Blockchain matters

Why does blockchain matter?

Balázs Héder, Ph.D.

December 2021

Have you ever heard these phrases?

Blockchain matters

Blockchain is going to change the World!

Bitcoin bubble has been popped!

Bitcoin is a bubble!

Bitcoin is the money of criminals!

Bitcoin bubble is going to be popped!

Bitcoin is dead! Bitcoin Obituaries, *url*

Blockchain is immutable!

Bitcoin is the blockchain!

Blockchain is not Bitcoin!

Blockchain contains the truth!

Smart contracts are running on the blockchain.

Cryptocurrencies are useless, but blockchain is good!

Blockchain is secure!

Have you ever heard these phrases?

Blockchain matters

Blockchain is going to change the World!

Bitcoin bubble has been popped!

Bitcoin is a bubble!

Bitcoin is the money of criminals!

Bitcoin bubble is going to be popped!

Bitcoin is the blockchain!

Blockchain is immutable!

Blockchain contains the truth!

Smart contracts are running on the blockchain.

Cryptocurrencies are useless, but blockchain is good!

Blockchain is secure!

Confusing, isn't it? To get better understanding and to be able to decide which statement is true, follow this presentation series!

Outline of the whole series

Blockchain matters

- Little steps to the beginning
- The born of the technology
- Bitcoin, why is it so important?
- OK, so what is blockchain? And what is DLT?
- Consensus mechanisms
- Oracles
- Ethereum, the world computer
- Smart contracts
- Tokens and the digitization of physical objects, NFTs, SFTs
- The tsunami of cryptocurrencies
- ICO, IEO, STO, CeFi/DeFi, DID and other buzzwords
- The enterprise answer: consortium/private blockchain solutions
- When can/should I use blockchain? - The blockchain solution feasibility chart
- Possible use cases

Notation of references

References related to a slide are listed at the bottom of the slide, or right next to the text.

Visual Capitalist, G. Bhutada, “Purchasing Power of the U.S. Dollar Over Time”, 2021, url.

EOS, url

Solana, url

CertiK, “The Blockchain Trilemma: Decentralized, Scalable, and Secure?”, 2019, url

Blockchain matters

Part 1 - Introduction

Little steps to the beginning

Blockchain matters

Why gold was important?

- **Only that country is powerful, whose money is hard** (Roman Empire until 54 AD, Byzantine Empire until 1042, Matthias Rex' Hungarian Kingdom, today's Switzerland)
- The country whose money is weak will finally fail (Yap Island after David O'Keefe „money import" in 1871, Roman Empire after 284 AD, Byzantine Empire in 1453)
- Only that money is hard, whose stock growth rate is small. Gold is good, silver is not!
- Money pegged to gold would be (and was) good enough!

S. Ammous, "The Bitcoin Standard: The Decentralized Alternative to Central Banking", 2018, url

Little steps to the beginning

Blockchain matters

Financial crisis in 1929

- 1717: gold standard first introduced in British Empire (Isaac Newton)
- 1880-1914: gold standard: thriving trade, easily convertible gold-based national currencies, wealth
- WW1: the gold standard is temporarily suspended, because war expenses covered by newly printed money (without gold as collateral) -> convertibility disappeared
- 1922 Genova Conference: partial return to gold standard, but USD and GBP can be a reserve currency.
- Due to the money printing in WW1, USD became harder than GBP -> gold was flowing to the USA.
- Sir Montagu Norman forces American colleagues to increase money supply, they wanted to stop gold migration to the USA -> Inflation policy in the USA.
  - The consequence of the inflation policy was a real estate and stock market bubble.
  - The government stops inflation policy in 1928 but it was too late… The result was the financial crisis in 1929.
- Recession
  - New Deal (Hoover, Roosevelt): gold standard suspended, interventionist policy, price regulations, but that is contra-productive…
    - There was surplus from some goods, but deficit from the others…
    - Certain agricultural goods were burnt… Unemployment because employer could not employ them due to the high obligatory minimum salary…
  - Gold standard was blamed, Roosevelt forbade to own gold, obligatory selling gold to the government, than USD was devaluated USD by 41%.

S. Ammous, “The Bitcoin Standard: The Decentralized Alternative to Central Banking”, 2018, url

Little steps to the beginning

Blockchain matters

Financial crisis in 2008

- 1944 Bretton Woods: new international monetary system
  - National gold reserves moved to the USA and USA undertook to change USD to gold anytime at a fixed rate. “Dollar as good as gold”, “Gold exchange window”. Other countries promised that they tried to keep their national currency to USD rate fixed.
  - But, national currency rates were permitted to change :) IMF became the regulator, USD became the reserve currency.
- Finally Bretton Woods didn’t work, because USA printed uncovered dollars, it was suspicious to other countries. They wanted to change dollars back to gold. (Charles de Gaulle sent soldiers to New York to bring national gold home.)
- 1971: End of Bretton Woods: “Floating currency rates” in Europe, Nixon stopped the fixed rate USD - gold conversion, final end of gold standard.
- Loan money, fiat money (fiat in latin = let it be)
- 2008: Financial crisis
  - FannyMae and FreddieMac, secondary mortgage market, sub-prime mortgages, MBS, CDO, synthetic CDO...
  - Lehman Brothers bankrupt on the 15th of September
  - Trust in the banking system is damaged (“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks” – Bitcoin genesis block)

S. Ammous, “The Bitcoin Standard: The Decentralized Alternative to Central Banking”, 2018, url

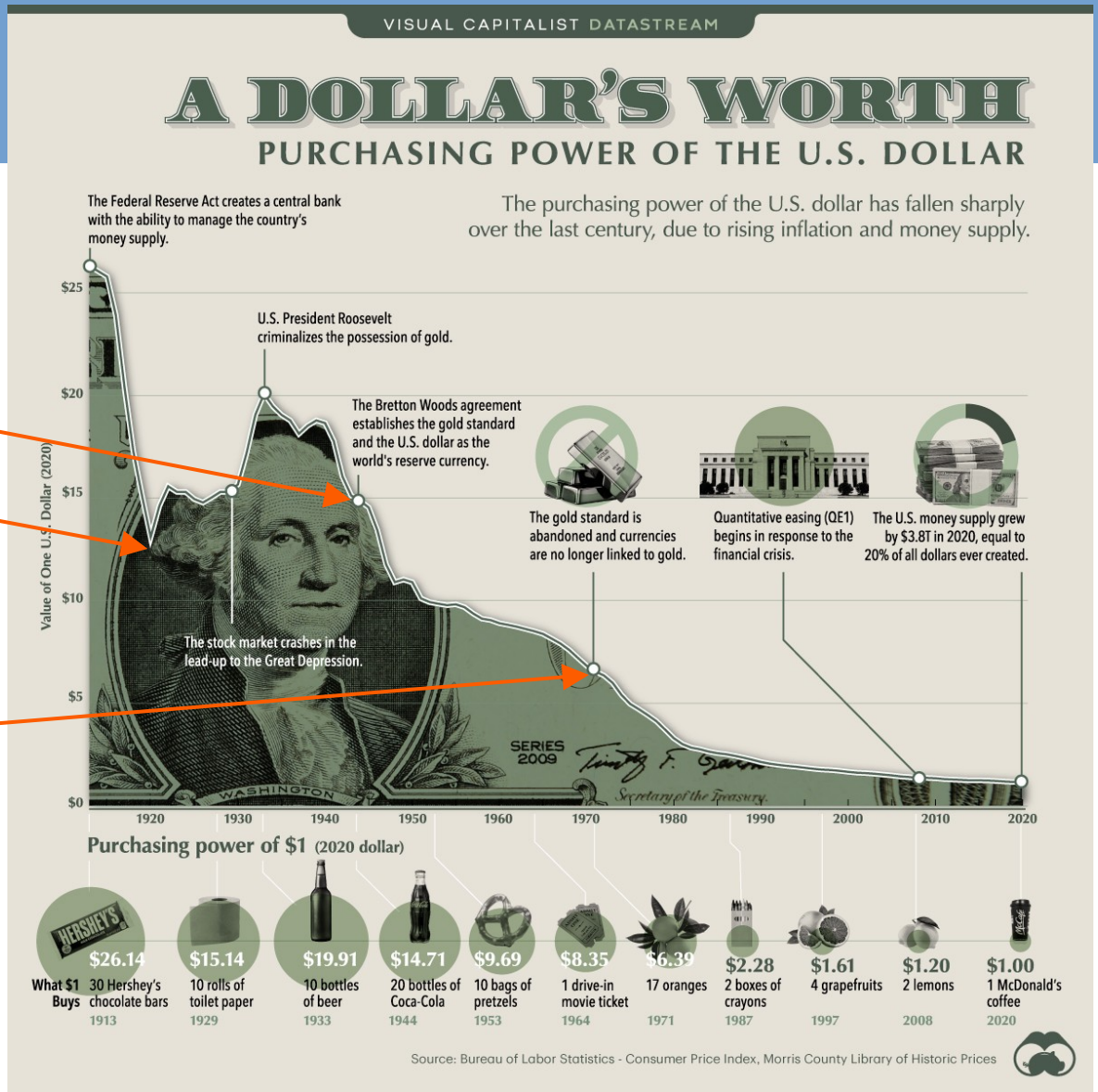
Little steps to the beginning

- General disappointment in the banking system.
- Disappointment in irresponsible monetary policies.
- The irresponsible banking and monetary policies lead to inflation and/or periodical financial crises.
- Fake news everywhere!
- People are hungry for the trust!

1944, Bretton Woods

1922, Genova Conference

1971, End of Bretton Woods

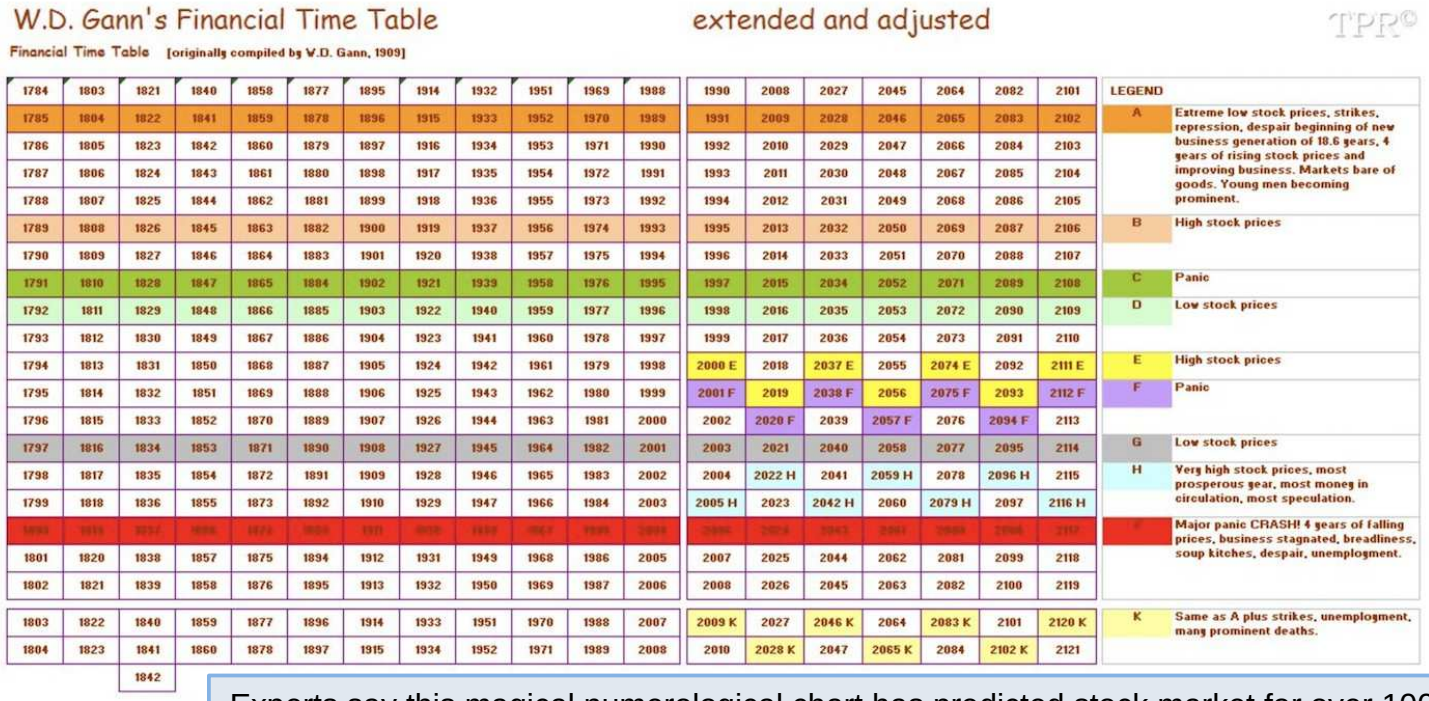


Visual Capitalist, G. Bhutada, "Purchasing Power of the U.S. Dollar Over Time", 2021, url.

W.D.Gann's Financial Time Table

Blockchain matters

- W.D.Gann noticed the 18 year periodicity of financial markets and created a prediction table in 1908 (the table on the left).
- The extended and adjusted (delay caused by the two World Wars) table in the right.



W.D. Gann's Financial Time Table — extended and adjusted

Financial Time Table [originally compiled by W.D. Gann, 1909]

1784	1803	1821	1840	1858	1877	1895	1914	1932	1951	1969	1988
1785	1804	1822	1841	1859	1878	1896	1915	1933	1952	1970	1989
1786	1805	1823	1842	1860	1879	1897	1916	1934	1953	1971	1990
1787	1806	1824	1843	1861	1880	1898	1917	1935	1954	1972	1991
1788	1807	1825	1844	1862	1881	1899	1918	1936	1955	1973	1992
1789	1808	1826	1845	1863	1882	1900	1919	1937	1956	1974	1993
1790	1809	1827	1846	1864	1883	1901	1920	1938	1957	1975	1994
1791	1810	1828	1847	1865	1884	1902	1921	1939	1958	1976	1995
1792	1811	1829	1848	1866	1885	1903	1922	1940	1959	1977	1996
1793	1812	1830	1849	1867	1886	1904	1923	1941	1960	1978	1997
1794	1813	1831	1850	1868	1887	1905	1924	1942	1961	1979	1998
1795	1814	1832	1851	1869	1888	1906	1925	1943	1962	1980	1999
1796	1815	1833	1852	1870	1889	1907	1926	1944	1963	1981	2000
1797	1816	1834	1853	1871	1890	1908	1927	1945	1964	1982	2001
1798	1817	1835	1854	1872	1891	1909	1928	1946	1965	1983	2002
1799	1818	1836	1855	1873	1892	1910	1929	1947	1966	1984	2003
[illegible]											
1801	1820	1838	1857	1875	1894	1912	1931	1949	1968	1986	2005
1802	1821	1839	1858	1876	1895	1913	1932	1950	1969	1987	2006
1803	1822	1840	1859	1877	1896	1914	1933	1951	1970	1988	2007
1804	1823	1841	1860	1878	1897	1915	1934	1952	1971	1989	2008
		1842									

1990	2008	2027	2045	2064	2082	2101
1991	2009	2028	2046	2065	2083	2102
1992	2010	2029	2047	2066	2084	2103
1993	2011	2030	2048	2067	2085	2104
1994	2012	2031	2049	2068	2086	2105
1995	2013	2032	2050	2069	2087	2106
1996	2014	2033	2051	2070	2088	2107
1997	2015	2034	2052	2071	2089	2108
1998	2016	2035	2053	2072	2090	2109
1999	2017	2036	2054	2073	2091	2110
2000 E	2018	2037 E	2055	2074 E	2092	2111 E
2001 F	2019	2038 F	2056	2075 F	2093	2112 F
2002	2020 F	2039	2057 F	2076	2094 F	2113
2003	2021	2040	2058	2077	2095	2114
2004	2022 H	2041	2059 H	2078	2096 H	2115
2005 H	2023	2042 H	2060	2079 H	2097	2116 H
[illegible]						
2007	2025	2044	2062	2081	2099	2118
2008	2026	2045	2063	2082	2100	2119
2009 K	2027	2046 K	2064	2083 K	2101	2120 K
2010	2028 K	2047	2065 K	2084	2102 K	2121

LEGEND

A	Extreme low stock prices, strikes, repression, despair beginning of new business generation of 18.6 years, 4 years of rising stock prices and improving business. Markets bare of goods. Young men becoming prominent.
B	High stock prices
C	Panic
D	Low stock prices
E	High stock prices
F	Panic
G	Low stock prices
H	Very high stock prices, most prosperous year, most money in circulation, most speculation.
I	Major panic CRASH! 4 years of falling prices, business stagnated, breadliness, soup kitches, despair, unemplogment.
K	Same as A plus strikes, unemplogment, many prominent deaths.

Experts say this magical numerological chart has predicted stock market for over 100 years, 2016, url.

W.D.Gann's Financial Time Table

Blockchain matters

Explanation

- Generally
  - Cycle begins with new generation of traders
  - First 5 years: slow grow -> high stock prices, then first panic
  - Down and up, then second panic
  - To the moon! :) , then final panic, purgatory of the market
- Current cycle
  - Began after the 2008 financial crisis
  - After 2010: fintech, tech, startup revolution (young generation)
  - 2015: first panic (S&P500: -15% after five years of strictly increasing)
  - 2017-2018: go up
  - 2020: correction, second panic (COVID), S&P500: -30%
  - What is coming? :)

1988	1990	2008
1989	1991	2009
1990	1992	2010
1991	1993	2011
1992	1994	2012
1993	1995	2013
1994	1996	2014
1995	1997	2015
1996	1998	2016
1997	1999	2017
1998	2000 E	2018
1999	2001 F	2019
2000	2002	2020 F
2001	2003	2021
2002	2004	2022 H
2003	2005 H	2023
2005	2007	2025
2006	2008	2026
2007	2009 K	2027
2008	2010	2028 K

LEGEND	
A	Extreme low stock prices, strikes, repression, despair beginning of new business generation of 18.6 years, 4 years of rising stock prices and improving business. Markets bare of goods. Young men becoming prominent.
B	High stock prices
C	Panic
D	Low stock prices
E	High stock prices
F	Panic
G	Low stock prices
H	Very high stock prices, most prosperous year, most money in circulation, most speculation.
	Major panic CRASH! 4 years of falling prices, business stagnated, breadliness, soup kitches, despair, unemplogment.
K	Same as A plus strikes, unemplogment, many prominent deaths.

The born of the technology, the pre-Bitcoin ages

Blockchain matters

- Approx. 100 AD – 476 AD: Roman Empire: first paper based DLT
- Approx. 1000 AD: YAP Island, Rai stones: kind of DLT
- 1982: Leslie Lamport, Robert Shost, Marshall Pease: describing Byzantine General Problem
- 1991: Stuart Haber, W. Scott Stornetta, “How to Time-Stamp a Digital Document”: time-stamping of digital document
- 1993: Cynthia Dwork, Moni Naor, “Pricing via processing or combatting junk mail”: PoW for deterring DoS attacks/spams by requiring some work from the service requester
- 1995: David Chaum’s Digicash: centralized, never realized!
- 2002: David Maziéres, Dennis Sasha, “Building secure file systems out of Byzantine storage”: basics of chain of blocks (blockchain) as data storage in a multi-user file system.
- 2005: Nick Sabo’s BitGold, PoW, but doesn’t solve double spending problem, never realized!
- 2008: Satoshi Nakamoto’s Bitcoin: decentralized, solves double spending and byzantine general problem, blockchain technology

Double Spending and Byzantine General Problem

Blockchain matters

- Double Spending: when usual digital data (i.e. a file) is sent from one computer to an other, the data is duplicated. This means that the original data can be sent again (and again). This is double s(p)ending, which is a huge problem if the digital data is money.
- Byzantine General Problem: in a distributed system, e.g. in case of a scattered army:
  - Coordinated attack leads to victory
  - Uncoordinated attack leads to defeat

Blockchain matters

Coming up next: Bitcoin

Blockchain matters

Thank you!

If you liked this material you can tip me

Blockchain matters

- Bitcoin: *3FvgmYScorEje3WTrdDn5synEU6j917SZz*
- Litecoin: *ltc1qs457h3899qj4yry8k6u5xva79wa8f6xspant4e*
- Ethereum: *0xdF7eAab54BC9070a140D0251247406cEe40029B7*
- QTUM: *MGo31aQ74yHJ9Lan4tgYeFy5XhtHZuoimQ*
- Tezos: *tz1VpDWz45fvqv69Laa6YVa3h6MtkCoq1BDc*

Blockchain matters

Thank you again!