TRUST SQUARE

BLOCKCHAIN SWISS MADE

Eine Einführung in die Blockchain

59. ITS Techno-Apéro “Blockchain – und was hat die Industrie davon?“
Schaffhausen, 18. Juni 2018

Daniel Gasteiger

Über 20 Jahre Bankerfahrung bei der UBS und Credit Suisse vor der Gründung verschiedener Blockchain Firmen in Zürich

- nexussquared – Blockchain Start-up Beratungsfirma (2015)
- Procivis AG – Blockchain Lösungen für Regierungen und NGOs (2016, acting CEO)
- Trust Square AG – Blockchain Start-up und Forschungszentrum (2018, Chairman)
- Verum Capital AG – Beratungsboutique für Blockchain Investments (in Gründung)

Mitglied von verschiedenen Blockchain Beratungsgremien

- Blockchain Task Force Switzerland Mitglied WG “Banking” / “ICO Token Map”
- Global Blockchain Business Council Verwaltungsrat
- Singularity Fund Advisory Board
- Horizon State und andere Start-up Advisor Mandate

Blockchain Grundlagen

Die 3. Phase des Internets

Phase 1 (seit 1994)
Das Web

Teilen von Informationen

Phase 2 (seit 2004)
Social Media

Teilen von Meinungen

Phase 3 (seit 2009)
Blockchain

Sicheres Teilen von “Werten”

Blockchains sind verteilte Datenbanken

Blockchain ist eine neue Art für die **Speicherung von digitalen Informationen und Transaktionen**, welche nie mehr verändert (manipuliert) werden können

Die Daten sind auf **unzähligen, unabhängigen Computern** auf der ganzen Welt gleichzeitig gespeichert

Kryptowährungen werden u.a. hergestellt, um die teilnehmenden Computer(besitzer) für ihren Strom-aufwand zu entschädigen

Durch Beizug **komplexer Verschlüsselungs-technologien** braucht es niemanden, welcher das System zentral überwacht und vor Manipulation schützt

Blockchain Anwendungen

Blockchain kann überall eingesetzt werden, wo

- **verschiedene Parteien an einer Transaktion** beteiligt sind, welche sich nicht unbedingt kennen oder trauen
- es um die **Uebertragung von Rechten und Werten** geht, welche unwideruflich und vor allem unkorruptierbar getätigt werden sollen

Anwendungsmöglichkeiten gehen weit über das Thema „Kryptowährungen“ hinaus

- **Wertschöpfungs- und Lieferketten** (z.B. zur Bekämpfung von Medikamentenfälschungen)
- **Register** der öffentlichen Hand (z.B. Handelsregister, Grundbuch etc.)
- (Selbsthoheitliche) **Digitale Identitäten** & Verwaltung persönlicher Daten

Es gibt nicht *eine* Blockchain

- **Öffentliche Variante** – jeder kann mitmachen und die Transaktionen prüfen (wie beim Internet)
- **Private Variante** – Schreibe- resp. Lese-/Schreiberechte sind limitiert (wie ein Intranet)
- **Hybrid Variante** – die Transaktionen werden im privaten Umfeld abgewickelt und nur digitale Zeitstempel (Hashs) werden regelmässig auf eine öffentliche Blockchain geschrieben

bitcoin

ripple

HYPERLEDGER

Die Anfänge der Blockchain

THE WALL STREET JOURNAL.

DOWJONES A NEWS CORPORATION COMPANY

TUESDAY, SEPTEMBER 16, 2008 - VOL. CCLII NO. 65

★★★★ $2.00

DJIA 10917.51 ▼504.48 -4.4% NASDAQ 2179.91 ▼3.6% NIKKEI Closed(12214.76) DJ STOXX 50 2744.81 ▼4.0% 10-YR TREAS ▲2 3/32, yield 3.482% OIL $95.71 ▼$5.47 GOLD $783.10 ▲$22.80 EURO $1.4310 YEN 104.88

AIG, Lehman Shock Hits World Markets

Focus Moves to Fate of Giant Insurer After U.S. Allows Investment Bank to Fail; Barclays in Talks to Buy Core Lehman Unit

The convulsions in the U.S. financial system sent markets across the globe tumbling, as two of Wall Street's biggest firms looked set to exit the scene and insurance titan American International Group Inc. turned to the Federal Reserve and the state of New York for assistance.

By Susanne Craig, Jeffrey McCracken, Jon Hilsenrath and Deborah Solomon

The U.S. stock market suffered its worst daily point plunge since the first day of trading after the Sept. 11, 2001, terrorist attacks. Financial markets were rattled by the rushed sale Sunday of Merrill Lynch & Co. and the bankruptcy-court filing of Lehman Brothers Holdings Inc., which scrambled Monday to sell its most-prized businesses before too many employees and customers walk out the door. (Please see related article on Page C1.)

All day Monday, top Lehman officials were huddled in Manhattan at their Seventh Avenue headquarters negotiating a sale of the U.S. investment bank—the core part of Lehman—to Barclays PLC of the U.K. People involved in the discussions were increasingly hopeful late Monday that a deal would be struck.

In stock markets from Sydney to London to New York, the news was greeted with immediate selling. For much of the day, the major U.S. market indexes were down 2%, which, while a good-sized decline, was smaller than many had thought would be the case. But in the final hour of trading, a wave of selling hit, driven by concerns about the fate of AIG. The Dow Jones Industrial Average ended down 504.48 points on Monday, off 4.4%, at its daily low of 10917.51, down 18% on the year. Of the Dow industrials' 30 components, all but one—Coca-Cola Co.—fell, led by a 60.8% plunge in AIG.

In Europe, London's FTSE 100 index dropped 3.9%. Several Asian markets, including Japan and China, were closed Monday due to holiday. By Tuesday, Tokyo shares were down 5.1% in early trading, and Hong Kong's Hang Seng index was down 6.1%.

Monday's action was the latest fallout in a widening financial crisis that began a year ago with the fall of American housing prices and is now reordering the U.S. financial system. Steps unveiled by the Federal Reserve to expand its emergency lending arsenal did little to snap the sense of gloom.

Plenty of potential land mines remain. Banks are increasingly hoarding cash, curbing lending at a time when the economy is slowing. They are also starting to dump assets to raise capital. A mass sale of assets by

Please turn to page A2

Traders around the world react to **sharp selloffs** after one of the most turbulent days in Wall Street's history.

AIG Faces Cash Crisis As Stock Dives 61%

By Matthew Karnitschnig, Liam Pleven And Serena Ng

American International Group Inc. was facing a severe cash crunch last night as ratings agencies cut the firm's credit ratings, forcing the giant insurer to raise $14.5 billion to cover its obligations.

With AIG now tottering, a crisis that began with falling home prices and went on to engulf Wall Street has reached one of the world's largest insurance companies, threatening to intensify the financial storm and greatly complicate the government's efforts to contain it. The company, whose stock fell 61% yesterday, is such a big player in insuring risk for institutions around the world that its failure could shake the global financial system.

AIG has been scrambling to raise as much as $75 billion to weather the crisis, and people close to the situation said that if

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

«...online payments to be sent directly from one party to another without going through a financial institution.»

Silk Road

anonymous market

messages 0 | orders 0 | account ฿0.00

Search Go

Shop by Category

- Drugs *8,670*
  - Cannabis *2,066*
  - Dissociatives *165*
  - Ecstasy *660*
  - Opioids *591*
  - Other *455*
  - Precursors *50*
  - Prescription *2,146*
  - Psychedelics *981*
  - Stimulants *1,102*
- Apparel *264*
- Art *127*
- Biotic materials *1*
- Books *861*
- Collectibles *5*
- Computer equipment *32*
- Custom Orders *68*
- Digital goods *509*
- Drug paraphernalia *305*
- Electronics *77*

1g MDMA 82%+ High Quality -Made in Germany-
฿1.30

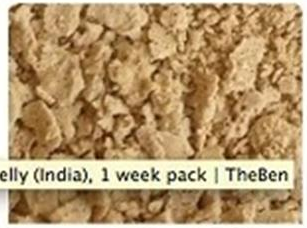
50 gr. Crystal MDMA Rocks
฿23.33

Valium 10mg/ Diazepam (100 Pills)
฿2.32

3g XxX AAA QUALITY WEED,AMAZING
฿0.98

Kamagra jelly (India), 1 week pack | TheBen

Kamagra jelly (India), 1 week pack
฿0.98



Honeycomb Wax (85+% THC) Fully Purged
฿1.45

1 gram ✖ Moroccan Hash ✖ DUTCH QUALITY
฿0.27

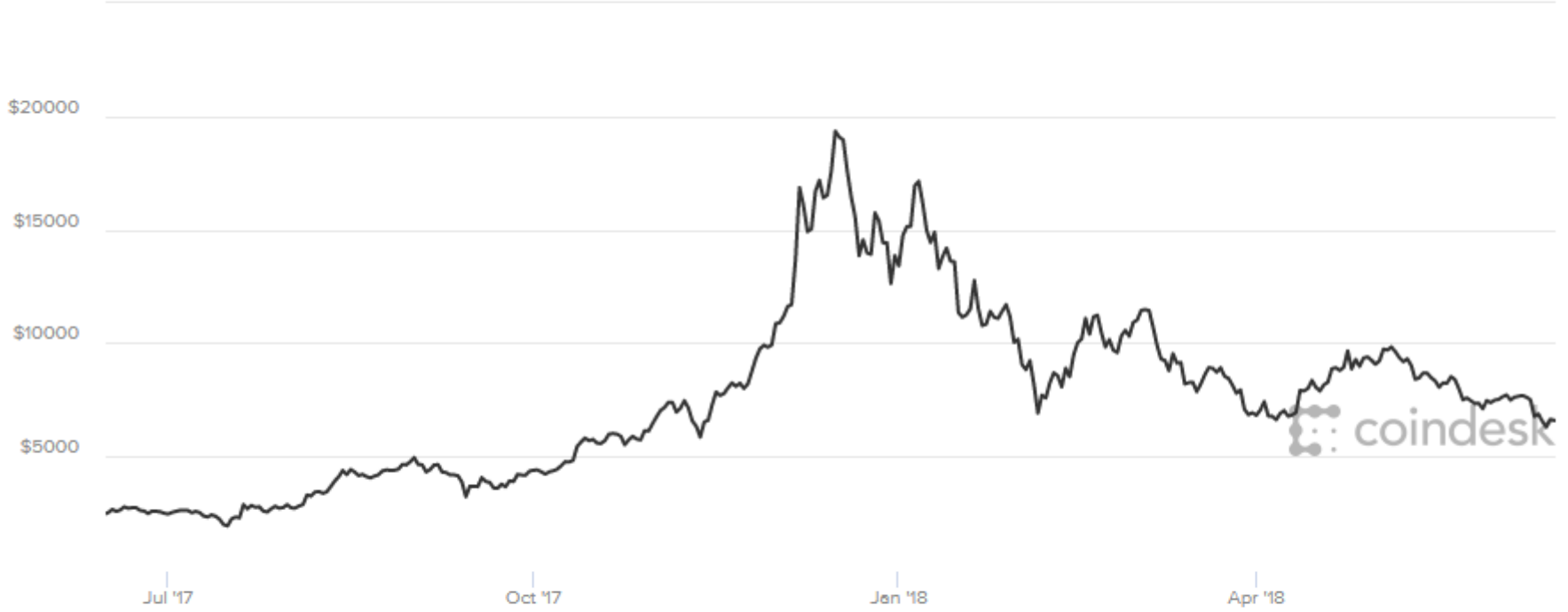
Citalopram 10x 20mg table
฿0.10

Bitcoin (USD) Price

Closing Price OHLC

1h 12h 1d 1w 1m 3m 1y All

Jun 15, 2017 to Jun 15, 2018 Export



$6,578.32 ▼-0.90%

Today's Open	$6,637.74	Change	▼$-59.42
Today's High	$6,642.42	Market Cap	$0.112T
Today's Low	$6,546.53	Supply	17,094,138

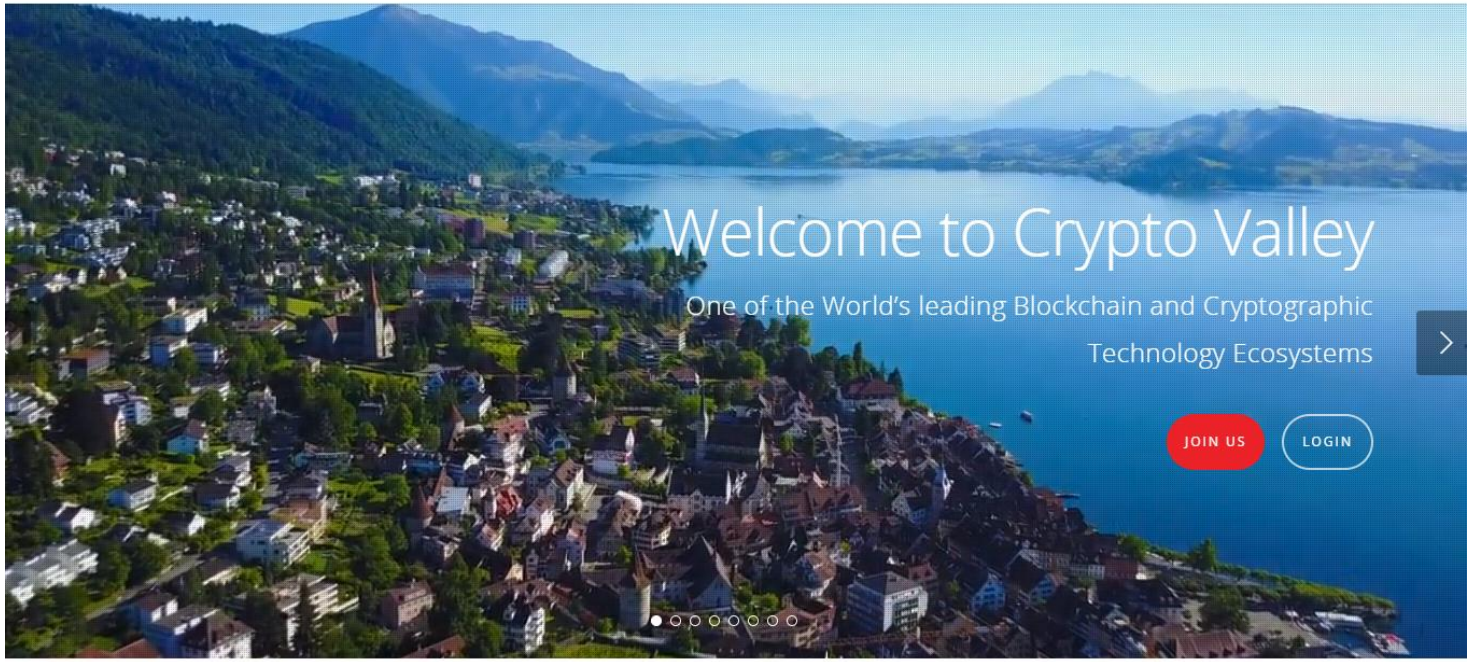
Blockchain 2018

CoinMarketCap Market Cap Trade Volume Trending Tools

#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d
1	Bitcoin	BTC	$159,106,772,939	$9,348.43	17,019,625	$6,701,120,000	-0.38%	-3.55%	0.38%
2	Ethereum	ETH	$74,777,050,792	$753.19	99,280,989	$2,905,870,000	-0.56%	-5.25%	9.70%
3	Ripple	XRP	$32,349,449,665	$0.825699	39,178,259,468 *	$603,599,000	-0.51%	-6.42%	-3.39%
4	Bitcoin Cash	BCH	$28,016,150,025	$1,637.00	17,114,325	$1,513,940,000	-1.04%	-6.15%	16.27%
5	EOS	EOS	$14,394,563,888	$17.12	840,607,562 *	$1,282,180,000	-0.45%	0.42%	-10.98%
6	Litecoin	LTC	$9,270,837,053	$164.32	56,420,438	$544,412,000	-0.64%	-4.81%	8.38%
7	Cardano	ADA	$8,586,319,804	$0.331172	25,927,070,538 *	$152,314,000	-0.15%	-5.35%	-5.80%
8	Stellar	XLM	$7,355,856,702	$0.396071	18,572,065,873 *	$38,946,600	-0.20%	-5.03%	-9.58%
9	IOTA	MIOTA	$6,043,782,852	$2.17	2,779,530,283 *	$97,796,500	0.55%	-7.05%	9.45%
10	TRON	TRX	$5,334,742,606	$0.081139	65,748,111,645 *	$336,710,000	-0.13%	-2.48%	-10.62%
11	NEO	NEO	$5,131,704,500	$78.95	65,000,000 *	$155,746,000	0.44%	-6.11%	-10.49%
12	Dash	DASH	$3,746,834,942	$465.04	8,056,982	$88,616,500	-0.14%	-5.65%	-4.32%
13	Monero	XMR	$3,608,817,045	$225.47	16,005,753	$42,777,400	-0.14%	-4.73%	-8.18%
14	NEM	XEM	$3,505,707,000	$0.389523	8,999,999,999 *	$22,226,600	0.25%	-5.71%	-5.92%
15	VeChain	VEN	$2,502,338,536	$4.76	525,899,138 *	$97,452,500	0.13%	-4.49%	3.96%
16	Ethereum Classic	ETC	$2,457,772,002	$24.20	101,567,122	$506,181,000	-0.39%	0.55%	8.65%
17	Tether	USDT	$2,196,259,760	$0.999599	2,197,140,814 *	$3,631,790,000	0.02%	0.05%	-0.10%
18	Qtum	QTUM	$1,903,578,295	$21.49	88,576,840 *	$239,603,000	-0.12%	-3.92%	-10.66%
19	OmiseGO	OMG	$1,650,783,177	$16.18	102,042,552 *	$43,570,300	0.77%	-5.09%	-7.54%
20	ICON	ICX	$1,580,926,192	$4.08	387,231,348 *	$31,291,600	0.47%	-3.09%	-9.21%

Crypto Valley

About Us Our Network Our Activities Join Us Login



Purchase your ticket to the 2018 Crypto Valley Conference while there is still availability.

PURCHASE TICKETS NOW

Trust Square Zürich-Bahnhofstrasse

Universität Zürich[UZH]

Universität Basel

ETH zürich

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Lykke

Services Sign in Get started

EXCHANGE WALLET COMMUNITY COMPANY

BTC ⇆ USD	BTC ⇆ EUR	ETH ⇆ USD	BTC ⇆ CHF	LKK ⇆ CHF	LKK ⇆ USD	LKK1Y ⇆ USD	BTC ⇆ LKK1Y
6941.447	5659.28	391.04988	6677.394	0.06375	0.0665	0.06634	104663.73

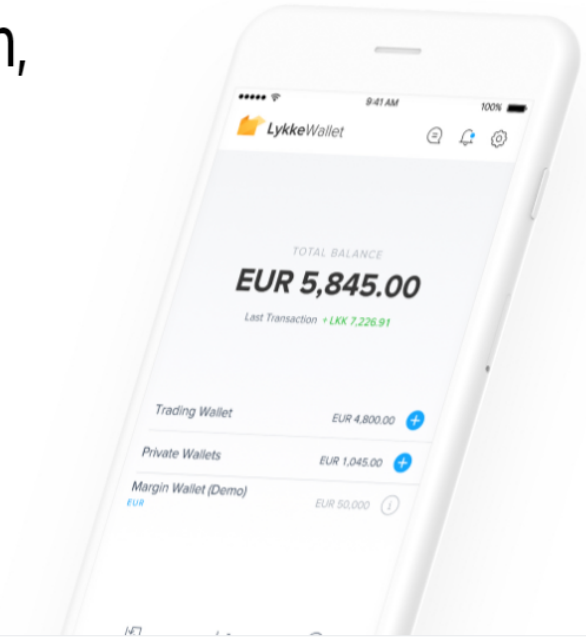
Trade Bitcoin, Ethereum, FX and digital assets

Access easily. Own directly.

Create free account

Download on the App Store GET IT ON Google Play

iOS 8.0+ and Android 4.4.2+ required

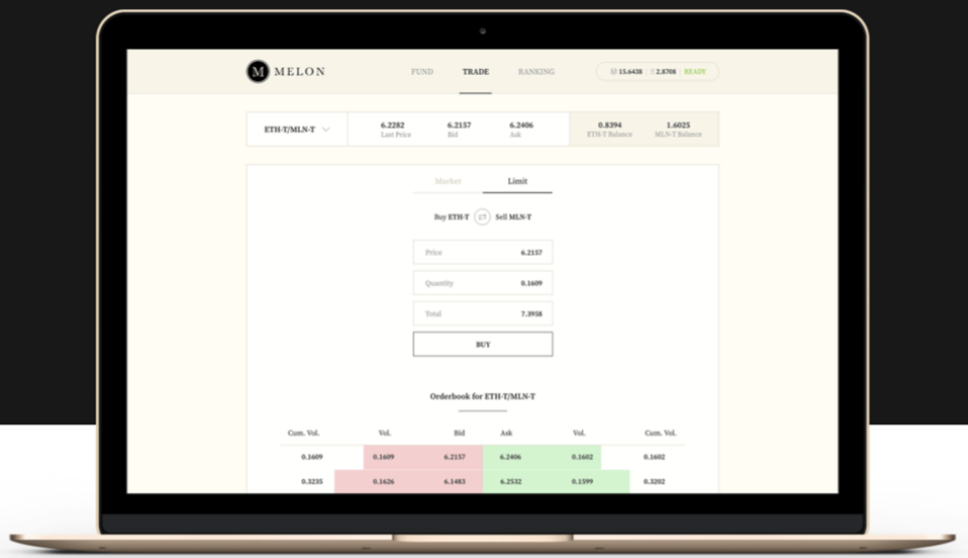


MELONPORT

ABOUT TEAM LEARN CONTACT

MELON

Melon is the first of its kind autonomous systems, designed specifically for the purposes of crypto asset management. Both its frontend as well as its backend are hosted and executed on decentralised platforms. The frontend operates on top of IPFS, while the backend leverages off a set of Ethereum smart contracts.



B3i

The Blockchain Insurance Industry Initiative

Less admin, more insurance

Welcome to B3i - The Blockchain Insurance Industry Initiative

B3i Services AG is a startup formed to explore the potential of using Distributed Ledger Technologies within the re/insurance industry for the benefit of all stakeholders in the value chain.

B3i provides insurance solutions on a blockchain platform offering opportunities for efficiency, growth and quality across the value chain to benefit all participants including end customers.

Following incorporation, B3i will grow its community of shareholders, partners and customers and create an ecosystem of products and services developed "by the market, for the market".

achmea AEGON ageas Allianz

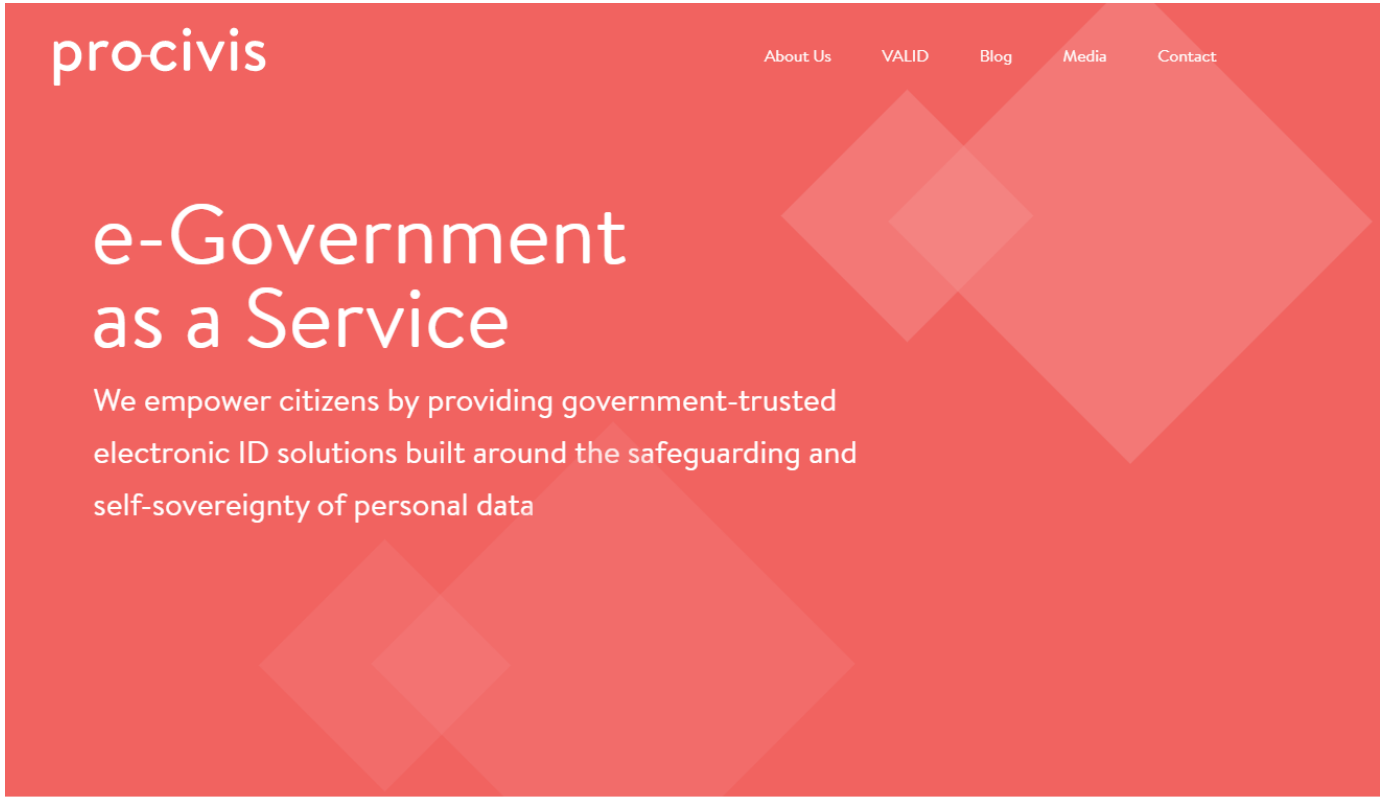
Latest News

Out of the starting blocks

Blog, 28/03/2018

Chris Madsen, CEO Aegon Blue Square Re writing for B3i
While (re)insurance has made great strides in process improvements over the past decades, many processes remain largely manual, frustrating and costing members of the insurance value chain. Now, imagine a world where data flows easily where it is supposed to go, and it does so in a controlled and secure manner, setting the stage for increasingly automated transactions and processing.
Further, consider that truly digitalising a process allows it to follow Moore's Law and thus improve exponentially in terms of processing time and capabilities. Setting the stage for this is therefore a valuable and sustainable endeavour that could benefit insurance value chain members for years and decades to come.

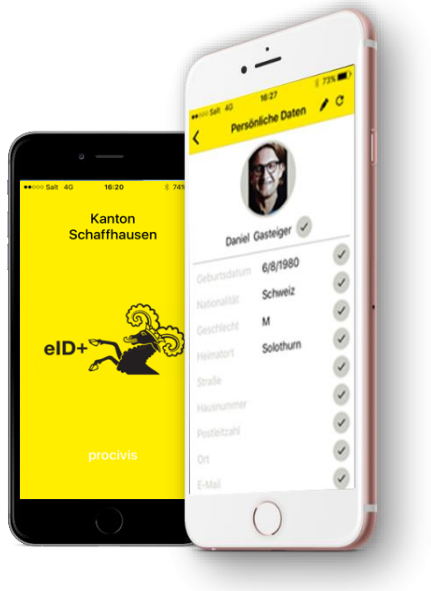
Read more →



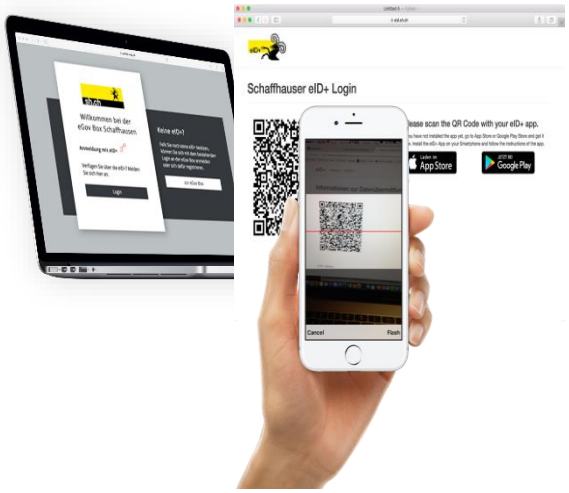
Enabling services: eID+

"eID+" is a secure, government trusted digital identity platform. At the core of the solution is a mobile app enabling citizens to create and manage their digital identities so they can access related online services. These include secure and convenient logins to websites using two-factor authentication as well as digital signing and secure storage of privacy sensitive documents.

Schaffhauser eID+



- Seit Anfang Juni im Regelbetrieb im Einsatz
- Erste produktive ‘eID’ in der Schweiz, hoheitlich attestiert von einem Kanton
- Hohe Vertrauenswürdigkeit der eID durch die persönliche Ueberprüfung der Daten durch den Staat = Einsatzmöglichkeit in der Privatindustrie
- Standart-Technologie (QR Code / OpenConnect ID)
- Einbindung von PKI, Signaturen und Blockchain in Version 2)



TRUST SQUARE

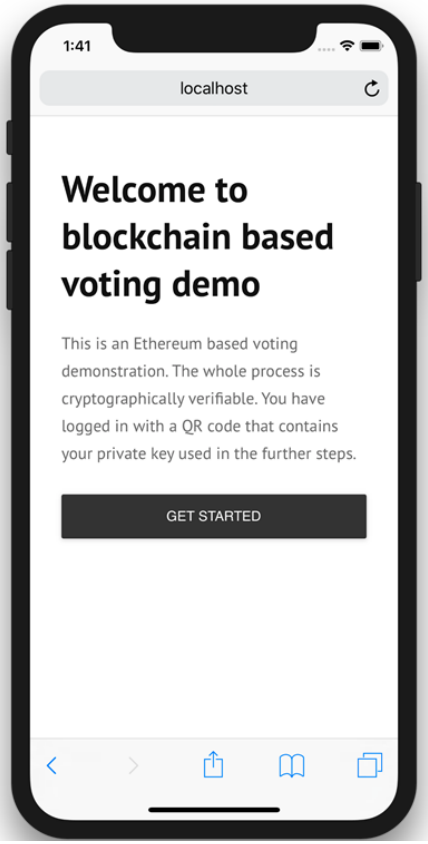
BLOCKCHAIN SWISS MADE

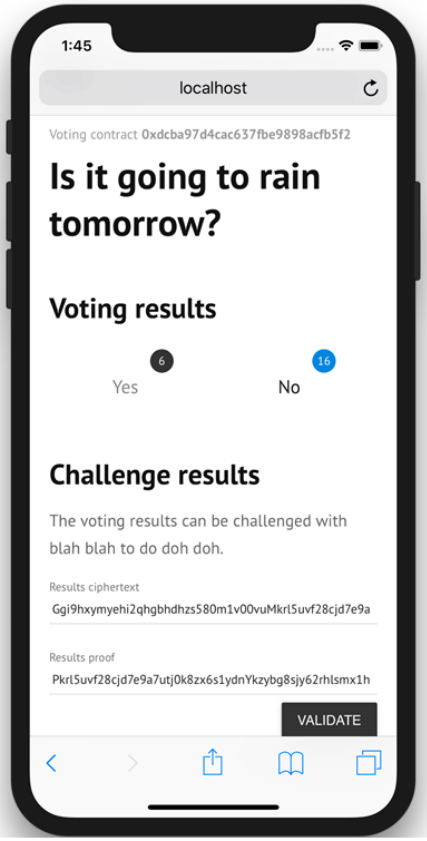
eID+ powers...

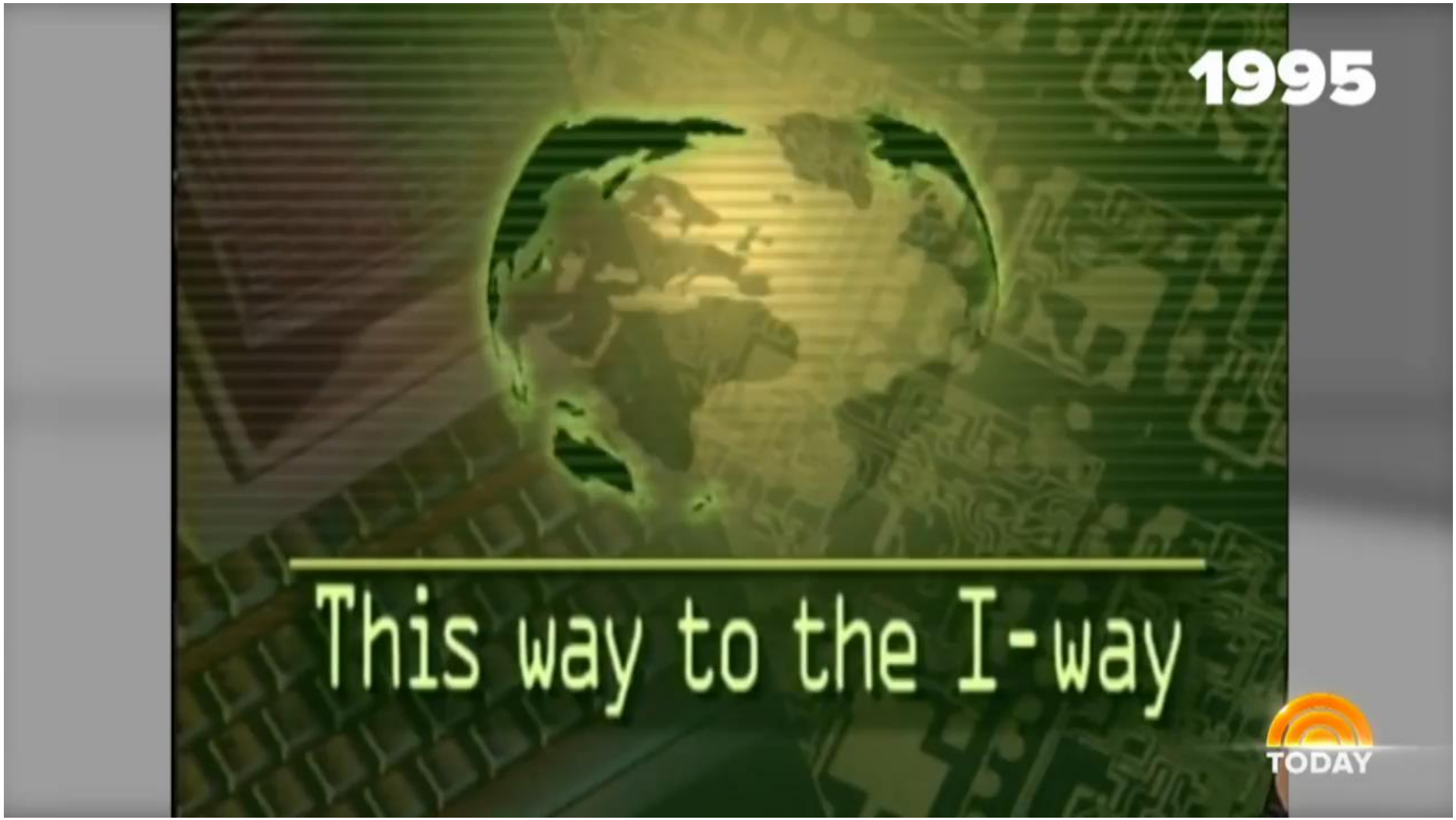
- e-health
- e-visa
- e-banking & KYC
- e-social welfare
- e-signature
- e-registry
- e-commerce
- e-voting
- e-license & certificate
- e-humanitarian & development

University of Zurich[UZH]

procivis
e-government as a service






1995
This way to the I-way
TODAY

Kontakt

DANIEL GASTEIGER

Trust Square AG

Bahnhofstrasse 3

8001 Zürich

gasteiger@procivis.ch

Telefon +41 78 686 48 19

www.trustsquare.ch