Lecture 20: A Grand Tour of Altcoins

Bill Laboon

Image: "Promenade de la Galerie du Palais Royal," by Philibert-Louis Debucourt after Claude-Louis Desrais

What is a Grand Tour?

- A tour around Europe, taken by aristocratic or well-off young men and women
- Allowed them to be briefly exposed to a variety of cultures, antiquities, and societies
- Generally done with the company of a *cicerone*, or guide

Image: "Francis Basset, 1st Baron de Dunstanville" by Pompeo Batoni

What is an altcoin?

- Generally speaking, any cryptocurrency which is not Bitcoin

- Many (most?) are simple cut-and-paste jobs or scams…

- … but some attempt to improve upon Bitcoin or make different trade-offs

Image: "A Money Scrivener" by Thomas Rowlandson

Bitcoin Strengths

- Ludicrously secure
- Technologically conservative, battle-tested
- Inflation-proof: only 21 million bitcoin will ever be mined
- Mind share: when people think "cryptocurrency," they think "Bitcoin"

Bitcoin Drawbacks/Trade-offs

- Relatively slow confirmation times
- Pseudonymous, not anonymous
- Simple scripting language
- Energy-inefficient
- Centralized mining (ASICs)
- Extremely large rewards to early adopters

Litecoin:

"Silver to Bitcoin's Gold"

- One of the oldest surviving altcoins - started in 2011
- Different hashing algorithm (Scrypt), blocks scheduled for 2.5 minutes instead of 10 minutes
- Acts as a testbed for new technologies (Lightning, SegWit, atomic swaps) before being added to Bitcoin

Image: "Maximilian II 1527-1576, Holy Roman Emperor" by Antonio Abondio

Monero:

“Secure, Private, Untraceable”

- Hard-forks every 6 months
- Ring signatures mask sender
- Stealth addresses mask receiver
- Thus, transactions and balances cannot be linked to individual users
- Anonymous, fungible currency

Image: “The Star of Kings, A Night Place” by Jan van de Velde II after Pieter Molijn

Ethereum:
"The World Computer"

- Supports Turing-complete (extremely powerful and expressive) programming
- Can run smart contracts and other "distributed applications" (dapps)
- Very fast (~ 20 seconds) confirmation times

Image: "Lady Wearing Spectacles" by Anonymous (America, c. 1840)

Cardano:

"A More Secure Ethereum"

- Similar to Ethereum - develop dapps and smart contracts which can be run and trusted

- Focuses less on usability, more on security

- Written in Haskell and allows formally verified smart contracts

Image: "The Teacher, The Clergyman, and Providence" by Albrecht Durer (detail)

Nano:

“Instant, Zero-Fee, Scalable”

- Every node has its own blockchain
- Coins already distributed - no mining
- Uses proof-of-stake instead of proof-of-work
- Updates occur via a single TCP packet - extremely fast and no fees for transfer

Image: “A Cart Race” by Thomas Rowlandson

Vertcoin:
"The People's Coin"

- Everybody can mine using a regular computer (no ASICs)
- Core development team has vowed that if an ASIC is developed for it, they will change the hashing algorithm
- Along with Litecoin, acts as a testbed for new technologies

Image: "The Worker and Kholkoz Woman", statue by Vera Mukhina, photo by Nathan Powell

Dogecoin:
"The People's Coin"

- Started as a joke cryptocurrency, but reached a peak value of more than two billion US dollars

- Often used for tipping for comments on Reddit or other social media sites

- Inflationary - ~ 5.2 billion new dogecoins produced every year

- The most stable coin - 1 DOGE = 1 DOGE

Image: "Doxe (Doge)" by Unknown (Master of the E-Series Tarocchi)

Ripple/XRP:
"The Banker's Coin"

- Ripple is a company which operates several kinds of credit settlement software

- XRP is a particular cryptocurrency which can be used as a settlement currency for Ripple system

- Ripple does not need XRP, and vice versa

- Consensus via voting, but Sybil attacks by deciding to trust a certain subset of possible Ripple nodes - much more efficient but also generally less secure

Image: "The Moneychanger and His Wife" by Marinus van Reymerswaele

Hyperledger:

"Blockchain Not Cryptocurrency"

- Hyperledger is a series of systems that allow users to make their own permissioned blockchains
- You choose who can join your blockchain - lots of efficiency gains to be made from this
- No currency inherent in the system - meant for specific use cases and industries

Image: "Portait of Luca Pacioli" attributed to Jacopo de' Barbari,

Dentacoin:

"The Blockchain Solution for the Global Dental Industry"

- A cryptocurrency meant for a specific use case, viz., dental offices
- Can get DentaCoins by providing dental reviews, doing dental research, or taking care of your teeth
- It's an ... unusual cryptocurrency but still going strong

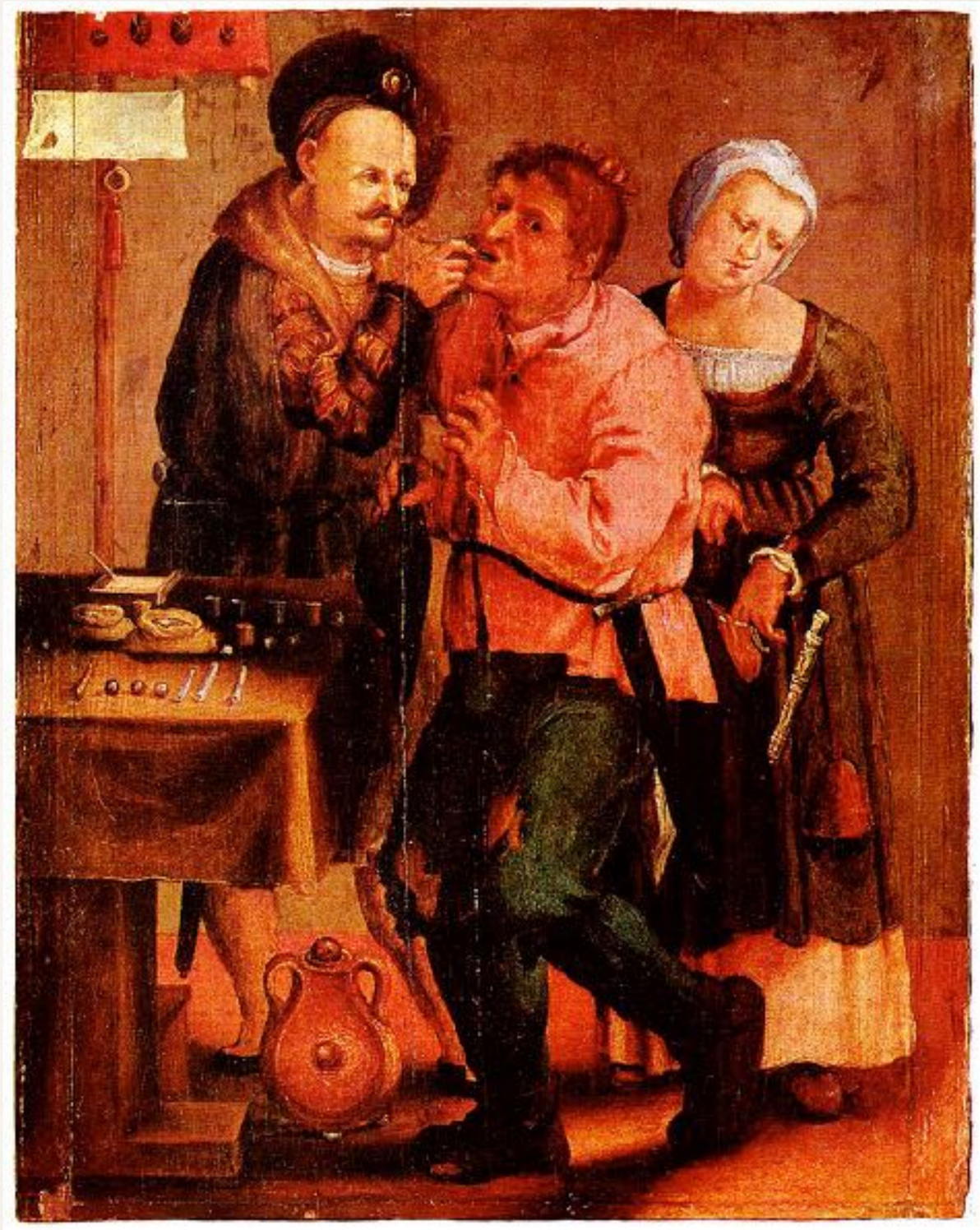

Image: "Farmer at the Dentist" by Johann Liss

The Future

- Is Bitcoin “digital gold”?
- Is it “the MySpace of cryptocurrency”?
- Or something else entirely?

Image: “Man of Science” by Anonymous (American, 19th c.)

All images courtesy of the
National Gallery of Art, Washington, D.C.

except

“Francis Basset, 1st Baron de Dunstanville” and
"The Moneychanger and His Wife",
courtesy of Museo del Prado, Madrid

and

“Picture of Worker and Kholkoz Woman”, courtesy of
Nathan Powell (Wikipedia username: limitchik)