bitcoin

CS1699: Blockchain Technology and Cryptocurrency

22. The Road Ahead

Bill Laboon

Technical and Societal

- Blockchain technology is changing our world
- Blockchain technology is itself changing
- Better security, more use cases, enhanced privacy, different trade-offs, improved usability, etc.

Staying Up To Date

- Bitcoin Optech Newsletter - https://bitcoinops.org/en/newsletters/
- News: Bitcoin News (https://news.bitcoin.com/), Cointelegraph (https://cointelegraph.com/), CCN (prev. CryptoCoinNews (https://www.ccn.com/),
- Analysis: Brave New Coin (https://bravenewcoin.com/), ICO Alert (https://www.icoalert.com/en/)
- Reddit: r/Bitcoin, r/BTC (Bitcoin Cash), r/Cryptocurrency, /r/BitcoinTechnology, r/Ethereum
- Jameson Lopp's Bitcoin Resources: https://lopp.net/bitcoin.html
- Twitter: @Melt_Dem , @el33th4xor , @VladZamfir ,@ethereumJoseph , @leashless , @PeterRizun , @udiWertheimer , @LukeDashjr , @jimmysong , @lopp, @naomibrockwell , @pierre_rochard , @VitalikButerin, @saifedean, @BillLaboon

SegWit

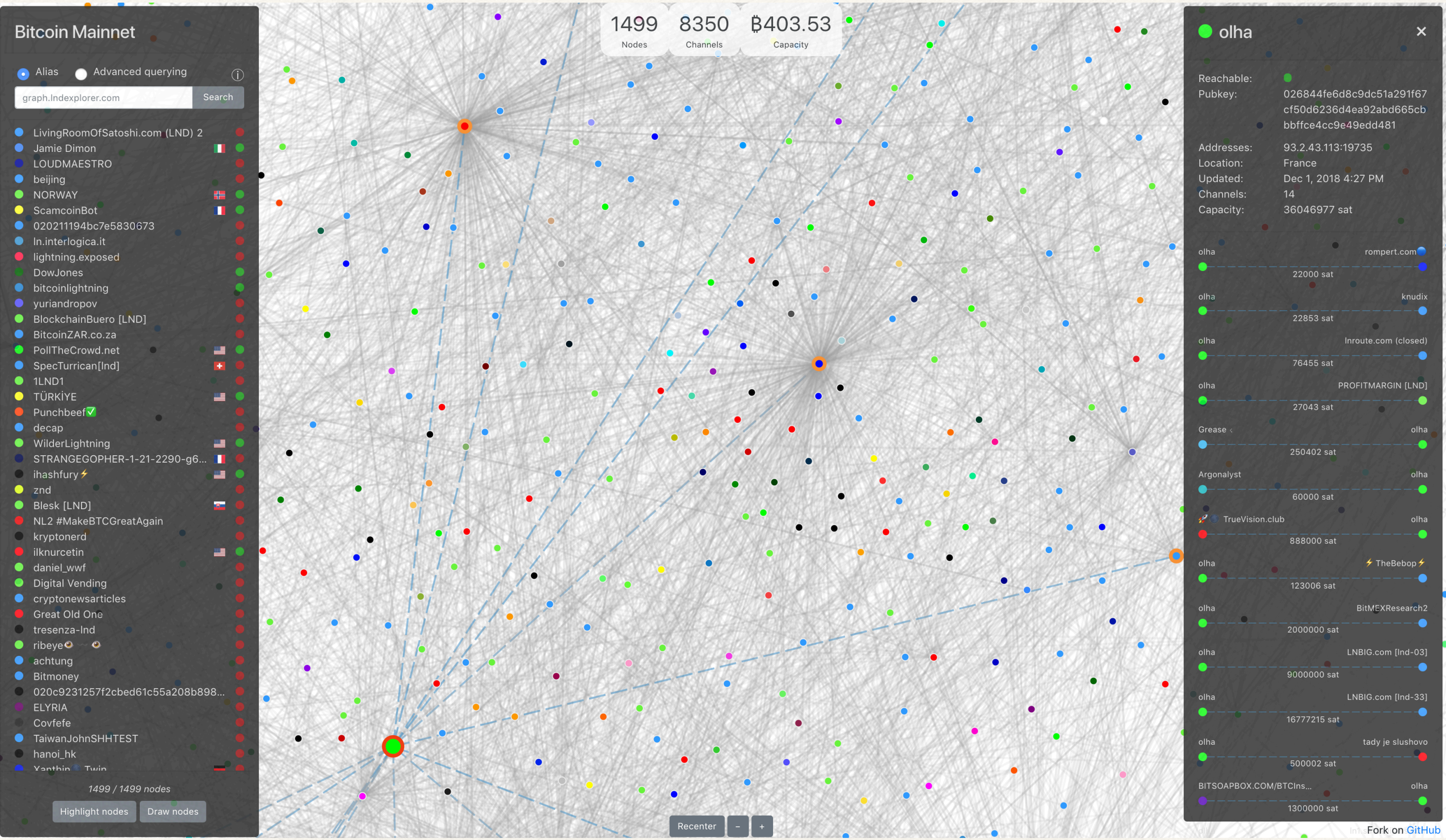
- SEGregated WITness - That is, digital signatures are stored separately from transaction data in blocks
- Originally meant as a solution to transaction malleability attacks (of Mt. Gox fame/infamy), but also reduces transaction size
- Now signatures and scripts can be changed without modifying the tx id
- Which means we can do interesting things like second-tier scaling and more complex smart contracts

SegWit and Bitcoin Cash

- The change which made Bitcoin and Bitcoin Cash split
- They both agree: SegWit allows secondary scaling!
  - Bitcoin Core - Which means that we can implement Lightning Network and other cool things!
  - Bitcoin Cash - Which means that we will have further centralization by whoever runs the secondary scaling systems and the Core Team!

Lightning Network

- Similar basic goal as Liquid - provide faster and cheaper Bitcoin transactions - but using a node-based, decentralized network instead of a sidechain
- Liquid - relatively centralized, Lightning is more like BitTorrent
- Instead of miners, nodes are paid to relay transactions, and this can be done by any full node running specialized software (in other words, your Raspberry Pi can be making you Bitcoin while you sleep)
- Home: https://lightning.network/
- Visualization: https://graph.lndexplorer.com/


Bitcoin Mainnet
Alias
Advanced querying
graph.lndexplorer.com
Search
LivingRoomOfSatoshi.com (LND) 2
Jamie Dimon
LOUDMAESTRO
beijing
NORWAY
ScamcoinBot
020211194bc7e5830673
ln.interlogica.it
lightning.exposed
DowJones
bitcoinlightning
yuriandropov
BlockchainBuero [LND]
BitcoinZAR.co.za
PollTheCrowd.net
SpecTurrican[lnd]
1LND1
TÜRKİYE
Punchbeef✅
decap
WilderLightning
STRANGEGOPHER-1-21-2290-g6...
ihashfury⚡
znd
Blesk [LND]
NL2 #MakeBTCGreatAgain
kryptonerd
ilknurcetin
daniel_wwf
Digital Vending
cryptonewsarticles
Great Old One
tresenza-lnd
ribeye
achtung
Bitmoney
020c9231257f2cbed61c55a208b898...
ELYRIA
Covfefe
TaiwanJohnSHHTEST
hanoi_hk
1499 / 1499 nodes
Highlight nodes
Draw nodes
1499 Nodes
8350 Channels
฿403.53 Capacity
Recenter
−
+
olha
Reachable:
Pubkey:
026844fe6d8c9dc51a291f67cf50d6236d4ea92abd665cbbbffce4cc9e49edd481
Addresses:
93.2.43.113:19735
Location:
France
Updated:
Dec 1, 2018 4:27 PM
Channels:
14
Capacity:
36046977 sat
olha
rompert.com
22000 sat
olha
knudix
22853 sat
olha
lnroute.com (closed)
76455 sat
olha
PROFITMARGIN [LND]
27043 sat
Grease
olha
250402 sat
Argonalyst
olha
60000 sat
TrueVision.club
olha
888000 sat
olha
⚡ TheBebop⚡
123006 sat
olha
BitMEXResearch2
2000000 sat
olha
LNBIG.com [lnd-03]
9000000 sat
olha
LNBIG.com [lnd-33]
16777215 sat
olha
tady je slushovo
500002 sat
BITSOAPBOX.COM/BTCIns...
olha
1300000 sat
Fork on GitHub

MAST

- BIP-144 - Merkleized Abstract Syntax Tree (https://github.com/bitcoin/bips/blob/master/bip-0114.mediawiki)
- Recall that Bitcoin scripts allow you to transfer your UTXOs if certain conditions are met (signatures, time-lock, knowing a value *x*, etc.) - the technical name for these are *encumbrances*
- MAST allows you to add additional encumbrances but only store the hash of certain parts of the script on-chain
- Reduces script size, allows more complex scripts, and ameliorates issue of nodes whitelisting scripts

Schnorr Signatures

- Proposed BIP: https://github.com/sipa/bips/blob/bip-schnorr/bip-schnorr.mediawiki
- Improvement over Bitcoin ECDSA but still EC crypto
- “Native multi-sig” - constant-size signatures no matter the number of participants, which also means better privacy (no way for external observers to know if sig is multi-sig)
- Also increases efficiency and capacity as a side effect (as signature will be smaller)
- Several technical and standardization issues still need to be worked - probably not coming any time soon

Bulletproofs

- Allows you to have privacy without much additional data - CoinJoin-style transactions can scale sublinearly, and with Schnorr signatures make cost for large anonymity sets… well, not trivial, but smaller
- Hide amount of transaction on blockchain (although bulletproofs by themselves keep sender/receiver addresses public)
- Already successfully implemented in Monero, but lots of (justified!) security concerns from the Bitcoin team - will probably not be implemented any time in the next few years
- See Bunz et al., *Bulletproofs: Short Proofs for Confidential Transactions and More* for more information: https://eprint.iacr.org/2017/1066.pdf

RSK

- “Ethereum on Bitcoin”
- A merge-mining Bitcoin sidechain that allows you run Solidity contracts
- 2-way peg of Bitcoin to Smart Bitcoin (S-BTC)
- https://www.rsk.co/
- https://docs.rsk.co/RSK_White_Paper-Overview.pdf

Societal Changes

- Blockchain technology is not entirely trustless..
- … but it does eliminate the need for a centralized trusted entity
- Given a few days and a modicum of computing power, **you** can verify that every single transaction that has occurred on the Bitcoin blockchain *follows the rules of Bitcoin* (that part in italics is important)

Political Decentralization

- Centralization vs decentralization is a trade-off (politics is simply a special case of software engineering, when you think about it)
- Centralization = economies of scale, large projects can be done, can impose will on bad actors
- Decentralization = many different approaches, localized preferences, resistance to tyranny
- Bitcoin provides a way to decentralize while maintaining *some* of the benefits of a centralized monetary system

Bitcoin is Sound Money

- Sound money does not have the risk of inflation
- It is not a panacea, but it can be argued that sound money is *correlated* with :
  - Lower time-preference in societies
  - Increased real innovation
  - Less likelihood of conflict
- Over the long run, hard to compete with currencies sounder than yours

Hyperbitcoinization

- If the following tenets are true:
  - Bitcoin is (at the moment) the soundest money
    - It is very difficult to compete against sounder money than yours
- then it follows that more and more people will prefer bitcoin, leading to hyperbitcoinization (the economy rapidly shedding reliance on non-Bitcoin currencies)

Non-monetary Uses of Blockchain

- Where do you want to verify facts without a centralized source of truth?
- Voting
- Real estate
- Supply chains
- Employment
- Dating!