SWINBURNE UNIVERSITY OF TECHNOLOGY

Theory of Blockchain

Session 1:

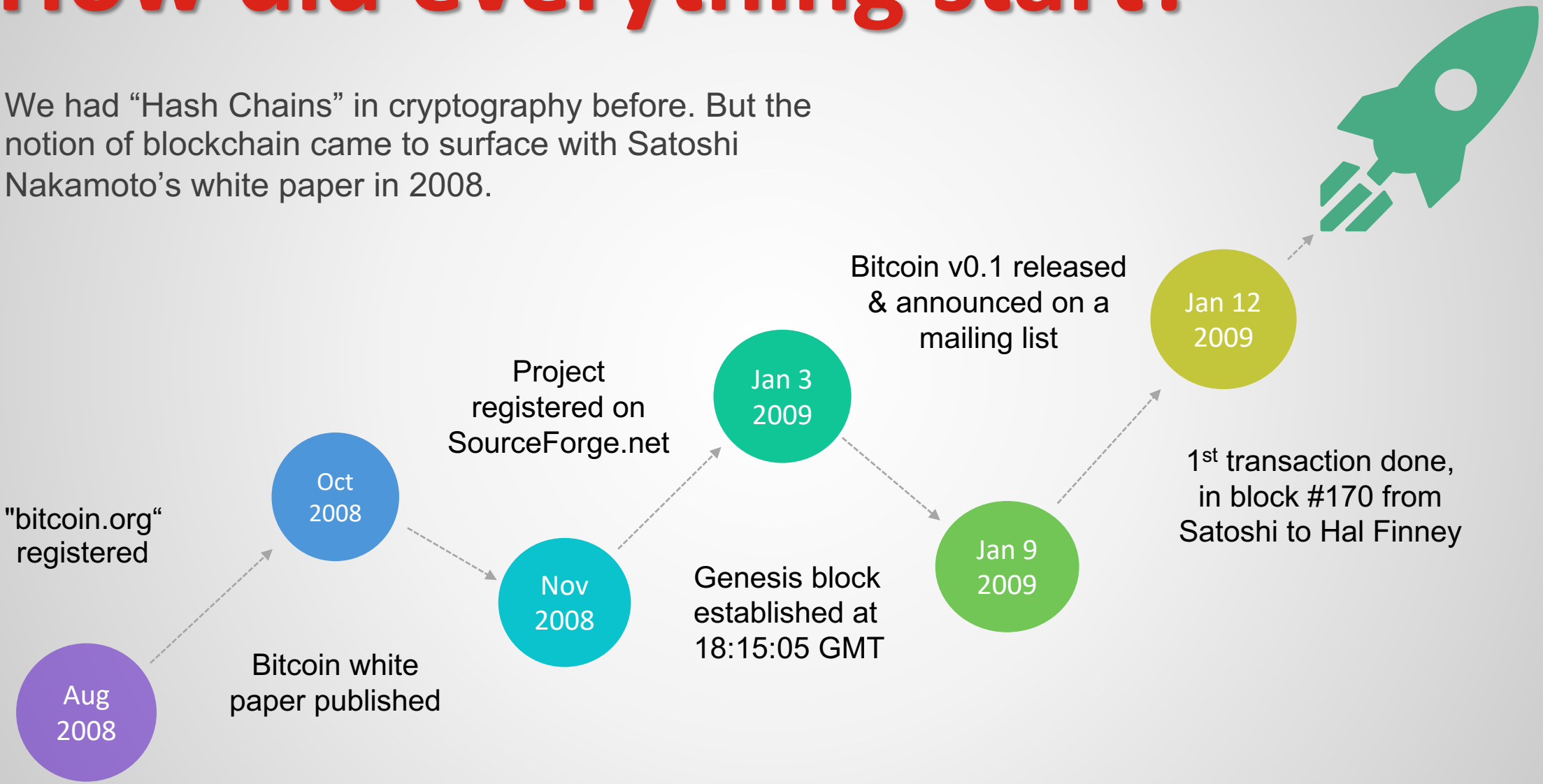
Fundamental Security Concepts

Module 1 - History and Motivation

Sayad Haghighi

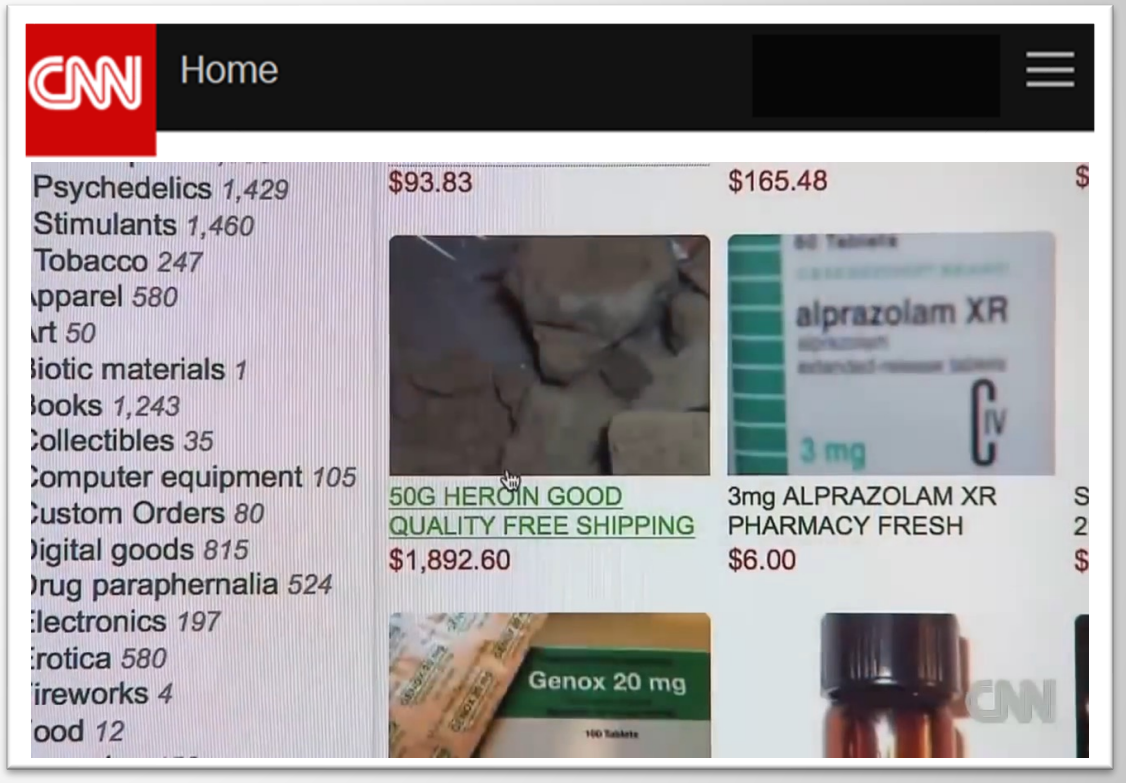
How did everything start?

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

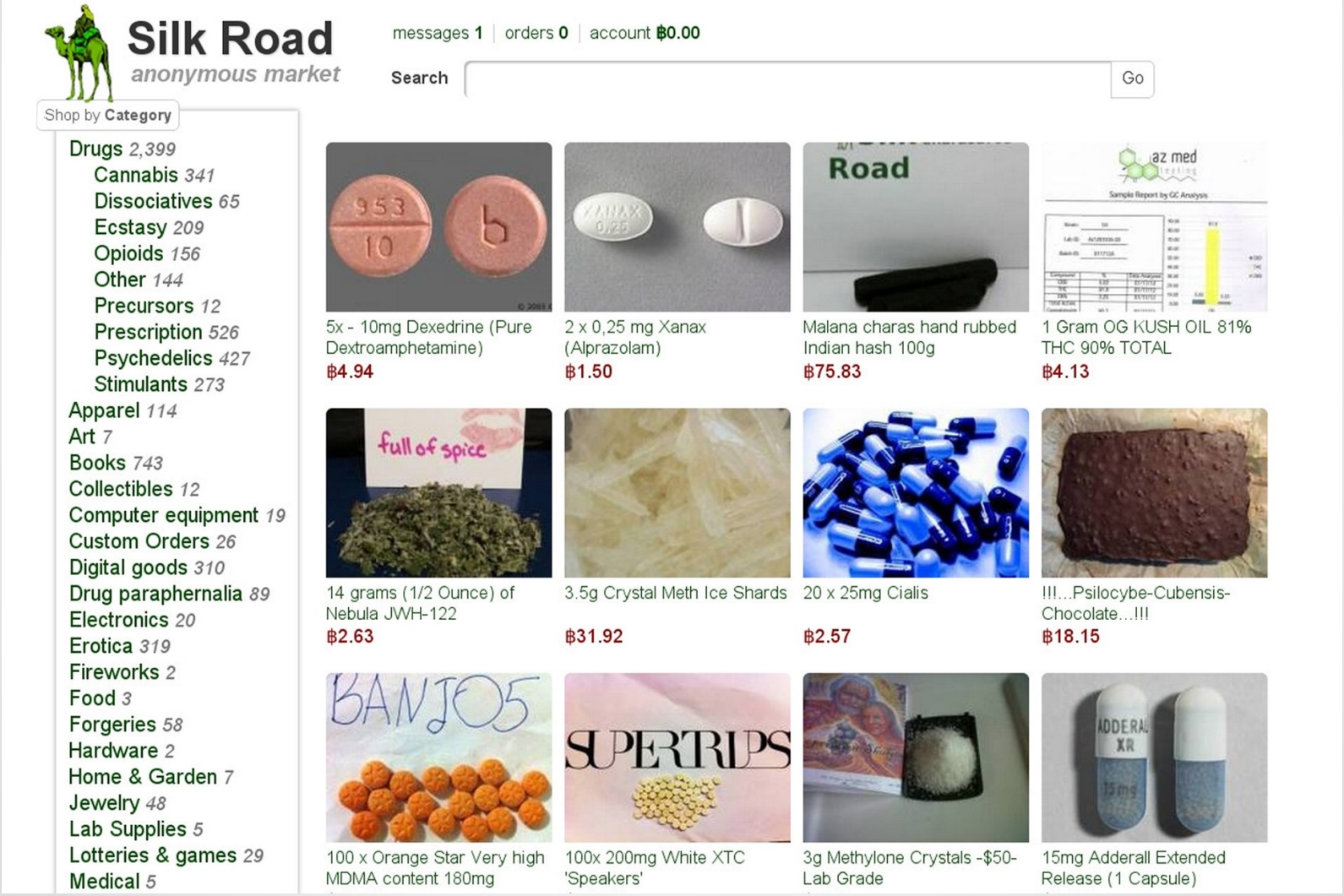


How did it become famous?

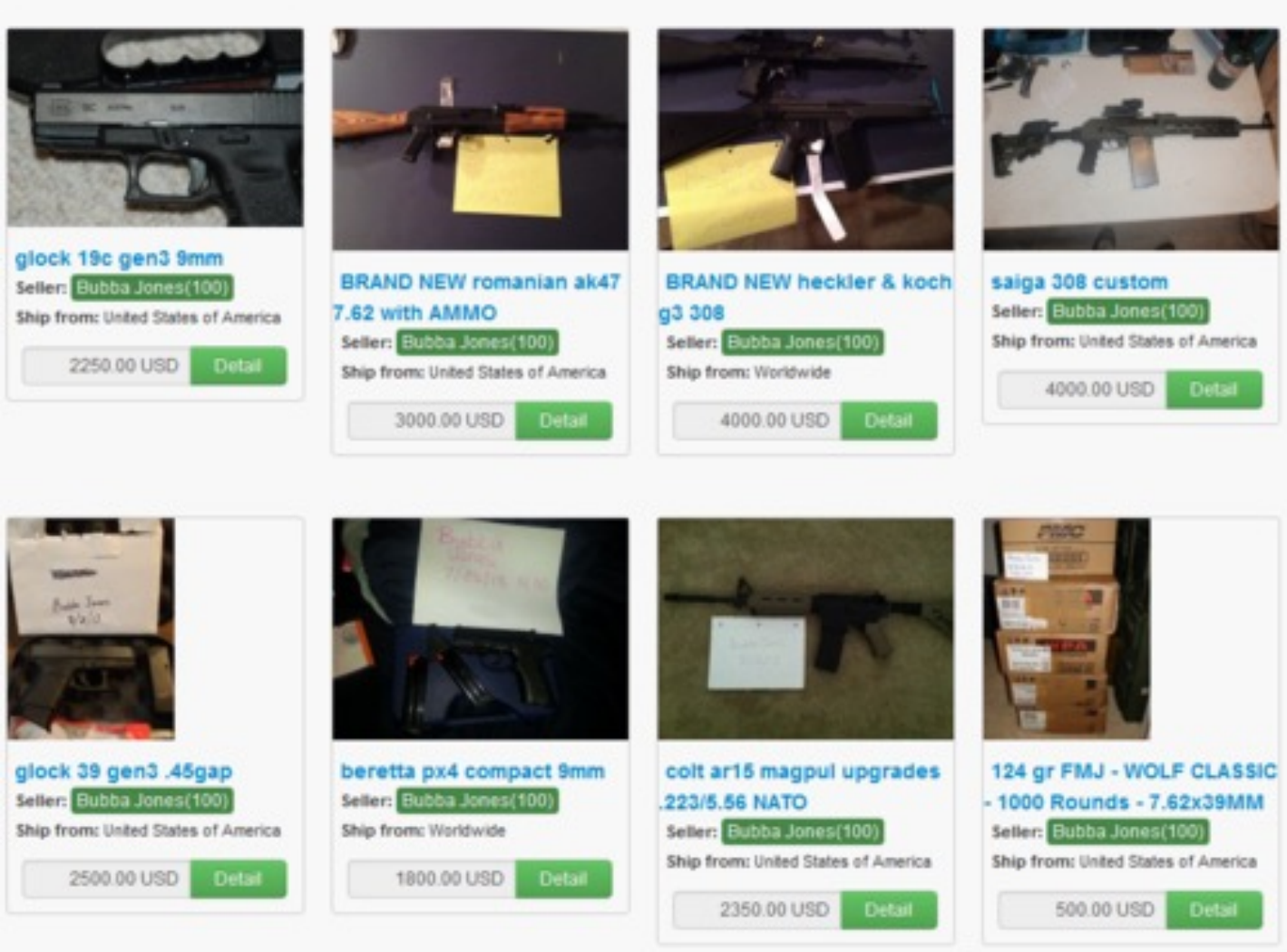
- Silk Road was one of the first online black markets that used Bitcoin and TOR technologies for anonymity.
- Silk Road was shut down in 2013 and the admin (Ross Ulbricht) was arrested. He was sentenced to life in prison!
- Not all the credit for Bitcoin's fame goes to Silk Road. The 2017's price surge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



Usage example: Anonymous p2p spending !



Usage example: Anonymous p2p spending !



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

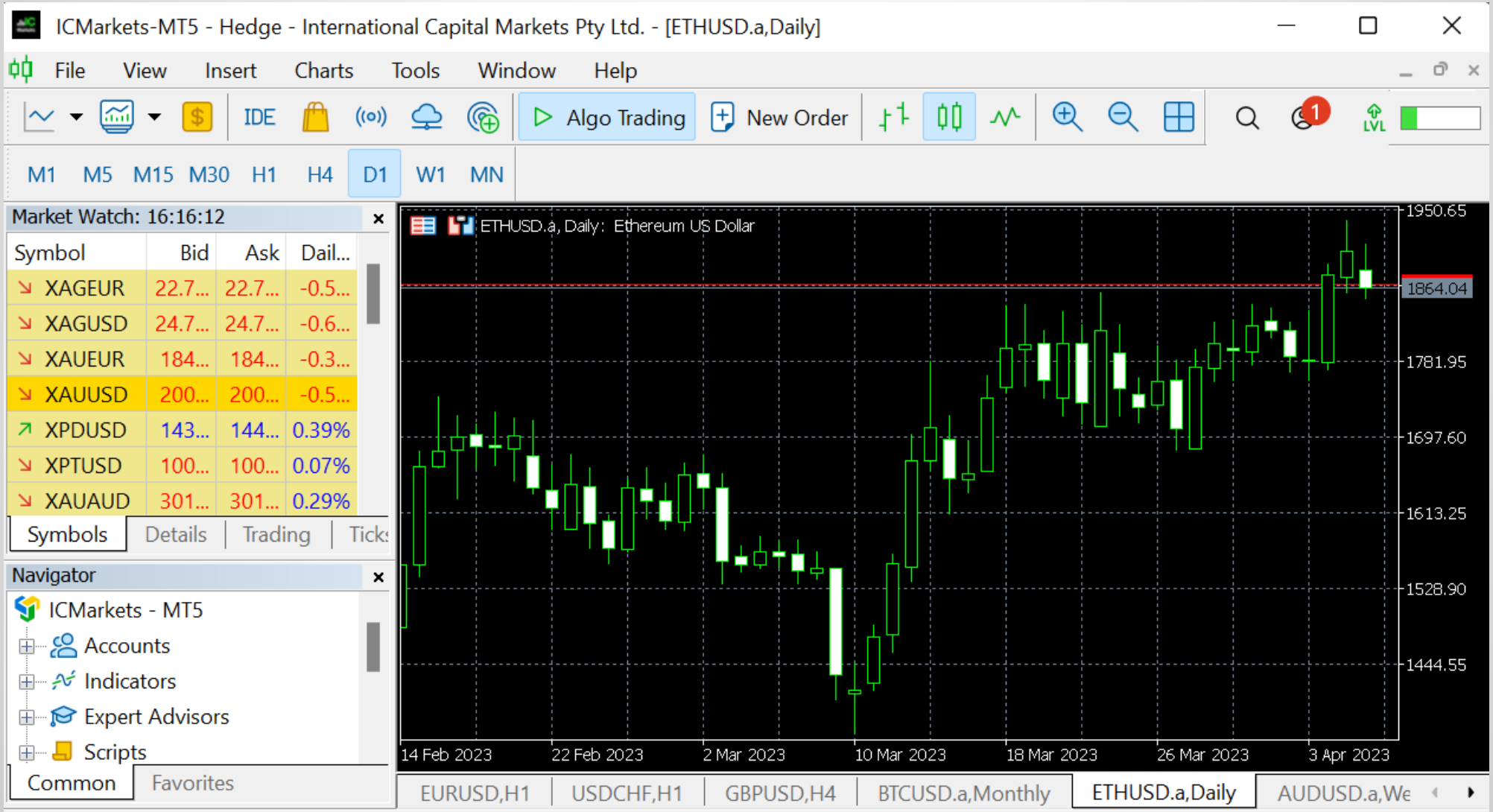
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required 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 …