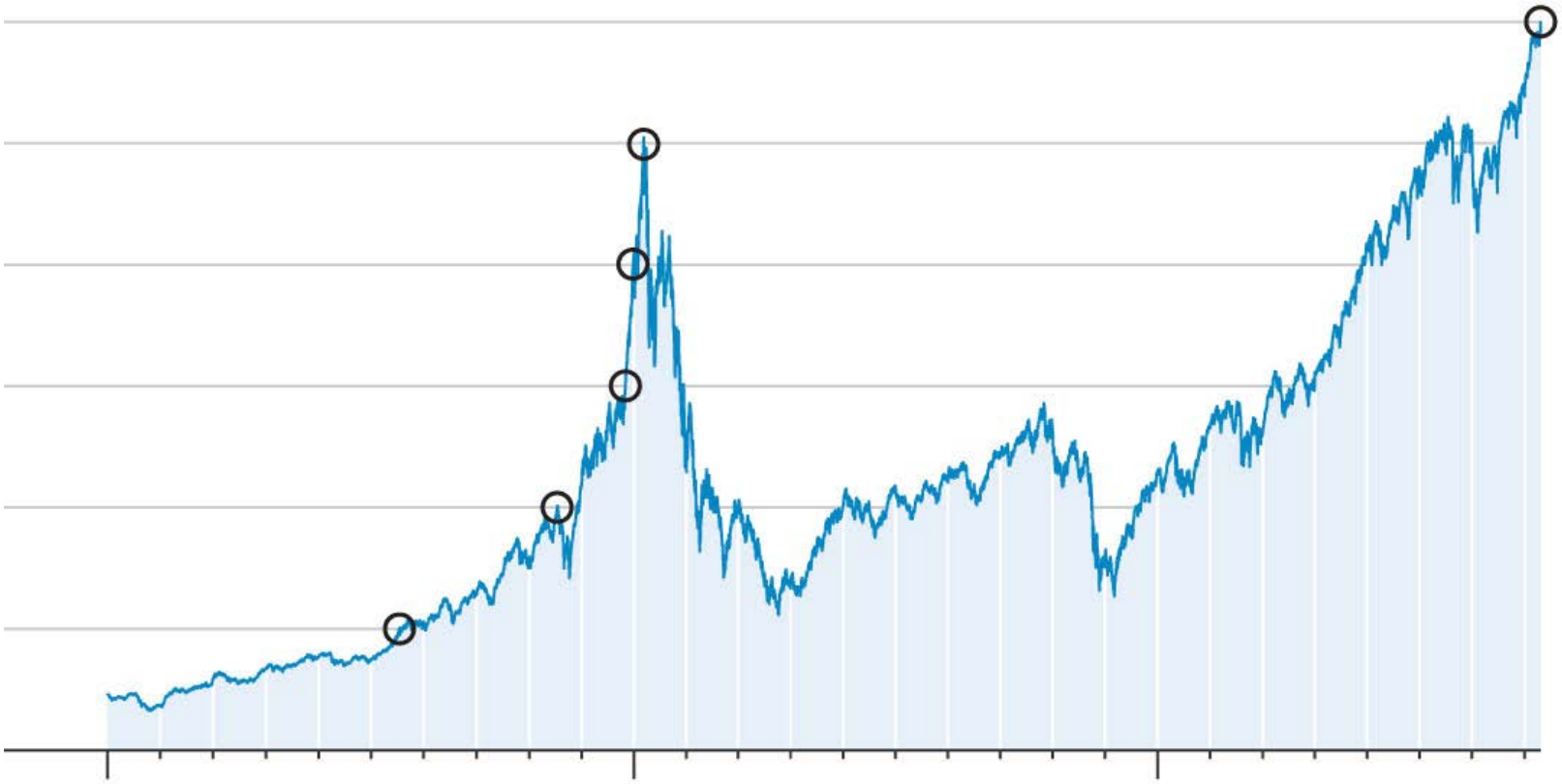
Smart Contracts
Revolution oder Hype?

gbf Technology Afternoon Workshop

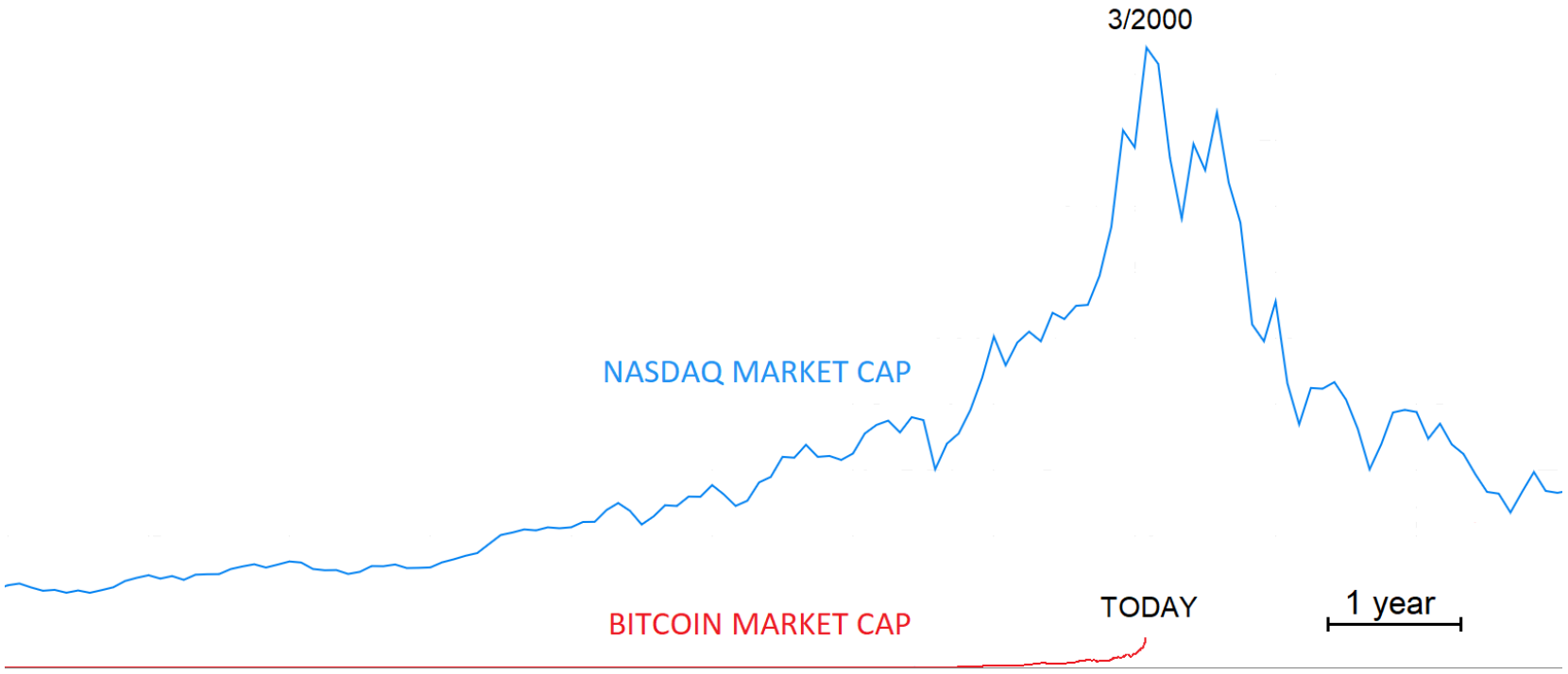
Marco Novoselac
19. April 2018

The Dotcom Bubble

gbf



The Crypto Bubble?


3/2000
NASDAQ MARKET CAP
BITCOIN MARKET CAP
TODAY
1 year

Revolution

- 100 Anwälte auf dem Meeresgrund?
- Neues (Rechts-)System
  - Vollkommene Umsetzung Parteiwillen ohne rechtliche Bindung
  - Automatisierung des Rechts – Vertragsrecht überflüssig -> Paralleles Transaktionsuniversum
  - Revolutionierung unternehmerische Ausgestaltung
  - Neustrukturierung Eigentum
  - Entindividualisierung der Vertragsbeziehungen
  - Autark - technologische Alternative zum Rechtssystem
  - Sicher, einfach, schnell, günstig

Hype

- Alter Wein in digitalen Schläuchen
- Keine Anwendungsfälle
- Viele Behauptungen bezüglich Potenzial und Möglichkeiten nicht überprüfbar
- Vieles gar nicht machbar
- Falsche Prämisse: Menschen schlecht – Computer gut
- Ponzi Scheme

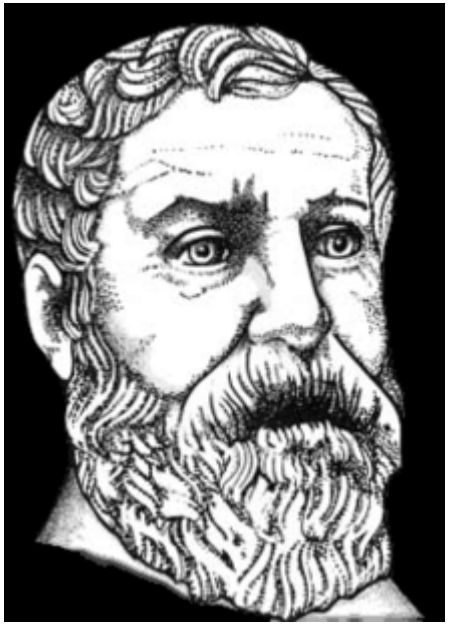
Nick Szabo

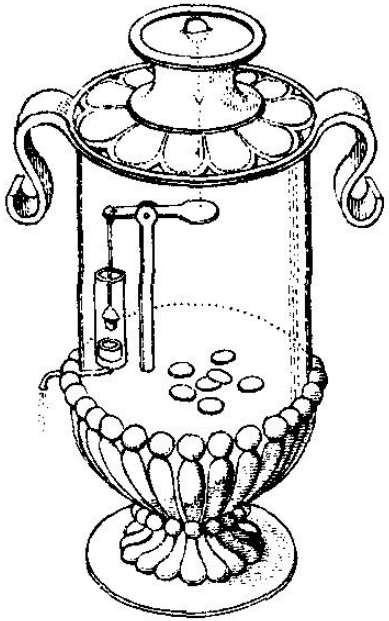
„Computerized transaction algorithm, which performs the terms of a contract.“

“a set of promises, specified in digital form, including protocols within which the parties perform on these promises”

“The basic idea of smart contracts is that many kinds of contractual clauses can be embedded in the hardware and software we deal with.”

Heron von Alexandrien





Antiker Münzautomat
Diesen Weihwasserspender für Tempel erfand der Physiker Heron von Alexandria im 1. Jh. n. Chr. In das Gefäß warf man oben eine Münze ein. Sie fiel auf einen Hebel, der daraufhin einen Stöpsel anhob und so geweihtes Wasser ausfließen ließ.

Was ist ein Smart Contract?

- Vertrag mit automatischer Abwicklung?
- Automated Trading Systems: 75% aller Aktien USA
- E-Commerce Verträge

Was ist ein Smart Contract

- Programmtechnische Wenn-Dann-Bedingungen
  - Ausführung automatisiert und selbständig
  - Eindeutige, klare Logik und exakte, vollständige Information
- **In Blockchain gespeichert und abgewickelt**
  - Keine menschliche Intervention, Überprüfung
  - Integrierter Vollzugsmechanismus
  - Kein Vertrauen notwendig
  - Unverfälscht
  - **Smart**
- Verstärkte bzw. absolute Bindung
- Entindividualisierung der Transaktionsabwicklung

Blockchain

- Technologie äusserst kompliziert -> Prinzip einfach: direkter Transfer von „Geld“ oder sonstigen Werten von Person A zu Person B
- Dezentrales, transaktionsbasiertes Verzeichnis
  - Distributed Ledger: Verteilt gespeichertes Geschäftsbuch
  - Netzknoten
  - Transaktion = Buchung im verteilten Verzeichnis
- Kryptografische Verbindung von Datenblöcken
- Konzeptionell unveränderbar
- Internet der Daten -> Internet der Werte

Arten von Smart Contracts?

- Gemischte Smart Contracts
- Übersetzung eines „natürlichen“ Vertrages
- Direct Coding
- Smart Alternative Contracts (Machine to Machine)

Entmystifizierung

- Selbstdurchsetzung
  - Nicht nur technisch, sondern auch rechtlich durchsetzbar
- Technisch garantierte, perfekte Ausführung
  - Code muss perfekt sein – ist er aber nie – perfekte Erfüllung kann nicht garantiert werden -> Technologische Anfälligkeit
  - „Geldbeträge“ müssen reserviert werden
- Unveränderbarkeit
  - Zukünftige Eventualitäten abbilden
  - Langfristige Vertragsbeziehungen
  - Beseitigung Flexibilität

Entmystifizierung

- Umsetzung Vertragssprache in Code
  - Viele Vertragsbestimmungen nicht kodierbar
    - Als Algorithmus abgebildet
    - Geeignet für formelhafte Umsetzung
    - ≠ Guter Glaube, Angemessenheit, nicht messbar etc.
  - Diskrepanzen zwischen Originalvertrag und Smart Contract
  - Technologische Komplexität
  - Fehlerquote steigt mit der Länge des Codes

Entmystifizierung

- Integration der physischen Welt (automatische Erkennung und Prüfung der Erfüllung)
  - On-Chain Events (Zeitablauf, Transfer von Tokens) <-> Off-Chain Events
  - Drittpartei signiert unlocking script nach Feststellung Off-Chain Ereignis (Orakel)
  - Skript kann nur signiert oder nicht signiert werden
  - Orakel nicht unfehlbar, vertrauenswürdig, bezieht Infos aus Quelle, nicht dezentral ≠ Blockchain, Konsistenz der Quelle
  - Notwendigkeit Sensoren, Tracking Technologie, automatische Überwachung; IOT, aber noch am Anfang

Anwendungsfälle

- Escrow Agreement
- Versicherungen
  - Entschädigung bei Flugverspätungen
  - Automatische Erhöhung Versicherungsprämie bei gefährlichem Fahrstil
- Automatische Einstellung Leistungen bei Zahlungsverzug
- Mietzinskaution

gbf

- Fahrservice mit selbstfahrenden Autos
- Auto holt ab und bringt an angegebenen Ort
- Auto lädt selbst auf
- Auto fährt selbst in Service

- Driverer AG <-> Kunde
- Driverer AG <-> Stromlieferant
- Driverer AG <-> Autogarage
- Driverer AG <-> Versicherung
- Driverer AG <-> Buchhaltung

Zusammenfassung

- Entwicklung Internet – E-Commerce
- Keine mystische Technologie
- Technisch **und** rechtlich vollstreckbar damit wirtschaftlich interessant
- Verständnis was rechtlich und technisch möglich
- Beschränkter Inhalt von Smart Contracts
- Trade-off Genauigkeit und Gewissheit <-> Flexibilität
- Für Vorteile -> Code perfekt: Keine Code-Fehler, korrekte Wiedergabe Parteiwillen, keine Sicherheitslücken
- Erfüllung von Obligationen in der physischen Welt -> Vorteile Blockchain weg

Revolution oder Hype?

Stupid Contracts.

Heute (kleiner) Hype - Peak of inflated Expectations?

Morgen grosser Hype, dann schleichende Revolution (5-10 Jahre).

Thank you for your attention!

Marco Novoselac
Partner
Attorney-at-law, M.B.L.-HSG
novoselac@gbf-legal.ch

gbf
Attorneys-at-law

P.O. Box 1661
Hegibachstrasse 47
8032 Zurich
Switzerland

T +41 43 500 48 50
F +41 43 500 48 60

P.O. Box 1911
Route de Pré-Bois 20
1215 Geneva Airport
Switzerland

T +41 22 533 48 50
F +41 22 533 48 54

contact@gbf-legal.ch
www.gbf-legal.ch