

Theory of Blockchain



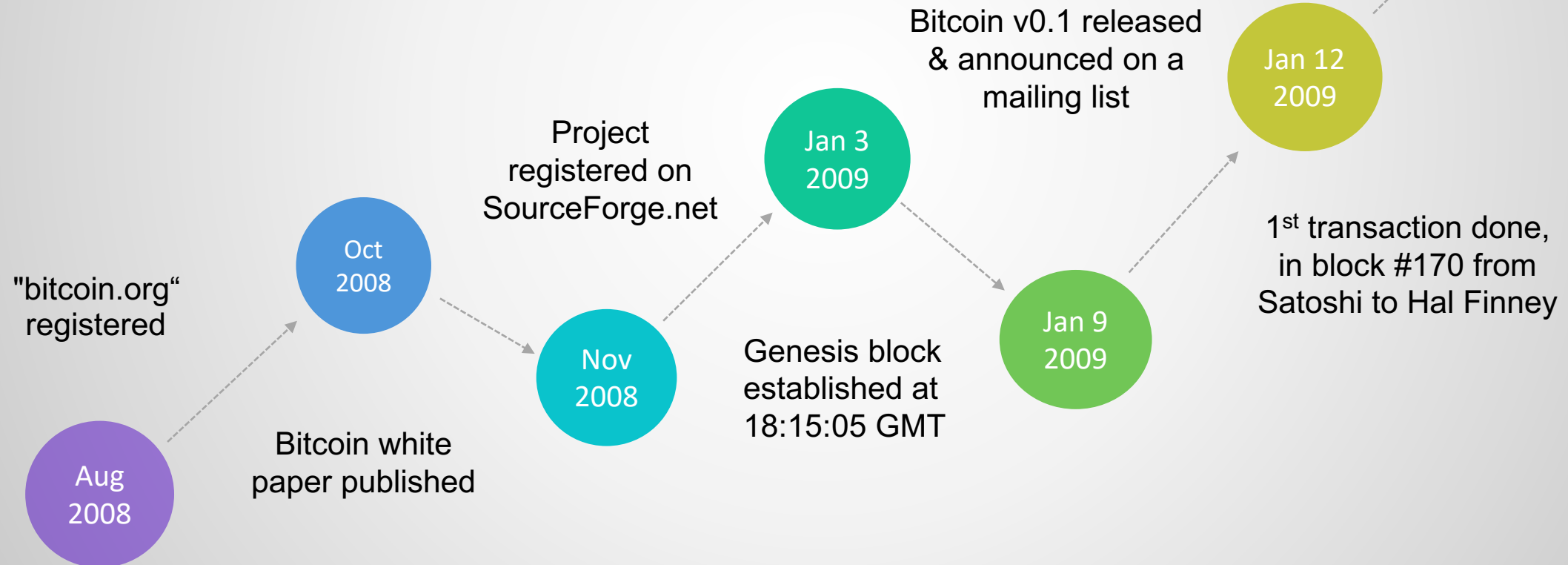
Session 1:

Fundamental Security Concepts

Module 1 - History and Motivation

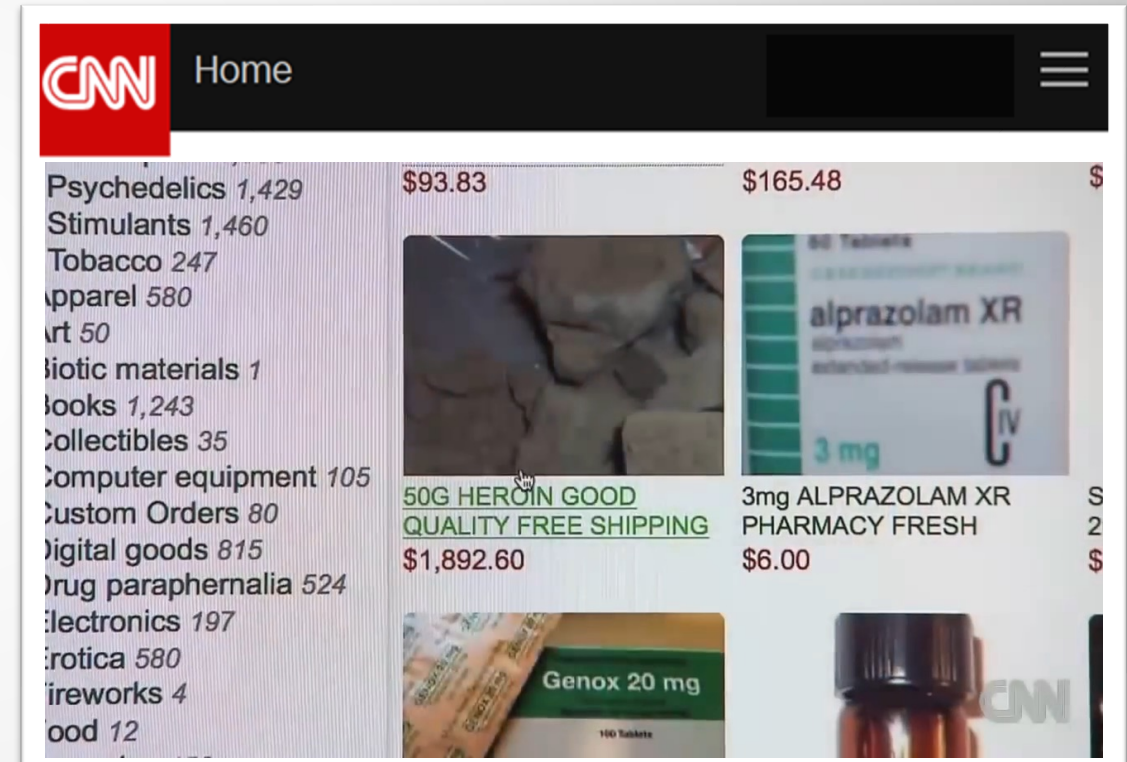
How did everything start?

We had “Hash Chains” in cryptography before. But the notion of blockchain came to surface with Satoshi Nakamoto’s white paper in 2008.




How did it become famous?

- Silk Road was one of the first online black markets that used Bitcoin and TOR technologies for anonymity.
- Silk Road was shut down in 2013 and the admin (Ross Ulbricht) was arrested. He was sentenced to life in prison!
- Not all the credit for Bitcoin's fame goes to Silk Road. The 2017's price surge was also a big shot.



Usage example: Anonymous p2p spending !


 **Silk Road**
anonymous market


messages 1 | orders 0 | account \$0.00


Search Go

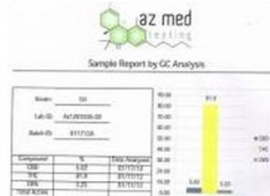
Shop by Category


- Drugs 2,399
 - Cannabis 341
 - Dissociatives 65
 - Ecstasy 209
 - Opioids 156
 - Other 144
 - Precursors 12
 - Prescription 526
 - Psychedelics 427
 - Stimulants 273
- Apparel 114
- Art 7
- Books 743
- Collectibles 12
- Computer equipment 19
- Custom Orders 26
- Digital goods 310
- Drug paraphernalia 89
- Electronics 20
- Erotica 319
- Fireworks 2
- Food 3
- Forgeries 58
- Hardware 2
- Home & Garden 7
- Jewelry 48
- Lab Supplies 5
- Lotteries & games 29
- Medical 5


5x - 10mg Dexedrine (Pure Dextroamphetamine)

\$4.94


2 x 0,25 mg Xanax (Alprazolam)

\$1.50


Malana charas hand rubbed Indian hash 100g

\$75.83


1 Gram OG KUSH OIL 81% THC 90% TOTAL

\$4.13


14 grams (1/2 Ounce) of Nebula JWH-122

\$2.63


3.5g Crystal Meth Ice Shards

\$31.92


20 x 25mg Cialis

\$2.57

!!!...Psilocybe-Cubensis-Chocolate...!!!

\$18.15









100 x Orange Star Very high MDMA content 180mg

\$50.00

100x 200mg White XTC 'Speakers'

\$20.00

3g Methylone Crystals -Lab Grade

\$15.00

15mg Adderall Extended Release (1 Capsule)

\$1.00

Usage example: Anonymous p2p spending !

 <p>glock 19c gen3 9mm Seller: Bubba Jones(100) Ship from: United States of America 2250.00 USD Detail</p>	 <p>BRAND NEW romanian ak47 7.62 with AMMO Seller: Bubba Jones(100) Ship from: United States of America 3000.00 USD Detail</p>	 <p>BRAND NEW heckler & koch g3 308 Seller: Bubba Jones(100) Ship from: Worldwide 4000.00 USD Detail</p>	 <p>saiga 308 custom Seller: Bubba Jones(100) Ship from: United States of America 4000.00 USD Detail</p>
 <p>glock 39 gen3 .45gap Seller: Bubba Jones(100) Ship from: United States of America 2500.00 USD Detail</p>	 <p>beretta px4 compact 9mm Seller: Bubba Jones(100) Ship from: Worldwide 1800.00 USD Detail</p>	 <p>colt ar15 magpul upgrades .223/5.56 NATO Seller: Bubba Jones(100) Ship from: United States of America 2350.00 USD Detail</p>	 <p>124 gr FMJ - WOLF CLASSIC - 1000 Rounds - 7.62x39MM Seller: Bubba Jones(100) Ship from: United States of America 500.00 USD Detail</p>

Bitcoin Whitepaper – 2008

Bitcoin: A Peer-to-Peer Electronic Cash System

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

Not even a real name

A Free Email Provider

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.

Market Capital of Major Cryptocurrencies

Rank	Name (Symbol)	Market Cap (\$)
1	Bitcoin (BTC)	543,035,122,099
2	Ethereum (ETH)	228,645,154,972
3	Tether (USDT)	80,104,006,725
4	BNB (BNB)	49,406,614,75

as of April 2023

Blockchains/Cryptos are Widely Accepted



What Comes Next ...

- In the “Theory of Blockchain” you will obtain an in-depth knowledge about the internals of blockchains and cryptos.
- To be able to understand the subsequent topics, you need to learn the basics of security and cryptography first.
 - Cryptocurrencies are “Cryptographic” after all, just as the name says.

See you in the next video ...