, weil sie nur unter Kenntnis der früheren Transaktionen erstellt worden sein kann (Beweis). Damit ist die Fälschungssicherheit eines Datenelementes gewährleistet, wenn eine Transaktion bereits «alt» ist (sprich «neue» Transaktionen auf dieser «alten» in der Blockchain persistierten aufgebaut sind), wenn der

Hash-Algorithmus korrekt ist, wenn der Konsens der Beteiligten nicht durch die Mehrzahl der Beteiligten unterlaufen wurde (collusion, 51% Angriff) und wenn jedem – auch einem Unbeteiligten an der bisher derartig aufgebauten verketteten Liste – Beteiligten die gesamte Transaktionskette zur Verfügung steht (sprich eine Beweisführung über Inkonsistenzen durch die Offenlegung von älteren Transaktionen und derer Hash-Werte möglich ist).

Aus diesen Überlegungen heraus ist eine Blockchain als eine Evolution der traditionell verketteten Listen anzusehen, welche durch die angewendete Erweiterung der Verkettung mit kryptografischen Hashes einem algorithmischen Schritt gleicht, der hier eine Datenstruktur gegen äussere Manipulationen schützt. Hunderte von Systemen und Datenstrukturen sind in der Vergangenheit gegen diverse Angriffe gesichert worden, was somit auch bei verketteten Listen einem klar logischen Evolutionschritt gleichkommt.

Kryptografische Währungen

Die Anwendung dieser Blockchain-Datenstruktur, verbunden mit der Idee der dezentralen Buchführung, liefert nun genau diejenige Grundlage, welche kryptografische Währungen, zum Beispiel Bitcoin oder Ether, benötigen, um eine Transaktionssicherheit ohne jedwede zentrale Instanz zu erreichen. Bitcoin und Ethers sind aus Sicht der elektronischen Währungen keine Neuigkeiten. eCash, DigiCash oder diverse «micro-payment»-Systeme sind seit den 80-er Jahren des letzten Jahrhunderts bekannt, aber das Fehlen jedweder zentralen Instanz stellt für Bitcoins, Ethers und andere das neue Alleinstellungsmerkmal von dezentralen, kryptografischen Währungen dar. Ohne an dieser Stelle auf die ökonomischen, finanzmarkttechnischen oder regulatorischen Auswirkungen eines derartigen Ansatzes detailliert eingehen zu können, lässt sich sicher schon erahnen, dass die hier eher als disruptiv zu verstehende Veränderung bekannter

Abläufe und Strukturen nicht ganz zu leugnen ist, d.h., dass der Einsatz einer sicherheitstechnisch veränderten Datenstruktur, das Verteilen dieser in grossem Masse auf weltweit verteilte bzw. verteilbare Maschinen und das Bereitstellen einer passenden Zugangsschnittstelle – für Benutzer als auch Entwickler – zu grösseren «Verwerfungen» nicht nur im IT-Sektor geführt hat. Inwieweit diese Verwerfungen nun nicht nur zu positiven Konsequenzen, sondern auch bereits jetzt in Bereichen ausserhalb der IT zu eher als schwerwiegend zu bezeichnenden und weiteren Konsequenzen (z.B. Verbote der Nutzung kryptografischer Währungen oder regulatorische Vorgaben) führen werden, wird die Zukunft zeigen müssen.

Smart Contracts

Jedoch ist bereits jetzt deutlich geworden, dass eine weitere sehr wichtige Ergänzung der verteilten Blockchains um generische Programmiersprachen, welche die formelle Grundlage der «Smart Contracts» darstellen und theoretisch jedes Turing-Programm implementieren können, weitere «Erschütterungen» hervorruft. Während im Anwendungsfall der Bitcoins diese Smart Contracts «nur» Bezahlvorgänge zwischen zwei Parteien zu spezifizieren und in der Blockchain persistierend auszuführen erlauben, kann Solidity als Programmiersprache für Ethereum – der Open Source Plattform für DLTs, welche Ethers als Währungseinheiten verwendet – bereits von potentiell beliebigen Anwendungsfeldern verwendet werden. Smart Contracts sind bereits 1996 von Nick Szabo als «Building Blocks for Digital Markets» definiert worden und finden jetzt ihre verteilte, dezentrale, sichere, manipulationsfreie und nachweisbare Implementation und Anwendung auf der Basis von DLTs. Als sehr wichtig anzumerken ist, dass der Inhalt der Transaktion als elektronischer «Wert» vorliegen muss, um persistiert werden zu können. Dieses ist bei originär elektronischen Daten fälschungssicher erreichbar (z.B. bei Bitcoins, elektronische Spiele sowie elektronische Texte oder Bilder),

hingegen ist es bei aus der realen Welt abzuleitenden, elektronischen Repräsentationen noch mit Unsicherheiten behaftet: wie kann man z.B. sicherstellen, dass das nur Vorweisen eines Byte-Strings juristisch einwandfrei einklagbar beweist, dass damit das Grundstück X mit dem Gebäude Y gemeint ist, wenn DLTs in Grundbuchämtern/Notariaten eingesetzt werden?

Anwendungsfelder und Entscheidungskriterien

Die Anwendungsfelder von Blockchains und DLTs sind mannigfaltig (z.B. in der Finanztechnologie, der Autorenschaft bzw. bei Besitzverhältnissen, dem Datenmanagement, der digitalen Identität oder dem eVoting), aber nicht jede Anwendung wird von einer Blockchain oder DLT profitieren. Sprich, die fast als «alternativlos» geführte Diskussion über den zwingenden Einsatz dieser neuen, dezentralen Lösungsalternative für diverse Client-Server-basierte Systeme entbehrt jeder rationalen Grundlage. Nur dort, wo es notwendige, dezentrale Kernanforderungen gibt und keine traditionelle Datenbanklösung funktioniert oder wo mehr als nur wenige, a priori unbekannte und sich gegenseitig nicht vertrauende Teilnehmer interagieren müssen oder keine zentrale Instanz als für alle als vertrauenswürdig einzustufen zu finden ist, kann eine

Blockchain Abhilfe schaffen. Und nachfolgend ist immer noch zu entscheiden, wie es um die Privatheit der zu speichernen Daten bestellt ist. Wenn jeder diese einsehen und jeder auch neue Datenelemente in eine Blockchain eintragen kann, ist eine öffentliche Blockchain – im Sinne derjenigen der Bitcoins – sinnvoll. Sobald Daten privat bleiben müssen, sind diese kaum mehr direkt in öffentlichen Blockchains zu persistieren, allerhöchstens in «privaten» Blockchains (wobei dabei die Frage bis anhin ungeklärt bleibt, inwieweit eine Kontrolle der «privaten» Teilnehmer nicht zu potentiellen internen, betrügerischen Absprachangriffen führen kann, welche für die Beteiligten gar nicht detektierbar und schwer nachweisbar wären).

Schlussbetrachtungen

Blockchains, Bitcoins (als ein Anwendungsbeispiel der Blockchains im Falle kryptografischer Währungen ohne zentrale Instanz) und deren Smart Contracts basieren alle auf einer reihenfolgegebundenen, durch Hashes gesicherten und damit verketteten Anordnung von Datenelementen. Die Verwendung dieser und im besonderen in bezug auf den Einsatz von Hash-basierten Verkettungen als sehr aufgeweckt zu bezeichnenden Idee zur sicherheitstechnischen Erweiterung verketteter Listen muss als

Evolution in den Datenstrukturen bewertet werden, weil es sich im Kern um eine Kombination bekannter Konzepte und Algorithmen handelt. Der Einsatz dieser Datenstrukturen für die kryptografischen Währungen stellt ebenfalls eine blendende Idee dar, welche im Bitcoin-Papier Nakamotos auch einem sehr logisch nachvollziehbaren Entwicklungsschritt in der Informatik gleichkommt. Hingegen trägt der Einsatz dieser Datenstrukturen, Systeme und Anwendungen auf der Basis von Smart Contracts im täglichen Umfeld unserer Gesellschaft mehr als nur evolutionäre Züge, weil bekannte Abläufe als nun eben nicht mehr als einzig machbare hinterfragt und die Rolle einer (wünschbaren oder notwendigen?) zentralen Instanz in Frage gestellt werden. Aus aktueller Sicht ist dieses aber auch kaum als Revolution zu bewerten, da vorhandene Strukturen nicht hinweggefegt und «gelöscht» wurden, sondern alternative Wege, die wohl in naher Zukunft auch sicher komplementär neben bekannten Strukturen existieren werden, in wohl definierten Situationen Vorteile, Effizienzgewinne und neue Einsatzfelder erreichen können, während gleichzeitig traditionell als zentrale Systeme betriebene IT-Infrastrukturen in vielen Anwendungsumgebungen ihre Bedeutung beibehalten werden.

In eigener Sache: News aus dem Vorstand



Liebe Alumni-Mitglieder,
liebe Leserin, lieber Leser

Zur 21. Ordentlichen Generalversammlung waren wir bei IBM Schweiz in Zürich-Altstetten zu Gast. 53 Mitglieder folgten der Einladung und nahmen am Anlass teil. Die vom Vorstand beantragte Statutenanpassung im Hinblick auf die Steuerbefreiung des Vereins und in Anlehnung an die Namensänderung unserer Dachorganisation wurde von der Versammlung einstimmig angenommen. Der neue Vereinsname ist «UZH Alumni Informatik», wenn nötig abgekürzt «UZH.AI». Die entsprechende URL ist bereits registriert ;-). Katja Kevic, unsere bisherige IfI-Koordinatorin, hat ihre Dissertation erfolgreich beendet und verlässt deshalb das IfI. Damit scheidet sie automatisch als IfI-Koordinatorin aus. Wir danken der neugebackenen Doktorin herzlich für ihre Mitarbeit im Vorstand und übersenden ihr ein kleines Abschiedsgeschenk nach Cambridge (UK). Mit Nathan Labhart





Präsident der UZH Alumni Informatik

Kontaktadresse:

Andri Färber

Tel.: +41 79 642 08 85

E-Mail: andri.farber@alumni.uzh.ch

haben wir eine gute Nachfolge gefunden. Er ist Akademischer Koordinator am IfI und steht uns als solcher – hoffentlich – längerfristig zur Verfügung.

Im Anschluss an die GV brachten uns Frau Dr. Karin Vey, Herr Dr. Ulrich Schimpel und Herr Dr. Abu Sebastian, alle von IBM Research, auf den neusten Stand bezüglich «IBM Research and the Status of Cognitive Computing», «Deeper Dive - Cognitive and Blockchain» und «Brain-inspired Computing». Vor allem der letzte Vortrag handelte nicht nur von Brains, sondern forderte auch diejenigen des Publikums gehörig. Den Abschluss des offiziellen Teils machte Abraham Bernstein, Direktor des Instituts für Informatik, mit «Aktuellem aus dem IfI». Der Abend endete mit einem feinen Apéro, offeriert von IBM.

Auch dieses Jahr haben wir wieder ein reichhaltiges Event-Programm. Ihr findet es auf unserer Website <https://alumni.ch> unter der Rubrik «Events». Nach einer längeren Pause haben wir die Business Lunches mit interessanten Vorträgen wiederbelebt. Die Titel der Vorträge erfährt Ihr jeweils einige Wochen im Voraus per E-Mail. Weitere Leckerbissen sind eine Führung durch das Opernhaus Zürich mit anschliessendem Apéro, der Geburtstagsbrunch mit Figurentheater (ehemals Marionettentheater), ein Abendvortrag von Swisspeers zum Thema «Blockchain

im Crowdlending» und die Sommer-nachtsparty mit Special ShowAct.

Herzlich und bis bald an einem unserer Anlässe,

Euer
Andri Färber



Abenteuer Crypto-Trading-Bot

Amancio Bouza

News zu Preisrekorden und das endgültige Aus für Bitcoin & Co. wechseln sich wöchentlich ab. Bitcoin wurde bereits über 300mal von Finanzexperten als endgültig gestorben deklariert. Man kann sehr schnell sehr reich werden und ebenso wieder alles verlieren. Ich erzähle von meinem persönlichen Abenteuer mit Crypto-Trading und die Entwicklung eines Trading-Bots.

Die News sind voll davon. Gestern waren es die galaktischen Preisentwicklungen von Bitcoin, Ether, Ripple & Co. Heute wird wiederum das endgültige Aus für Bitcoin angekündigt. Und morgen stehen wieder neue Preisrekorde auf dem Programm. Es scheint wie ein Märchen, aus einem fernen Land, wo das Geld auf den Strassen liegt. Es klingt alles zu schön, um wahr zu sein. Doch dann kommt dieser eine Freund und berichtet mir von seinem Bitcoin-Reichtum.

Mein «Freund, der Bitcoin-Millionär»

Ich kann mich noch genau daran erinnern. Es war Ende April 2017, ein warmer Sommertag. In der Markthalle beim Viadukt in Zürich haben wir gerade zu Mittag gegessen und gingen draussen dann zum Espresso über. Stolz zückte mein Freund sein Handy hervor und zeigte mir eine Hockey-Stick-Kurve zur Preisentwicklung von Ether, der Währung für die Ethereum Blockchain. Er sagte bloss: «Hier unten habe ich gekauft. Heute ist es hier oben und achtmal so viel wert!»

Dieses Bitcoin-Märchen war auf einmal real. Und ich trank gerade Espresso mit dem Beweis in der Hand! Ich fragte nur: «Wo kann ich mitmachen?» Er zeigte mir, auf welcher Crypto-Coin-Plattform ich am günstigsten einsteigen kann. Jeder trifft früher oder später seinen «Freund, den Bitcoin-Millionär».

Über den Fluch des ersten Bitcoin-Kaufs

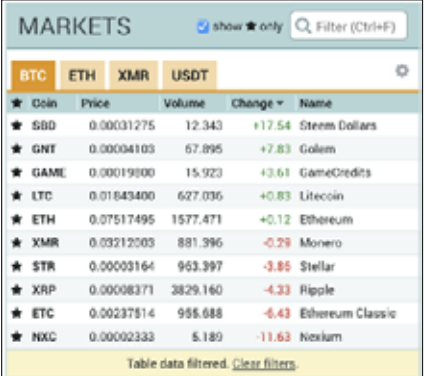
Der Registrierungsprozess auf solchen Crypto-Coin-Plattformen ist sehr aufwendig: Live-Identifikation per Video inklusive – sehr amüsant. Nach ein paar Tagen konnte ich den Registrierungsprozess endlich abschliessen. Schnell habe ich mir für 200 Euro ganze 0.95547288 Ethers gekauft – an die Nachkommastellen gewöhnt man sich sehr schnell.

Und los geht's mit meinem Abenteuer Crypto-Trading. «Klatsch. Autsch.» Selbstverständlich fällt der Kurs gerade jetzt um 20%. Der Fluch des ersten Bitcoin-Kaufs hat mich getroffen. Vorsicht: Dein «Freund, der Bitcoin Millionär» gibt natürlich immer dann mit seinen Bitcoins an, wenn der Kurs gerade sehr hoch ist.

Deshalb hier mein Tipp: Geduld! Warte nach einer euphorischen Bitcoin-News-Meldung erst mal zwei Monate ab und kauf erst dann.

Vorsicht: Suchtgefahr trotz Langeweile

Die Preise von Crypto-Coins fluktuieren sehr stark. 10% mehr oder weniger ist an der Tagesordnung, eine Preis-Achterbahn. Folgende Abbildung zeigt die Preisentwicklung von Bitcoin in den letzten 24h. Von -12% bis +18% ist alles dabei.



MARKETS				
show ★ only Filter (Ctrl+F)				
BTC	ETH	XMR	USDT	
★ Coin	Price	Volume	Change	Name
★ SBD	0.00031275	12.343	+17.54	Steem Dollars
★ GNT	0.0004103	67.895	+7.83	Golem
★ GAME	0.0001900	15.923	+3.61	GameCredits
★ LTC	0.0184340	627.036	+0.83	Litecoin
★ ETH	0.07517495	1577.471	+0.12	Ethereum
★ XMR	0.03212003	881.396	-0.29	Monero
★ STR	0.00003164	963.397	-3.85	Stellar
★ XRP	0.00008371	3829.160	-4.33	Ripple
★ ETC	0.00237514	955.688	-6.43	Ethereum Classic
★ NXC	0.00002333	5.189	-11.63	Nexium

Table data filtered. Clear filters.

[Quelle: Poloniex, 6.3.2018]

Ich war fasziniert. Es ging immer wieder hoch, dann aber wieder runter. Ich wurde schnell ungeduldig. «Ich muss Crypto-Coins handeln, täglich, um von dieser Preis-Achterbahn zu profitieren», dachte ich. Day-Trading war angesagt. Meine Milchbüchlein-Rechnung lautete ganz einfach: CHF 100 investieren, täglich 10% Gewinn erwirtschaften. Damit bin ich in 100 Tagen Millionär.

Ich habe also meine Ether auf Poloniex transferiert, einen der grössten Marktplätze für Crypto-Coins und mit Day-Trading angefangen. «Oops». Rasch habe ich einen Grossteil meiner Ether verspielt und in die falschen Crypto-Coins investiert. Dabei habe ich folgenden Grundsatz gelernt: Was hochsteigt, fällt auch wieder runter. Was unten ist, bleibt unten.

Ich bin direkt in die Anfänger-Falle getappt und habe meistens dann gekauft, wenn der Markt euphorisch war. «Too greedy». Das ist aber das Verhalten von 90% der Trader.

Ich habe kein Talent für das Trading, aber Talent für Technologie. Warum entwickle ich nicht einfach einen «smarten» Trading-Bot?

Proof-of-Concept eines Trading Bots: Epic Fail

Crypto-Coin-Marktplätze wie Poloniex bieten APIs an, um Marktinfs abzufragen und sein Crypto-Coin-Portfolio zu managen. Wunderbar! Nun steht einem Trading-Bot nichts mehr im Weg.

Mit Node.js habe ich rasch einen Proof-of-Concept (PoC) entwickelt. Die Idee des Bots war simple: Sammle alle 5 Sekunden Marktpreise. Berechne damit den durchschnittlichen Marktpreis. Wenn der Marktpreis unterhalb oder oberhalb des Durchschnittspreises +/- Zielgewinn liegt, verkaufe bzw. kaufe.

Build, deploy, run, get rich. «Oje, Denkfehler!». Der Bot hat innerhalb kurzer Zeit sein gesamtes Budget aufgebraucht und nacheinander zum gleichen Preis gekauft. Auf Produktion zu testen ist nicht ungefährlich. Mein Glück war, dass der Preis ein paar Tage danach wieder stieg und ich mit 3% Gewinn alles verkaufen konnte. Ich sah die Zeit gekommen, mich mit dem Thema Trading näher zu befassen.

Genetische Algorithmen, Real-Time Processing, Sentiment Analysis

Schnell habe ich mich in die Trading-Alchemie eingelesen: MACD, RSI, Pareto-Levels etc. Das Erfolgsgeheimnis liegt in der richtigen Auswahl und der

Parametrisierung dieser Metriken, ein sehr schönes Optimierungsproblem.

Ich habe Marktinfs über einen langen Zeitraum gesammelt. In Python habe ich einen genetischen Algorithmus entwickelt, welcher die optimale Parametrisierung über ein evolutives Verfahren in Kombination mit Simulated Annealing anhand der gesammelten Marktinfs identifiziert. Zusätzlich verwende ich auch Apache Spark, eine Big-Data-Technologie, um Sentiments von Twitter-Meldungen in Echtzeit mittels Machine Learning zu klassifizieren, sprich Sentiment Analysis. Ich wende bspw. MACD auf Sentiments an, um Trendwechsel von Sentiments zu erkennen und dem Bot Marktkontext zu geben. Beides kombiniere ich in einer sogenannten Lambda Architektur. Das klingt nach Overkill. Ja, ist es. Aber in der IT muss man ständig neue Technologien kennenlernen und meistern, und das sehr schnell. Mein Ansatz: Wenn Du nicht mehr lernen kannst, lerne mehr. D.h. ich kombiniere gerne verschiedene Technologien mit Business-Cases, um parallel Verschiedenes kennen zu lernen, um damit schneller zu lernen und Erfahrung zu sammeln.

Bin ich dein «Freund, der Bitcoin-Millionär»?

Mein Trading-Bot hat mein Investment von CHF 100 in wenigen Monaten knapp verdoppeln können (<http://notr.li/notraiderr/>). Wenn das so weitergeht, habe ich in rund 2761 Tagen 1 Mio. erwirtschaftet. Ich werde also in der 55. Alumni-Ausgabe gerne über den Stand berichten ;-) Fairerweise muss ich aber auch sagen, dass sich der Bitcoin in der gleichen Zeit verdreifacht hat.

Bots machen Spass, ein schönes Hobby. Die bessere Strategie ist aber: «Kauf Bitcoins heute und rühr sie 10 Jahre nicht mehr an.»



Amancio Bouza schloss 2008 sein Wirtschaftsinformatik-Studium an der Universität Zürich ab. Danach doktorierte er bei Prof. Avi Bernstein und Prof. Harald Gall im Bereich von Empfehlungssystemen, Machine Learning und Semantic Web. Amancio Bouza arbeitet bei der ipt - Innovation Process Technology AG, einer Schweizer IT-Consulting-Boutique. Zuvor gründete er ein Tech-Startup im Bereich Big Data und Crowd-Sourcing. Er ist Autor von API Product Management. Als Intrapreneur und Lean-Startup-Fan hilft er Unternehmen, digitale Technologien wirksam und messbar für Business Value einzusetzen. Er ist enthusiastisch bzgl. API und AI. Aktuell hilft er als Smart Data Coach, Unternehmen fit für Data-Driven Business zu machen.

Kontaktadresse:
Dr. Amancio Bouza
Innovation Process Technology AG
Poststrasse 14
CH-6300 Zug
Tel: +41 79 3987 69 35
E-Mail: amancio.bouza@ipt.ch
<http://www.ipt.ch>

Entwicklung von Customized Indizes am Beispiel des Crypto Market Index 10

Christian Bahr

Das Ziel des Crypto Market Index 10 ist die verlässliche Messung des Kursverlaufes der grössten und liquidesten Kryptowährungen und -tokens. Ausserdem wurde der Crypto Market Index 10 auch als investierbarer Benchmark designed. Um die Preisfindung im Index möglichst breit abzusichern, werden Kurse der Kryptowährungen und -tokens von vielen verschiedenen Kryptobörsen benutzt. Der Crypto Market Index 10 wurde am 30. Dezember 2016 auf 1000 Punkte normiert und wird seit dem 9. Januar 2018 fortlaufend berechnet.

SIX betreibt erfolgreich seit Jahren ein Schweizer Indexgeschäft und misst für verschiedene Asset-Klassen wie Aktien, Anleihen und auch Immobilien das Marktgeschehen. Viele der an der SIX handelbaren Finanzinstrumente finden auch in einem der über 1500 Indizes eine Berücksichtigung. Heutzutage spiegeln Indizes nicht nur das Marktgeschehen, sondern sind Basis für weitere Finanzinstrumente.

Neben den offiziellen SMI, SPI und SBI Indizes berechnet SIX als sogenannter Calculation Agent auch im Auftrag von Kunden Indizes. Die Kunden schätzen die Kompetenz bei der Indexentwicklung sowie den zuverlässigen und professionellen Betrieb, den SIX gewährleistet. Kundenindizes tragen keinen SIX Brand im Namen. Die Methodik wird zudem stärker vom Kunden beeinflusst und muss nicht dem Standard von SIX entsprechen. Trotzdem setzt SIX bei Customized Indizes die gleichen Qualitätsmassstäbe an wie bei seinen eigenen Indizes.

Kryptowährungen als Datenquelle

Das Thema Kryptowährungen verfolge ich schon seit einigen Jahren auf Grund der neuartigen Technologie, Unabhängigkeit von zentralen Institutionen und aus Datensicht. Als langjähriger Entwickler von Finanzindizes versuche ich entweder

neue Algorithmen bei der Indexkonstruktion anzuwenden oder mich auf neuartige Daten zu stützen.

Während es in den letzten Jahren auf Kundenseite für solch einen Index noch keinen Bedarf gab, änderte sich das im Jahr 2017. Von Kundenseite wurde ich angesprochen, Krypto-Coins und -Tokens abzudecken und die Brücke von der Welt der Kryptowährungen zu traditionellen Finanzinstrumenten zu schlagen. Es war ein innovatives und herausforderndes Projekt, da die Daten im Gegensatz zu unseren bisherigen Indizes nicht aus dem Handelssystem von SIX kommen. Konkret lagen die Herausforderungen in den Bereichen Entwicklung des Indexkonzepts zusammen mit dem Kunden Crypto Finance AG, Software Engineering sowie Etablierung einer Infrastruktur.

Identifikation der Preisquellen für Kryptowährungen

Das Ziel war, einen diversifizierten Hauptindex zu entwickeln, der die Renditeentwicklung der grössten und liquidesten Kryptowährungen von verschiedenen Kryptobörsen widerspiegelt. Die Konstruktion des Index soll den Einsatz als Basiswert für Finanzprodukte wie Indexfonds und Strukturierte Produkte ermöglichen. Im Gegensatz zu klassischen Finanzinstrumenten gibt es bei Kryptowährungen keine zentrale Preisquelle



Christian Bahr ist seit dem 1. September 2016 als Head Market Data & Analytics für die börseneigenen Indizes und die Markt- und Referenzdaten Services von SIX Swiss Exchange AG zuständig. Vor seinem Wechsel zur Schweizer Börse war Christian Bahr 14 Jahre in verschiedenen Positionen bei STOXX Ltd. und Dow Jones Indexes tätig, wo er eine globale Indexfamilie ausrollte und weitere spezialisierte Indizes für strukturierte Produkte, ETFs und Benchmarking Zwecke entwickelte. Während dieser Zeit war er bereits für die Indizes von SIX Swiss Exchange zuständig und Mitglied der Aktien- und Bondindex Kommissionen. Christian Bahr hat an der Universität Hannover in Wirtschaftswissenschaften Abschlüsse als Diplom-Ökonom und Dr. rer. pol. erworben.

Kontaktadresse:
Dr. Christian Bahr
Head Market Data & Analytics
SIX Swiss Exchange
Pfungstweidstrasse 110
CH-8021 Zürich
Tel: +41 58 399 2884
E-Mail: christian.bahr@six-group.com

und auch keine Schlussauktionen. Es war daher notwendig, einen Algorithmus zu entwickeln, der pro Kryptowährung unterschiedliche Preisquellen und Währungspaare berücksichtigt.

Anhand von verschiedenen Iterationen in Excel und Python auf einem Standardlaptop sowie in Absprache mit dem Kunden wurde die folgende Methodik konzipiert: Quartalsweise Auswahl der Kryptowährungen anhand der Marktkapitalisierung und als Preis den volumengewichteten Durchschnittspreis von verschiedenen Kryptobörsen über eine Stunde. Gerade dieser letzte Aspekt unterscheidet den Index für die Crypto Finance AG von anderen Bitcoin- oder Alt-Coin-Indizes und ermöglicht eine echte Preisfindung für eine Kryptowährung sowie gute Voraussetzungen für die Nachbildung durch einen Fonds. Wie es bei Indizes üblich ist, erfolgt die Auswahl der Währungen und der verwendeten Kryptobörsen regelbasiert.

Unerwartete Herausforderungen und technologische Lösungen

Nachdem das Konzept stand, musste es in die Produktion überführt werden. Im Hochsicherheitsumfeld von SIX sind viele Websites und Ports standardmässig gesperrt. Ein nicht zu unterschätzender Aufwand entstand im Zusammenhang mit individuellen Sondergenehmigungen für den Zugriff auf die APIs der Kryptobörsen und im Aufsetzen von dedizierten Servern für die Etablierung der neuen Calculation-Infrastruktur. Gerade wenn es um komplett neue Datenquellen oder Algorithmen geht, sollte diesen letzten beiden Themen ausreichend Zeit eingeräumt werden.

Trotz den Herausforderungen gelang es dem Team von Grund auf ein neues System zu erstellen, welches in ein paar Monaten produktionsreif war. Die sehr enge, agile Zusammenarbeit zwischen

Business und IT, aber sicher auch die gewählten Technologien wie Scala und das Akka Toolkit haben massgeblich zur schnellen Umsetzung beigetragen. Das Akka Toolkit ermöglichte es, sich auf die Geschäftslogik zu konzentrieren. So gingen der Crypto Market Index 10 und dessen Subindizes am 9. Januar 2018 live.

Gerade in diesem teilweise hochvolatilen und wachsenden Umfeld der Kryptowährungen ist es unseren Kunden wichtig, Indexdienstleistungen von einem verlässlichen Partner zu haben. SIX plant den Bereich der Customized Indizes auszubauen und hat mit diesem Projekt gezeigt, dass sie die Kompetenz besitzt, auch mit alternativen Datenquellen innovative Indexkonzepte erfolgreich umzusetzen.



impressum

readme Nr. 39/März 2018

Herausgeber:
UZH Alumni Informatik

Chef-Redaktor:
Dr. Kornél Szabó

Redaktion:
Andri Färber
Nicola Fantini
Bruno Kaiser
Dr. Esther Kaufmann

Nathan Labhart
Carl Oliver
Esther Rölli

Adresse:
UZH Alumni Informatik
Schönberggasse 15a, 8001 Zürich
Homepage: www.alumni.ch

Redaktionsadresse:
readme@alumni.ch

Redaktionsschluss Nr. 40/Sept. 2018
26. August 2018

Titelbild:
pixabay.com

Auflage:
922 Exemplare

Produktion und Druck:
ETIDRUCK AG, Hausen am Albis

Fondueplausch im Le Dézaley

Bereits zum 20. Mal trafen wir Alumni Informatiker der Universität Zürich uns am Dienstag 5. Dezember zu unserem traditionellen Fondueplausch im Restaurant Dezaley im Zürcher Niederdorf. Ein volles Haus und eine gute Stimmung prägten den Jubiläumsabend. Ob Rückblick auf das vergangene Jahr, Veränderungen in Job und Familie, autonome Fahrzeuge oder Datenschutz und Sicherheit, es gab wie immer viel zu diskutieren und der Abend war eigentlich wiederum zu kurz dazu. Erneut konnten wir auch einige ICU-Mitglieder bei uns begrüßen und hatten eine gute Durchmischung

von jungen, am Anfang ihrer Laufbahn stehenden Informatikern und erfahrenen Alumni. Auch wurde das Wiederaufnehmen der Business Lunches angesprochen. Als Resultat wurden 2018 bereits wieder 3 Business Lunches durchgeführt. Wir hoffen, noch weitere in diesem Jahr zu haben. Interessenten für Kurzvorträge sind immer herzlich willkommen. Meldet Euch bei Anja Cavigilli oder Nicola Fantini.

Mit Waadländer Plättchen, Fondue mit Kirsch und Wein bis zum Fruchtsalat, Kaffee und Grappa wurde der Abend kulinarisch begleitet.

Für die grosszügige Unterstützung des Fondueplauschs durch die Firma Avaloq Evolution AG möchten wir uns ganz herzlich bedanken. Auch durften wir weitere Vertreter von Sponsoren der Alumni an unserem Fondueplausch begrüßen.

2018 findet selbstverständlich unser nächster Fondueplausch statt. Wir haben bereits wieder den Dienstag 11. Dezember 2018 entsprechend reserviert. Also bitte schon in Eure Agenda eintragen und frühzeitig anmelden!



Abendvortrag von Chat Wacharamanotham: «How do we read statistics?»

«Traue keiner Statistik, die du nicht selbst gefälscht hast» – dieses Bonmot wird statistisch gesehen am häufigsten Winston Churchill zugeschrieben. Aber eben, kann man dieser Statistik trauen? Vielleicht ist eine Statistik gar nicht absichtlich gefälscht, sondern wird nur falsch gelesen. Wie genau man statistische Daten – Texte und Grafiken – liest und welche Rückschlüsse dies auf das Verstehen und Interpretieren, aber auch auf das Verfassen von Statistiken ermöglicht, war Kernthema von Chat Wacharamanothams Vortrag, den er vor rekordverdächtigen 21 Zuhörerinnen und Zuhörern am Institut für Informatik hielt.

Experimente mit Eye-Trackern, die aufzeigen, dass manche Personen statistische Angaben beim Lesen unbewusst überspringen sowie Projekte wie AnnoTracer (welches die Textmarkierungen von verschiedenen Leserinnen und Lesern aggregiert, um die wichtigsten Daten aus statistischen Papers zu erkennen) und LocusStat (in welchem Grafiken mit Simulationen angereichert werden, um einfacher ein mentales Modell



zu erlangen), helfen Chat und seinen Mitarbeitenden, zu verstehen, wie wir Statistiken lesen... und wie Computer uns dabei helfen können.

Nach unterhaltsamen 30 Minuten und einer angeregten Diskussion wartete vor dem Hörsaal ein reichhaltiger Apéro mit Sandwiches, Canapés, Spiesschen, Wein,

Soft und diversen Desserts auf Referent und Publikum. Statistisch gesehen waren die Sandwiches am wenigsten beliebt, aber um diese Aussage zu überprüfen, hätten die geneigte Leserin und der geneigte Leser selber anwesend sein müssen. Wer nicht kommen konnte, hat auf jeden Fall etwas verpasst – kulinarisch wie auch vortragstechnisch.



Sind ICOs Stolperstein oder Chance?

Ralph Mogenicato und Roger Darin

Der Begriff Initial Coin Offerings (ICO) ist eines der am häufigsten verwendeten Schlagwörter im Bereich Bitcoin, Blockchain & Co. Als Instrument für die Gründungsfinanzierung scheint es die traditionellen Finanzierungsvehikel zu verdrängen – man könnte sogar von disruptieren sprechen. Doch der aktuelle Boom zeigt ebenso, dass dieses Instrument auch Schwächen hat und der Regulator bereits genau hinschaut. Als Fazit darf gesagt werden, dass ein ICO die Grundgesetze der Startup-Finanzierung nicht auf den Kopf stellt: Ein gutes Team mit einer guten Idee und harter Arbeit sind genauso wichtig wie das schnelle Geldeinsammeln à la Tezo.

Kaum zwei Wochen, nachdem in der Schweiz die Finanzmarktaufsicht (FINMA) einen Leitfaden für Initial Coin Offerings (ICO) veröffentlicht hatte, kam aus Übersee die Botschaft, dass die amerikanische Börsenaufsichtsbehörde (SEC), welche für den Wertschriftenhandel zuständig ist, Dutzenden von Firmen, die in ICOs involviert waren, eine Vorladung zugestellt hat. Unter den Angeschriebenen befinden sich nicht nur Technologieunternehmen, die selbst ein ICO in die Wege geleitet haben, sondern auch Investoren, Berater und Marketingverantwortliche. Insgesamt seien etwa 80 Personen von dieser härteren Gangart in Bezug auf ICOs betroffen.

Doch während sich Regulatoren über den Umgang mit diesen neuen Technologien noch uneins sein mögen, stellt sich für gewiefte Investoren die Frage nach den Auswirkungen auf den eigenen Investitionsprozess.

Angel Investoren als wichtiger Teil des Startup Eco Systems

Dabei konzentrieren wir uns in dieser Betrachtung auf Angel Investoren, welche traditionell in der ersten Wachstumsphase eines Unternehmens dazukommen und somit in der Regel die ersten «fremden» Investoren sind: Personen, die nicht aus dem direkten Familien- und Freundeskreis der Firmengründer stammen.

Oft sind Angel Investoren (auch Business Angels genannt) selbst erfahrene Unternehmer und organisieren sich in Gruppen, um den Investitionsprozess sowohl für sich selber als auch für die Startups möglichst schlank zu halten. Eine dieser Vereinigungen ist der Swiss ICT Investor Club (SICTIC); mit über 170 Mitgliedern nicht nur die grösste Business Angel Organisation in der Schweiz, sondern auch klar fokussiert auf Tech Startups.

SICTIC organisiert über die ganze Schweiz verteilt mehr als 10 Events pro Jahr, um einerseits den Startups eine Plattform zu geben und andererseits den Business Angels einen direkten Kontakt mit ausgewählten Investitionsmöglichkeiten zu ermöglichen. Anders als gewinnorientierte Business Angels Organisationen finanziert sich SICTIC dabei lediglich aus den einsteigerfreundlichen Jahresbeiträgen der Business Angels und nimmt keinerlei Kommissionen oder Gewinnbeteiligungen bei Investments. Die Nachhaltigkeit dieses Modells haben auch namhafte Firmen erkannt, die SICTIC mit Sponsorbeiträgen unterstützen.

ICO als neue Form der Gründungsfinanzierung

ICOs sind die Fortsetzung eines Trends, der mit Crowdfundingplattformen wie Kickstarter seinen Anfang nahm. Innovative Jungunternehmer und Enthusiasten

suchten nach neuen Finanzierungsformen, um noch zu entwickelnde Produkte auf den Markt bringen. Dabei war es den Initianten zwar wichtig, die Kontrolle über das Projekt behalten zu können, doch andererseits verstanden sie, dass auch die Geldgeber auf irgendeine Art entschädigt werden müssen.

Diese Trennung zwischen wirtschaftlichem Erfolg und Kontrolle über Unternehmen zeigt die sich verschiebenden Machtverhältnisse zwischen Kapitalgebern und Gründern auf. Man denke an Unternehmen wie Facebook, wo der Firmengründer Mark Zuckerberg durch Stimmrechtsaktien eine überproportionale Kontrolle über das Unternehmen hat.

Nun konnte sich nicht jeder Jungunternehmer so erfolgreich gegen die Interessen der Risikokapitalgeber durchsetzen wie Zuckerberg. In ihrer Rolle als Türhüter zum Kapital konnten letztere in der Regel ihre eigenen Interessen durchsetzen und sich sowohl Kontrolle als auch einen bedeutenden Anteil am wirtschaftlichen Erfolg sichern.

Das Aufkommen der ICOs hat für Startups den Zugang zum notwendigen Startkapital weit geöffnet. Anstatt Aktienanteile werden nun beispielsweise künftige Umsatzprozente oder bestimmte Nutzungsprivilegien verkauft. Die Startups

sind diesbezüglich sehr kreativ. Manche treiben es soweit, dass die Risikokapitalgeber für ihr Investment kaum viel mehr als einen warmen virtuellen Händedruck bekommen. Auch die Investoren sind nicht unschuldig, denn im Hype um Bitcoin & Co. wollen alle auf diesen Zug aufsteigen, um schnell gutes Geld zu machen. Tatsächlich haben im letzten Jahr von 902 untersuchten ICOs nur 760 genügend Geld bekommen, um dann ihre Geschäftstätigkeit auch aufnehmen zu können. Und von diesen 760 sind 276 eingegangen, entweder weil die «dynamischen Jungunternehmer» sich mit dem Erlös abgesetzt haben oder die Mittel verbrannten, ohne im Gegenzug dafür etwas zu liefern.

ICO als heiliger Gral für Startups

In anderen Worten: Initial Coin Offerings vereinfachen zwar das Leben der Jungunternehmen, entbinden Angel Investoren aber nicht von ihren Hausaufgaben. Dazu gehören erstmal die gleichen Fragen, wie bei jedem anderen Startup:

- Wie ist die Qualität der Gründer und des Teams
- Welches Problem löst das Unternehmen
- Wie ist die Qualität der bisher produzierten Software
- Wie gross ist der Markt, wer sind die Kunden, wie werden diese erreicht
- Was ist das Businessmodell (also wie verdient man Geld)
- Was ist die «Time to Market»

Insbesondere in der schnellen Welt der ICOs kann natürlich besonders beim letzten Punkt (Time to Market) deutlich an Zeit gewonnen werden, wenn damit von Anfang an der Kapitalbedarf des gesamten Aufbaus in einer einzelnen Transaktion abgedeckt werden kann, anstatt über Jahre hinweg Management Ressourcen für mehrere separate Finanzierungsrunden zu beanspruchen.

Doch mit dem Geldsegen steigt möglicherweise auch das Risiko, dass das Projekt scheitert. Dies mag auf den ersten

Blick nicht sonderlich intuitiv erscheinen, bis man sich vergegenwärtigt, dass jede Finanzierungsrunde auch eine Form der Validierung darstellt. Fallen diese wertvollen Feedback-Loops weg, wird ein Scheitern erst offenbar, wenn der letzte Cent aufgebraucht ist. Im Gegensatz zu einer traditionellen Finanzierung kann dieser letzte Cent unter einem Haufen von Hunderten Millionen weiteren Cents und Franken begraben und erst nach Jahren aufgebraucht sein.

Ausserdem schaltet das Vorhandensein finanzieller Mittel im (scheinbaren) Überfluss natürliche Filter aus. Insbesondere in den Innovationszentren von Grossunternehmen kommt es daher immer

wieder vor, dass am Schluss eben doch nichts Brauchbares produziert wird - man musste sich ja nie wirklich entscheiden, sondern konnte stets sowohl-als-auch. Bei der Entwicklung von neuen Diensten und Produkten nie Nein sagen zu müssen, endet in überbeurteilten und am Markt vorbei entwickelten Leistungen.

Des Weiteren bringen ICOs in vielen Rechtsfragen inhärente Unsicherheit mit sich. Zu den Empfängern der eingangs erwähnten Vorladungen der SEC gehört auch ein Investment Fund von Michael Arrington, dem Gründer von TechCrunch. Er zeigte sich davon mehr als überrascht, als er sagte, dass er mit den besten Anwaltskanzleien des Landes



Als Roger Darin (SICTIC Advisor) mit nur 17 Jahren sein erstes Startup gründete, demonstrierte er nebst einer unternehmerischen Ader auch seinen angeborenen Enthusiasmus. Obwohl er dann schliesslich eine traditionelle Karriere im Investment Banking verfolgte – was ihm erlaubte, in grossen Finanzzentren wie Singapur, Tokio und Sydney zu arbeiten – bewahrte er stets seine Liebe zur Informationstechnologie (seine ersten Seminare dazu gab er im Alter von 14 Jahren im lokalen Computerclub, wo er mit Abstand das jüngste Mitglied war). Diese Vorliebe kombiniert er heute mit seinen beruflichen Erfahrungen im Handel und Risikomanagement sowie einer gesunden Portion Kreativität. Nachdem er die letzten zwei Jahre als Product Manager beim Aufbau einer Plattform für Vermögensverwalter mitwirkte, wechselte er zu Lakeside Partners, um deren Anstrengungen beim Aufbau eines umfassenden Ökosystems rund um die Blockchain zu unterstützen. Zudem ist Roger Darin beim Swiss ICT Investor Club im Advisory Board tätig.

Kontaktadresse:
Roger Darin
Principal
Lakeside Partners AG
Gotthardstrasse 26
CH-6300 Zug
Tel: +41 79 421 52 43
E-Mail: roger@lakeside.partners



Ralph Mogenicato, ein Ifl-Alumnus mit Abschluss 1990 und Beirat des Ifl, ist seit über mehr als 30 Jahren in der Finanz-, Consulting- und IT-Branche in der Schweiz, Deutschland, Österreich und Singapur tätig. Er ist Mitbegründer und war CEO bei der Schweizer Beratungsgesellschaft Synpulse (ehemals Solution Providers) mit über 350 Mitarbeitern. Heute ist er Unternehmer, Senior-Berater, Vorstandsmitglied und Angel Investor bei Tech Start-ups, Lehrbeauftragter an der Universität Zürich und Dozent an der Fachhochschule Kaleidos sowie Gastdozent am IFZ, Universität St. Gallen und Swiss Finance Institute. Er ist zudem Verwaltungsrat bei der CREALOGIX Holding AG und Assepro AG, Vizepräsident des Schweizer ICT Investor Club (SICTIC) und Mitglied verschiedener Fintech-Verbände in der Schweiz, England und Asien. Sein Startup Portfolio umfasst aktuell 15 Firmen, u.a. Swiss Diamond Coin, Starmind, unblu, Sonect, APIAX, esurance oder IMburse.

Kontaktadresse:
Ralph Mogenicato
Vice President
Swiss ICT Investor Club
Stockerstrasse 44
CH-8002 Zürich
Tel: +41 79 356 99 11
E-Mail: ralph@sictic.ch



NEUE IDEEN? WIR ENTWICKELN DIE SOFTWARE DAZU.

MIT ADN OVUM ALS SOFTWARE-PARTNER ERLANGT IHRE BUSINESS-IDEE SCHNELL DIE NÖTIGE MARKTREIFE. WIR UNTERSTÜTZEN SIE VON DER IDEENFINDUNG BIS ZUR PRODUKTLANCIERUNG UND MACHEN SIE BEI DER MARKEINFÜHRUNG ZUM FIRST MOVER. NEHMEN SIE FRÜHZEITIG MIT UNS KONTAKT AUF – SELBST WENN DIE BIG IDEA NOCH NICHT SO BIG IST. ADN OVUM INFORMATIK AG, RÖNTGENSTRASSE 22, 8005 ZÜRICH, SCHWEIZ, TELEFON +41 44 272 61 11, WWW.ADN OVUM.CH

zusammengearbeitet habe und diese penibel darauf geachtet hätten, dass jedes Kreuzchen in allen erdenklichen Böxchen gesetzt sei.

Zu den rechtlichen Herausforderungen beim ICO selber kommt die Rechtsunsicherheit bei gewissen Corporate Events: Es ist heutzutage jedem KV-Lehrling klar, wie die Kapitalerhöhung einer Aktiengesellschaft abgewickelt werden muss,

doch selbst gelernte Juristen sind sich uneins darüber, wie solche Transaktionen in gewissen ICO-Strukturen ablaufen müssen, wodurch weitere Finanzierungsrunden verunmöglicht werden mögen.

Trotz der vielen Warntafeln auf dem Weg ins Crypto Valley soll nun aber die Schlussfolgerung nicht lauten, die beschwerliche Reise sei das Ziel nicht wert. Die neuen Finanzierungsformen haben durchaus

ihre Daseinsberechtigung und diverse SICTIC Investoren sammeln nun erste Erfahrungen in ICOs. Wie so oft in der Geschichte des Fortschritts werden wohl diejenigen Projekte von Erfolg gekrönt sein, welche geschickt die Vorteile der neuen mit den Vorteilen der alten Welt kombinieren, um bestehende Schwächen auszumerzen. Genauso wie beim Studium gilt auch hier: «Fertig gelernt» gibt's nicht.

Unsere Sponsoren und Partner

Das vielfältige Angebot der UZH Alumni Informatik wäre ohne die tatkräftige und langjährige Unterstützung unserer Sponsoren und Partner nicht möglich. Generell ermöglichen sie uns, unsere Alumni-Aktivitäten in der gewohnten Art und Weise durchzuführen, sei es für Inserate im readme oder who-is-who, Events oder Emailversand. Weitere Infos sind auf unserer Website unter der Rubrik «Sponsoren & Partner» zu finden.

ADINOVUM

 **ausbildung-
weiterbildung.ch**
Das Schweizer Bildungsportal

avalog
essential for banking

 GOLDWYN PARTNERS GROUP

NSM
Engineering AG

 **PROACADEMICSAG**

Möchten Sie ebenfalls Sponsor oder Partner werden?
Nehmen Sie mit uns Kontakt auf: info@alumni.ch

Neues aus dem IfI

Prof. Dr. Abraham Bernstein, Institutsdirektor



Abraham Bernstein studierte an der ETH Zürich Informatik und promovierte am Massachusetts Institute of Technology (MIT). 2002 folgte er dem Ruf an die Universität Zürich, wo er heute Direktor des Instituts für Informatik ist. Abraham Bernsteins Forschungsinteressen beinhalten das Semantische Web, Big Data, Data-Mining, heterogene Datenintegration, Crowd Computing und das Wechselspiel zwischen sozialen sowie technischen Elementen der Informatik.

Kontaktadresse:
Prof. Dr. Abraham Bernstein
Institut für Informatik
Universität Zürich
Binzmühlestrasse 14
CH-8050 Zürich
Tel: +41 44 635 45 79
E-Mail: bernstein@ifi.uzh.ch
<http://www.ifi.uzh.ch>

Liebe Alumni

Es ist wieder mal soweit:
Wir haben zweifachen Zuwachs erhalten.

Thomas Fritz, der Nachfolger von Martin Glinz, ist bei uns angekommen. Er war ja schon mal bei uns, und nun hat er den Weg aus Vancouver wieder zu uns zurückgefunden. Thomas wird das Human-Oriented Software Engineering bei uns vertreten. Einige mögen sich vielleicht noch daran erinnern, wie er vor etwas mehr als einem Jahr in der intentionalen Presse Furore machte mit einer Art Ampelsystem. Die rote bzw. grüne Ampel signalisiert den anderen Mitarbeitenden, wann die Softwareentwickler bei ihrer Arbeit gestört werden können und wann nicht. Wir sind froh, dass Thomas wieder bei uns ist. Somit ist das Software Engineering mit Alberto Bacchelli, Harald Gall und Thomas Fritz in einer noch nie gesehenen Stärke vertreten. Der Schwerpunkt auf die Menschenzentriertheit und die Empirie ist dabei eindeutig erkennbar. Wir freuen uns auf viele schöne Forschungsergebnisse.

Wie der Schweizerische Nationalfonds neulich verkündete, dürfen wir ab diesem Sommer Ingo Scholtes als zweiten

SNF Förderungsprofessor bei uns begrüßen. Ingo entwickelt neue Methoden zur Analyse zeitgestempelter Daten zu komplexen Netzwerken. In anderen Worten: Er entwickelt Algorithmen, die Veränderungen in Netzwerken vorhersagen und überwachen können wie z.B. in sozialen Netzwerken, Firmennetzwerken, Finanztransaktionen, Analysen biologischer Interaktionen oder ähnlichem. Der besondere Beitrag von Ingo ist, dass er die Zeit als entscheidenden Faktor berücksichtigt. Er betrachtet die Netzwerke nicht als statische Objekte, sondern als sich verändernde Gebilde. Aktuelle Verfahren berücksichtigen die Semantik von zeitlichen Abläufen nicht. Ingo wird also eine neue Generation von Datenanalyseverfahren entwickeln, die genau dies berücksichtigen. Seine neuen Verfahren haben das Potenzial, unser Verständnis komplexer sozialer, technischer und biologischer Systeme zu verbessern. Diejenigen, die mich kennen, wissen, dass ich Netze (oder Graphen, wie ich sie nenne) besonders mag. Sie sind eine flexible Datenstruktur, mit der man eine Vielzahl von Tätigkeiten vereinfachen kann. Insofern freue ich mich auch persönlich auf die zukünftige Forschungszusammenarbeit mit Ingo.

Zu guter Letzt haben wir noch einen «Halbzuwachs» zu vermelden. Das Institut für Computerlinguistik, welches ja praktisch seit den Anfängen mit dem Ifl assoziiert ist, konnte Volker Delwo als Professor gewinnen. Volker ist Professor für Phonetik und Spezialist für Sprachsynthese. In der SRF-Sendung «Kulturplatz» vom 31. Januar 2018 orientierte er über die menschliche Stimme im Zeitalter der Digitalisierung. Er deckt also ein weiteres, immer wichtigeres Element in der Mensch-Maschinen-Interaktion ab.

Auch an der Forschungsfront schlafen wir nicht. So haben sich Gerd Schwabe und Burkhard Stiller den Blockchains zugewandt und eine Reihe von hochinteressanten Projekten lanciert. Gerd Schwabe geht Betrügern im Autohandel an den Kragen, zusammen mit AdNovum und unter Zuhilfenahme von Distributed Ledgers. Dank Blockchain soll sichergestellt werden, dass z.B. der Käufer und die Versicherungen gesicherte und korrekte Informationen über die Fahrzeuge erhalten. Burkhard Stiller widmet sich dem e-Voting auf Blockchain-Basis, zusammen mit Procivis. Um das Blockchainbild abzurunden, haben die beiden gemeinsam mit Kollegen aus der BWL

und der Rechtswissenschaftlichen Fakultät (RWF) einen Verbund von Professoren gegründet, der das ganze Spektrum von Blockchains und Smart Contracts beleuchtet.

Auch aus der Lehre darf ich Erfreuliches berichten. So ist unser CAS Big Data und Machine Learning erfolgreich und voll ausgebucht gestartet. Die Teilnehmenden erwarten ein abwechslungsreiches Programm mit neuen Technologien und Managementmethoden sowie rechtlichen und ethischen Überlegungen. Ich war besonders froh, am CAS auch Alumni begrüßen zu dürfen. Überhaupt zeigt sich, dass genau diese interdisziplinären Fragen viele interessieren. Unsere Vorlesung Big Data: Technology and Law, welche Studierende der WWF und RWF gemeinsam besuchen, ist auch sehr beliebt. In der Vorlesung arbeiten interdisziplinäre Teams gemeinsam an Projekten aus dem Bereich der Big-Data-Verarbeitung. So hatten wir letztes Jahr in dieser Vorlesung aus aktuellem Anlass viele Projekte, die sich mit GDPR auseinandersetzten. Ein Team fokussierte sich auf ein anderes Thema und entwickelte eine Web-Seite mit Newsletter-Angebot. Nach der Newsletter-Anmeldung

verwendete das Tool eine Reihe von Open-Source-Komponenten, um möglichst viele Informationen über den neuen Abonnenten zu erfahren. Nach dem Anmeldeprozess sendete das Tool dem neuen Abonnenten alle Informationen, zusammen mit dem Hinweis auf deren Herkunft. Ich kann nur sagen, dass einige der Teilnehmenden überrascht waren, wie viele öffentliche Informationen so im Internet rumliegen und wie sie sich miteinander kombinieren lassen.

Mit besten Wünschen
Euer Abraham Bernstein

Gaming oder Mining?

Marc Stampfli

Der Markt für Graphikkarten ist komplett ausgetrocknet, unter anderem weil die Hardware auch für Crypto-Mining eingesetzt werden kann. Der Beitrag zeigt auf, was die Marktreiber tatsächlich sind und wie es zu dieser Situation gekommen ist.



Marc Stampfli studierte Wirtschaftsinformatik an der Universität Zürich mit Abschluss im Jahre 2001, bevor er bei PricewaterhouseCoopers im Management Consulting für Informationstechnologien seine Karriere begann. Anschliessend arbeitete er in verschiedenen Positionen; zuerst für Oracle und IBM im Softwarelösungsverkauf, danach bei Colt Technology Services in leitender Funktion für das Netzwerk- und Rechenzentrumsgeschäft. Seit 2017 ist er bei NVIDIA Schweiz dafür zuständig, das Geschäft für die Schweizer Niederlassung im Bereich moderner künstlicher Intelligenz mit Deep Learning, High Performance Computing und Professional Visualization (VR/AR) aufzubauen.

Kontaktadresse:
Marc Stampfli
NVIDIA Schweiz
Technoparkstrasse 1
CH-8005 Zürich
Tel: +41 44 564 76 28
E-Mail: mstampfli@nvidia.com

GPGPUs statt GPUs

Game oder Mining? Diese Frage stellt man sich, wenn nicht genügend Chips für den Markt produziert werden können. Seit einiger Zeit haben wir die Situation, dass der Markt für GPUs, sogenannte Graphics Processing Units, v.a. im nicht professionellen Bereich ausgetrocknet ist.

Um die Situation wirklich in der Tiefe erfassen zu können, muss man zuerst verstehen, warum GPUs, welche ja eigentlich für Grafikverarbeitung gedacht sind, plötzlich so stark nachgefragt werden. Für GPUs gibt es heute unterschiedliche Anwendungen, weshalb ich lieber von General Purpose Computation on Graphics Processing Unit (GPGPU) spreche. Damit bezeichnet man die Verwendung eines Grafikprozessors für Berechnungen über seinen ursprünglichen Aufgabenbereich hinaus.

Von Single zu Multi Kernels

Die Hauptkomponente eines jeden Computers ist die CPU, die für Central Processing Unit steht. Die CPU erhält Anweisungen und führt dann Berechnungen durch. Wenn ein Prozessor nur einen Satz von Befehlen auf einmal verarbeiten kann, bedeutet das, dass er nur einen einzigen Kern hat.

Wenn ein Prozessor zwei Befehlssätze gleichzeitig verarbeiten kann, dann gilt er als Dual-Core-Prozessor. Wenn es vier Befehlssätze gleichzeitig verarbeiten kann, dann ist es ein Quad-Core-Prozessor. Je mehr Kerne ein Prozessor hat, desto mehr Befehlssätze kann er

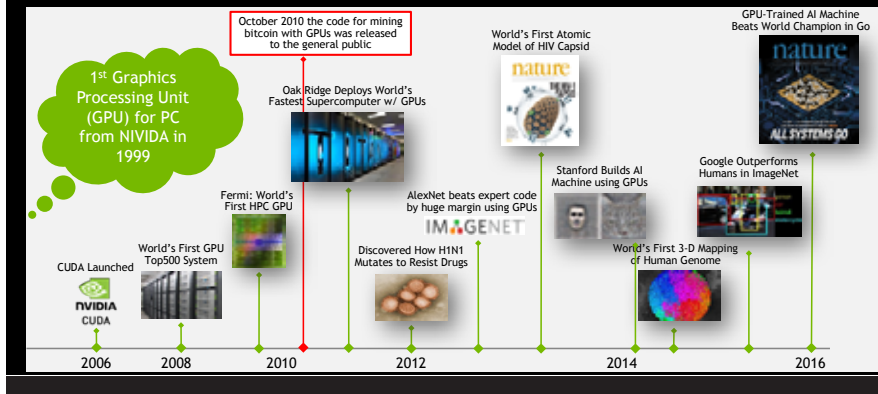
gleichzeitig verarbeiten. Auf einem Server können es durchaus 12 oder mehr Kerne sein pro CPU. Die Software muss jedoch auf Multithreading ausgelegt sein, um von der grösseren Anzahl Kerne profitieren zu können.

Im Vergleich dazu hat eine einzelne moderne GPU wie bspw. eine NVIDIA Volta V100 über 5120 Kerne. Zusätzlich ist sie im Gegensatz zur CPU auf massiv parallele Verarbeitung ausgelegt und kann parallel zusammengeschaltet werden. Im Prinzip stehen damit $n \times 5120$ Kerne zur Verfügung, theoretisch nur limitiert durch die finanziellen Möglichkeiten.

Erschliessung neuer Anwendungs-Domänen

Diese extreme Kapazität für Parallelverarbeitung wurde ursprünglich entwickelt für die Verarbeitung und Darstellung von hochauflösender 3D-Grafik in Echtzeit. Dabei kann jedes reale Objekt im virtuellen Raum mit Polygonen (typischerweise in Form eines Dreiecks) approximiert und entsprechend die Schattierung einer Fläche berechnet werden. So kann die Auflösung (oder Filigranität in der Form) eines 3D-Objekts mit der Verkleinerung der Polygone erhöht werden, bis der Mensch keine Polygone mehr wahrnimmt, sondern nur noch ein einzelnes Pixel (Picture Element). Via linearer Algebra und Verwendung von Matrizen und Vektoren erfolgt die Beschreibung oder eben Berechnung dieser 3D-Objekte und Welten. Eine GPU ist darauf optimiert, lineare Algebra mit Matrizen und Vektoren parallel zu verarbeiten.

HISTORY OF ACCELERATED COMPUTING WITH GPU



Deshalb wurden GPUs ursprünglich vor allem für Computerspiele auf Grafik-Workstations eingesetzt (NVIDIA GPU, 1999). Mit dem Schritt von NVIDIA, eine Softwareschnittstelle (CUDA, 2006) zu entwickeln, welche erlaubte, die GPU auch für andere Zwecke als Grafik einzusetzen, konnte ein ganz neuer Markt erschlossen werden. Zuerst wurden die GPUs für wissenschaftliche Simulationen (Moleküle, Flüssigkeiten, Strömungen uvm.) angewendet. Die ersten Supercomputer begannen GPUs im Jahr 2008 einzusetzen. Heute gibt es kaum einen neuen Supercomputer, der keine GPUs von NVIDIA einsetzt.

Kickstart für Bitcoin-Mining

2010 wurde das erste Mal eine Software veröffentlicht, welche erlaubte, Bitcoins auf GPUs zu minen. Man konnte zu diesem Zeitpunkt noch mit einer einzelnen GPU erfolgreich minen. Die Schwierigkeit, um erfolgreich Bitcoin zu minen, stieg aber die Monate und Jahre darauf erheblich. Und die Miner begannen, ganze Cluster mit Tausenden von Grafikkarten auszurüsten. Da der Bitcoin Preis noch viel tiefer war, wurden vor allem günstige Gaming-Grafikkarten verwendet. Der Markt für Gaming-Grafikkarten begann sich zu verknappen. Die Entwicklung von spezieller Mining-Hardware für Bitcoin hat dabei die Situation nicht entspannt, da zur gleichen Zeit verschiedene

neue Kryptowährungen und Blockchain-Anwendungen auf den Markt kamen, welche zu klein waren für spezialisierte ASICs (Application Specific Integrated Circuit).

Zusätzlich wurden zwischen 2012 und 2014 das erste Mal GPUs verwendet, um künstliche neuronale Netzwerke mit mehreren Schichten zu berechnen. Moderne künstliche Intelligenz mit Deep Learning war geboren. Es begann eine kambrische Explosion von KI-Anwendungen aufgrund der tiefen Kosten und massiven Rechenkapazität, welche nun mit GPUs zur Verfügung stand. NVIDIA wurde innert kürzester Zeit zum dominanten Player am Markt für moderne künstliche Intelligenz mit Deep Learning. Heute wird der Grossteil von Anwendungen moderner künstlicher Intelligenz auf GPUs und Software von NVIDIA entwickelt, wobei sämtliche Standard Deep Learning Frameworks unterstützt werden.

Wer kauft die GPUs

Verschiedene Markttreiber wie ein stark wachsender Computerspielermarkt, neue wissenschaftliche Anwendungen und Deep Learning beschleunigt durch GPUs liessen nicht mehr viel Handlungsspielraum für Mining-Hardware. Der Markt für die günstigeren Modelle von Grafikkarten begann auszutrocknen, während auf der anderen Seite der Markt für neue

Anwendungen mit teureren Tesla-Karten florierte. Dies ging so weit, dass die Verfügbarkeit für Computerspieler über Restriktionen und Rationierung sichergestellt werden musste. Es gibt nur beschränkte Produktionskapazität am Markt und die grosse Menge an Computerspielern durfte man nicht verärgern. Im Moment können deshalb pro Person nur maximal zwei günstige GeForce-Grafikkarten bestellt werden. Dies war notwendig, um sicherzustellen, dass jeder Computerspieler auch wirklich seine Grafikkarte erhält. Auf der anderen Seite sind neuere Tesla-Grafikkarten (z.B. P100 oder V100) verfügbar, welche dediziert für Cluster-Anwendungen gedacht sind und bereits vermehrt für Crypto-Mining eingesetzt werden. Die Rechnung geht aufgrund der Kurse der Kryptowährungen und der Möglichkeit, doch genügend (jedoch teurere) Karten zu erhalten, trotzdem auch für die Miner auf. Denn Warten ist keine Option, der Preis könnte auch jederzeit fallen und dann könnte man die Karten immerhin noch für andere Zwecke einsetzen.

Tod dem Passwort – Es lebe das Passwort

Adrian Bachmann

Das Passwort lebt immer noch

Schon bereits vor einigen Jahren kündigten die Medien (siehe z.B. [1]) aber auch Fachkreise den Tod von Passwörtern an. Biometrie in allen Facetten (z.B. Fingerabdruck, Iris, Handvenen, Herzrate, Stimme) ist nur ein Beispiel, welches den nahen Tod herbeiführen sollte. Jahre später hantieren wir auch in Zeiten von Blockchain und Kryptowährungen nach wie vor täglich mit Passwörtern. An der Situation hat sich dabei wenig geändert: Jeder Nutzer verfügt über unzählige Accounts und es werden immer mehr. Ein jeder dieser Accounts möchte dabei mit einem Passwort abgesichert werden. Mal mindestens 8 Zeichen, mal maximal 8, mal mindestens mit einer Ziffer und einem Sonderzeichen, mal garantiert ohne Sonderzeichen und manchmal auch ohne jegliche Vorgaben. Dabei den Überblick nicht zu verlieren, ist nahezu unmöglich. Und so kommt es wie es kommen muss: Nutzer verwenden wo immer möglich das gleiche Passwort oder variieren dieses nur geringfügig. Für böse Buben ein gefundenes Fressen. Da hilft es auch wenig, dass Umfragen zufolge 98% der Hacker keine Skimaske vor dem Computer tragen [2]. Nur was kann der einzelne Nutzer tun, wenn die gefühlten 200 benutzten Accounts nach wie vor nach einem Passwort lechzen? Um es vorweg zu nehmen: Lösungen zur Entmachtung des Passworts sind in Sicht, dürften aber noch etwas Zeit beanspruchen. Es gilt daher praktikable Lösungen für das momentane Passwortchaos zu finden.

Das Account 1x1 für Nutzer

Mit den nachfolgenden zwei Grundregeln lässt sich das Risiko eines Account-Missbrauchs massgeblich senken und den Komfort für den Nutzer sogar erhöhen.

1. Nutze pro Dienst ein eigenes, sicheres Passwort. Kein Passwort Recycling! Nein, wirklich nicht! Die Nutzung eines sicheren Passwortsafes (z.B. Keeypass [3] oder lastpass [4]) ist hierfür ab einer bestimmten Anzahl Accounts zwingend empfohlen. So dürfte es auch kein Problem sein, jeweils automatisch generierte, starke Passwörter zu verwenden, da man sich diese aller Voraussicht nach nicht mehr merken kann und jeweils aus dem Safe holen muss. Eine Mehrfachverwendung des gleichen Passworts, vielfach in Kombination mit der eigenen E-Mail-Adresse als Benutzername, eröffnet Kriminellen Tür und Tor, um nach einem erfolgreichen Angriff auf einen Dienst weitere Dienste eines Nutzers zu missbrauchen. Im 2017 wurden über 90'000 Accounts und deren Passwörter von Schweizer Internetdiensten entwendet [5, 6]. Ob Du selber davon betroffen bist, kann über eine Online-Abfrage bei der Melde- und Analysestelle des Bundes (MELANI) festgestellt werden [7]. Ohne Passwort Recycling kann man solchen Account-Diebstählen deutlich entspannter entgegenblicken, da dann nur der jeweilig spezifische Account betroffen ist, nicht noch mutmasslich viele weitere persönliche Accounts plötzlich auch gefährdet sind und sich somit ein abenderfüllendes Passwortwechseln aufdrängt.
2. Nutze wo immer möglich eine starke bzw. 2-Faktor Authentisierung (z.B. SMS/mTAN, OTP-App, FIDO-Device wie YubiKey) zur weiteren Absicherung Deines Accounts. Damit lässt sich der Schutz massgeblich erhöhen. Trotz Absicherung mit einem weiteren Faktor wäre es aber ein Irrtum anzunehmen, dass Regel Nr. 1 damit seine Bedeutung verliert.

Immer öfter bieten Internetdienste inzwischen auch die Nutzung eines vertrauenswürdigen und sicheren Identity Providers (IdP) wie Google, Microsoft oder Facebook anstelle eines lokalen Accounts an. Dies ist eine komfortable Möglichkeit, die Anzahl Accounts zu reduzieren, wobei der verwendete IdP-Account dabei zwingend über eine starke Authentisierung abgesichert sein sollte. Es ist damit zu rechnen, dass die Bedeutung von Identity Provider künftig stark zunehmen wird, was auch aktuelle, nationale Initiativen im Umfeld von eID, SwissID, SwissPass, etc. zeigen.



Dr. Adrian Bachmann studierte Wirtschaftsinformatik an der Universität Zürich und verfasste dort auch seine Dissertation zum Thema Datenqualität im Software Engineering Prozess. Nach einigen Jahren im IT Projekt- und Risikomanagement bei einer grösseren Schweizer Bank berät er seit 2011 seine Kunden in Themen der Informationssicherheit und leitet entsprechende Projekte.

Kontaktadresse:
Dr. Adrian Bachmann
Partner, IT Security Consultant
TEMET AG
Basteiplatz 5
CH-8001 Zürich
Tel: +41 79 464 01 46
E-Mail: adrian.bachmann@temet.ch
<http://www.temet.ch>

Passwort ja – aber sicher!

Offensichtlich werden wir noch einige Zeit mit Passwörtern umgehen müssen. Dabei stellen nebst recycelten insbesondere schwache Passwörter ein grosses Sicherheitsproblem dar. Betrachten wir die 20 am häufigsten verwendeten Passwörter in der Schweiz, so ergibt sich eine Liste des Schreckens (Stand 02.03.2018) [8]:

1. 123456
2. 123456789
3. 12345678
4. 1234
5. 12345
6. 111111
7. 1234567
8. hallo
9. abc123
10. password
11. qwertz
12. passwort
13. 1234567890
14. 666666
15. soleil
16. sommer
17. 123123
18. daniel
19. blabla
20. andrea

Darüber hinaus sind in der Schweiz offenbar besonders Jahrgänge und Postleitzahlen in Passwörtern beliebt. Insbesondere die Zahlen 12, 01, 11, 14, 13, 10, 99, 77, 69 und 22 scheinen es den Schweizer Nutzern angetan zu haben.

Sichere Passwörter sollten nicht nur mindestens 8 Zeichen, sondern auch eine gewisse Komplexität aufweisen. Wörter, Namen oder Tastaturmuster sind dabei möglichst zu vermeiden. Mit der Nutzung eines Passwortsafes lassen sich für jeden genutzten Dienst rasch und unkompliziert sichere Passwörter erzeugen, verwalten und bei Bedarf abrufen inkl. automatischem Abfüllen in die Login-Maske der Internetdienste. Es besteht also keine Notwendigkeit, sich unzählige, aus einem Buchstaben-, Zahlen-, und Sonderzeichensalat zusammengesetzte, sicherere Passwörter merken zu müssen.

Der Mensch als Schwachstelle

Es ist offenkundig, dass nicht (nur) Passwörter ein Problem darstellen, sondern vor allem die Komponente Mensch. Unser Umgang mit Passwörtern stellt Sicherheitsspezialisten seit Jahren vor Herausforderungen und motiviert dazu, alternative Verfahren und Lösungen zu suchen. Das regelmässige Ändern oder

Minimalvorgaben bezüglich Komplexität sind nur zwei Beispiele, die dazu führen sollen, dass Passwörter (vermeidlich) sicherer werden sollen. In der Praxis zeigt sich dafür, dass z.B. Post-it Zettelchen dem Nutzer als Gedankenstütze dienen und somit solche Passwort-Regeln das Risiko eines erfolgreichen Account-Missbrauchs gar noch erhöhen.

Lasst Euch von diesem Artikel inspirieren und ändert Euer Passwort-Verhalten noch heute. Die Einrichtung eines Passwortsafes dauert nur wenige Minuten, erspart das unzählige Anklicken von «Passwort vergessen»-Links und dient der massgeblichen Verbesserung der Account-Sicherheit.

Tot dem universal, überall verwendeten, schwachen Passwort – es lebe das sichere, spezifische Passwort und dieses wo immer möglich in Kombination mit einer starken Authentisierung.

PS: Kurz vor dem GzD dieser readme Ausgabe wurde im c't 07/18 das Leitthema «Vergessen Sie Passwörter!» behandelt. Dabei werden weitere Punkte im sicheren Umgang mit Passwörtern diskutiert und unter anderem auch 15 Passwortmanager einem Test unterzogen. Lektüre uneingeschränkt empfohlen! [9]

Referenzen

- [1] <https://www.tagesanzeiger.ch/digital/internet/Tod-dem-Passwort-/story/26979882>
- [2] <http://www.der-postillon.com/2012/01/umfrage-98-prozent-aller-hacker-tragen.html>
- [3] <https://keepass.info>
- [4] <http://www.lastpass.com>
- [5] <https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/passwoerter-von-21000-e-mail-konten-im-umlauf.html>
- [6] <https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/passwoerter-von-70000-e-mail-konten-im-umlauf.html>
- [7] <https://www.checktool.ch>
- [8] <http://www.swissleak.ch>
- [9] c't magazin für computer technik, Ausgabe 07/18 vom 17.03.2018, Heise Zeitschriften Verlag, <https://goo.gl/rSS9Eg>

Tokeneconomy – Wieso macht das Sinn?

Moritz Baggenstos

Wir verbriefen schon seit hunderten von Jahren Wertgegenstände. Was ist anders, wenn wir den Besitz via Blockchain regeln? In einem Feldversuch hat der Autor einen Teil seiner Zeit tokenisiert.

Tokeneconomy – Wieso macht das Sinn?

Die Blockchain Technologie ermöglicht es uns, Buchführung effizient, sicher und transparent zu gestalten. Ein Token ist ein digital verbrieftes Wertgegenstand mit einer kryptologisch eindeutigen Signatur. Der Preis eines solchen Tokens hängt von der herausgebenden Entität und dem freien Markt ab. Der Herausgeber eines Tokens definiert den Basiswert, in einigen Fällen ist dieser durch unser Rechtssystem abgesichert, in anderen Fällen besteht er nur auf Vertrauensbasis. Besitztum und Transfer von Tokens sind dank der Infrastruktur der Blockchain unglaublich kosteneffizient. Ein Beispiel einer solchen Infrastruktur ist das Ethereumnetzwerk.

Wir verbriefen seit Jahrhunderten Wertgegenstände

Heute ist vieles verbrieft – von physischem Land über Unternehmen bis hin zu Gold. Ein Papier auszutauschen ist einfacher und effizienter als zum Beispiel zehn Kilogramm Gold. Es gibt ein riesiges Ökosystem, um das nötige Vertrauen zu schaffen, damit ein kleines Stück Papier mit Tinte signifikanten Wert erhält. Ein Staat gibt Unmengen von Ressourcen aus, um schwer fälschliche Identitätsdokumente und Register herzustellen und aufzubewahren. Notariate, Ämter und Börsen profitieren von deren Autorität und Informationsintransparenzen.

Wenn jeder wüsste, dass eine bestimmte Person wirklich 100 Aktien der UBS in Form von Tokens hält, könnte man ihm theoretisch 1700 CHF als Tauschgeschäft

anbieten. Dank smart contracts bräuhete es keine Mittelsmänner oder Autoritäten für diesen Tausch. Das World Wide Web ermöglicht es uns, Informationen auszutauschen. Blockchain Netzwerke ermöglichen es uns, einzigartige Informationen auszutauschen und diese sicher und permanent abzuspeichern.

Mein persönliches Experiment: der MoCoin (MOCO)

Jeder mit einem Internetanschluss kann mit dieser Technologie experimentieren. Ich habe zum Beispiel einen eigenen ERC-20 Token (MOCO) auf Ethereum programmiert. Ein einzelner MoCoin repräsentiert den Wert einer Arbeitsminute von mir. Der Basiswert ist lediglich von mir definiert und es gibt nur einen Linked-in Artikel darüber, keine gesetzliche Grundlage. Ich bin nicht gezwungen, eine Minute für einen Besitzer von MOCOs zu arbeiten, wenn ich das nicht will. Trotzdem gibt es einige Leute, die den MOCO wollen. Es kostet nichts, einen MOCO zu besitzen, und die Transferkosten sind vernachlässigbar klein. Ethereum ist eine riesige, verteilte Datenbank für jedermann. Es kostet kaum etwas, diese Datenbank zu nutzen. Man kann alles Tokenisieren, genauso wie man für alles Mögliche einen Gutschein ausstellen kann. Im Gegensatz zu einem physischen Papier ist es jedoch viel effizienter, ein digitales Gut auszutauschen und zu lagern.

Es gibt insgesamt 99'929 (grösste 5 stellige Primzahl) MoCoins. Ich verschenke jedem Bekannten, der welche möchte, 60 Stück davon. Leider ist die Nachfrage nach den MOCOs nicht gross. Es sind 1140 MOCOs im Umlauf. Einige Freunde haben

mich zum Essen oder zu Drinks eingeladen und wollten dafür mehr MoCoins. Die Herausforderung ist, eine ERC-20 kompatible ETH Adresse zu erstellen. Viele haben Ihre Kryptowährungen auf Exchanges liegen und keine eigene Wallet. Sie wissen nicht, wo sie den Backup für eine Wallet abspeichern sollten.



Moritz Baggenstos hat während seines Wirtschaftsinformatik Studiums an der Universität Zürich ein Startup gegründet. Dies öffnete ihm die Tür ins Silicon Valley, wo er im Bereich Venture Capital neue Technologien und deren Potential beurteilte. Nach seinem Studienabschluss im 2016 arbeitete er für Cisco. Heute ist er bei der Schweizer Softwarefirma ti&m als Consultant mit Fokus auf Blockchain Anwendungsfälle tätig.

Kontaktadresse:
Moritz Baggenstos
Consultant
ti&m AG
Limmatstrasse 35
CH-8005 Zürich
Tel: +41 77 445 33 65
E-Mail: moritz@hotmail.ch

Wo stehen wir heute?

Noch steckt die Adaption der Blockchain Technologie in Kinderschuhen. Vertraute Mittelsmänner sind heutzutage kaum wegzudenken. Die Usability von Blockchain Technologien hält sich noch in Grenzen, doch die Effizienzgewinne sind schon jetzt riesig. Ein Schweizer kann sich mit einem Token das Recht auf Anteile an einer japanischen Unternehmung mit wenigen Mausklicks erkaufen. Er muss sich weder registrieren noch muss er irgendwo unterschreiben. Nur in der Blockchain ist sein Eigentum registriert. Ich habe schon bei diversen ICOs mitgemacht und verfolge den Projektfortschritt genau. Einige wie zum Beispiel Swissborg liefern viele Informationen und andere halten sich eher zurück. Ich investiere in ein Projekt, da ich an die

langfristige Vision glaube und denke, das Team hat die Fähigkeiten, dies erfolgreich umzusetzen. Für kurzfristiges Kaufen und Verkaufen fehlt mir aber die Erfahrung und die Zeit. Diese neue Art der Kapitalbeschaffung finde ich als Unternehmer sehr gut. Wenn man einen ICO richtig unter die Lupe nimmt, kann man auch grobe Fehlgriffe vermeiden.

Mit genügend Zeit werden immer mehr Menschen dem Code und der Logik der Blockchain vertrauen und möchten von den Effizienzvorteilen profitieren. Mittelsmänner und Plattformen werden von der Technologie Blockchain disruptiert werden. Die Karten werden neu gemischt. Wir befinden uns an der Schwelle des «Internet of Information» zum «Internet of Value».

Spin-off gegründet?

Das Institut für Informatik sammelt Angaben zu Spin-offs, die am IfI entstanden resp. ein Resultat von Arbeit/Forschung am IfI sind.

Bitte meldet Euch bei Nathan Labhart (labhart@ifi.uzh.ch) oder verwendet das Formular, welches unter <http://www.ifi.uzh.ch/en/departement/about/spin-offs.html> verlinkt ist.

Danke!

kalender

Sonntag, 8. April 2018

Alumni Geburtstagsbrunch für die ganze Familie mit Figurentheater (ehemals Marionettentheater)

Dienstag, 8. Mai 2018

Swisspeers, Thema: «Blockchain im Crowdlending»

Donnerstag, 28. Juni 2018

Alumni Golf-Turnier inkl. Anfängerkurs

Samstag, 8. September 2018

Alumni Sommernachtsparty mit Special ShowAct und mit PartnerIn

Montag, 29. Oktober 2018

Goldwyn Partners Group Workshop: «Executive Videotraining – Bewerbung und Rekrutierung in Echtzeit üben!»

Montag, 12. November 2018

Alumni Generalversammlung (mit IPT-Programm)

Dienstag, 11. Dezember 2018

Fondue Plausch mit PartnerIn

Details zu den einzelnen Veranstaltungen werden jeweils vorgängig mitgeteilt. Änderungen sind jederzeit möglich. Siehe auch www.alumni.ch/events.

Statistiken über Studierende und Alumni

	2008			2009			2010			2011													
	Studierende			Studierende	Beginner	Abschluss	Studierende	Beginner	Abschluss	Studierende	Beginner	Abschluss											
	m	w	Total	m	w	Total	m	w	Total	m	w	Total											
Lizentiat, Diplom	51	8	59	19	4	23	-	29	5	34	-	-	-										
Bachelor	164	24	188	172	19	191	62	24	26	188	25	213	79	22	24	301	38	339	98	24	4	28	
Master	34	1	35	46	1	47	18	14	-	14	57	4	61	19	12	12	82	21	103	19	21	-	21
Doktorat	62	15	77	71	15	86	7	5	2	7	67	13	80	6	12	1	72	13	85	8	5	-	5
Master of Advanced Studies	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	19	5	24	-	10	-	10
Lehrdiplom	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	4	3	7	-	-	-	-

	2012			2013			2014			2015		
	Studierende	Beginner	Abschluss	Studierende	Beginner	Abschluss	Studierende	Beginner	Abschluss	Studierende	Beginner	Abschluss
Lizentiat, Diplom	m	w	Total	m	w	Total	m	w	Total	m	w	Total
Bachelor	19	2	21	-	-	-	15	2	17	-	-	-
Master	296	46	342	91	38	129	317	66	383	120	30	150
Doktorat	107	29	136	18	21	39	132	23	155	9	21	30
Master of Advanced Studies	63	17	80	6	20	26	58	9	67	5	11	16
Lehrdiplom	1	-	1	-	16	17	-	-	-	-	-	-

	2016			2017		
	RO06 (ab 2. Sem.)	RO08	RO16	RO06 (ab 2. Sem.)	RO08	RO16
Bachelor	m	w	Total	m	w	Total
Master	68	14	82	121	25	146
Doktorat	30	2	32	97	36	133

	2012										2013										
	Wirtschaftsinf.			Softwaresysteme			Angw. Inf./MMCS		Computational Sc.		Wirtschaftsinf.			Softwaresysteme			Angw. Inf./MMCS		Computational Sc.		
	m	w	Total	m	w	Total	m	w	Total	m	w	Total	m	w	Total	m	w	Total	m	w	Total
Bachelor Beginn	45	5	50	12	0	12	10	2	12				44	12	56	18	4	22	9	7	16
Bachelor Abschluss	30	2	32	6	1	7	2	1	3				18	3	21	9	0	9	3	0	3
Master Beginn	4	2	6	5	2	7	3	0	3	0	2	2	3	1	4	3	0	3	2	0	2
Master Abschluss	8	3	11	6	0	6	3	0	3	1	1	2	6	3	9	8	2	10	4	0	4
Fast Track Beginn	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Fast Track Abschluss	2	0	2	1	0	1	0	0	0	0	0	0	2	0	2	0	0	0	0	0	0
Doktorat Anfang	3	3	6										5	0	5						
Doktorat Abschluss	20	1	21										11	5	16						

	2014										2015										
	Wirtschaftsinf.			Softwaresysteme			Angw. Inf./MMCS		Computational Sc.		Wirtschaftsinf.			Softwaresysteme			Angw. Inf./MMCS		Computational Sc.		
	m	w	Total	m	w	Total	m	Total	m	w	Total	m	w	Total	m	w	Total	m	w	Total	
Bachelor Beginn	54	4	58	18	4	22	5	8	13				62	12	74	24	5	29	11	5	16
Bachelor Abschluss	29	1	30	8	0	8	2	0	2				20	2	22	6	0	6	4	2	6
Master Beginn	3	0	3	2	6	8	4	1	5	0	0	0	3	2	5	6	1	7	7	0	7
Master Abschluss	20	1	21	15	3	18	4	1	5	1	0	1	14	2	16	11	0	11	5	0	5
Fast Track Beginn	1	0	1	0	1	1	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0
Fast Track Abschluss	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
Doktorat Anfang	4	2	6										6	2	8						
Doktorat Abschluss	5	1	6										8	1	9						

	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000
Alumni neue	0	6	12	11	13	12	28	21	23	29	18	25	25	22	18	16	13
Alumni total	0	6	18	29	42	54	82	103	126	155	173	198	223	245	263	279	292
Wachstum (%)			200%	61%	45%	29%	52%	26%	22%	23%	12%	14%	13%	10%	7%	6%	5%

	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Alumni neue	16	14	22	53	39	34	86	85	38	24	26	56	15	19	18	15	16
Alumni total	308	322	344	397	436	470	556	641	679	703	729	785	771	768	797	824	861
Wachstum (%)		5%	7%	15%	10%	8%	18%	15%	6%	4%	4%	8%	-2%	0%	4%	3%	4%



#WeAreAvaloq

At Avaloq, we are committed to innovation and efficiency for the financial industry. Banks and wealth managers in all major financial centres rely on our software and services, and this unique Community grows every day. We are a value-driven fast-paced technology and financial services company.

We pride ourselves in a diverse, international and interdisciplinary team: we are more than 2'000 people which already today originate from 56 nations. And we are looking for even more personalities who would like to join us – if you are one of them, we look forward to meeting you!

Learn more about our open positions at www.avaloq.com/careers.

