

Consensus Changes in Bitcoin

(in 20 minutes)

LABITCONF, San Salvador
Nov 19th, 2021

John Newbery

brink

Building Bitcoin

A dark, high-contrast image of a construction site. In the foreground, the silhouettes of several construction workers are visible against a bright, cloudy sky. One worker stands prominently on the left, while others are positioned further back and to the right. A large construction crane is positioned in the upper left, its arm extending across the frame. The background is filled with the intricate structures of a building under construction, with multiple levels of scaffolding and steel beams.



Anyone can ...



Store value



Transfer value



No entity can ...



Corrupt value

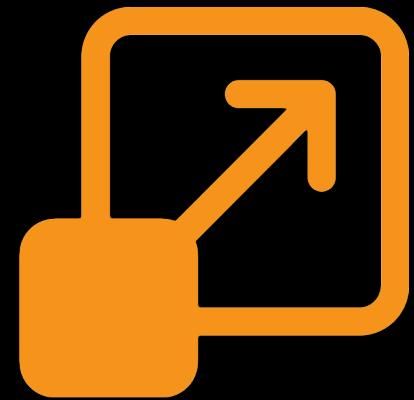


Censor transactions

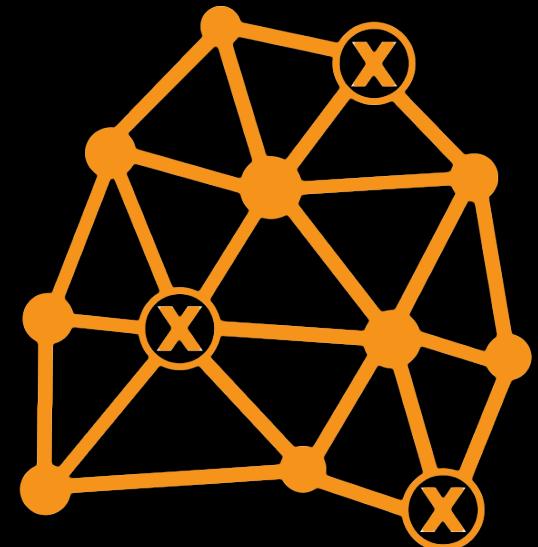
Properties



Private and Fungible



Scalable



Decentralized



Incentive-compatible

“This adds an incentive for nodes to support the network [...]”

The incentive may help encourage nodes to stay honest [...]”

He ought to find it more profitable to play by the rules”

Incentive Compatibility

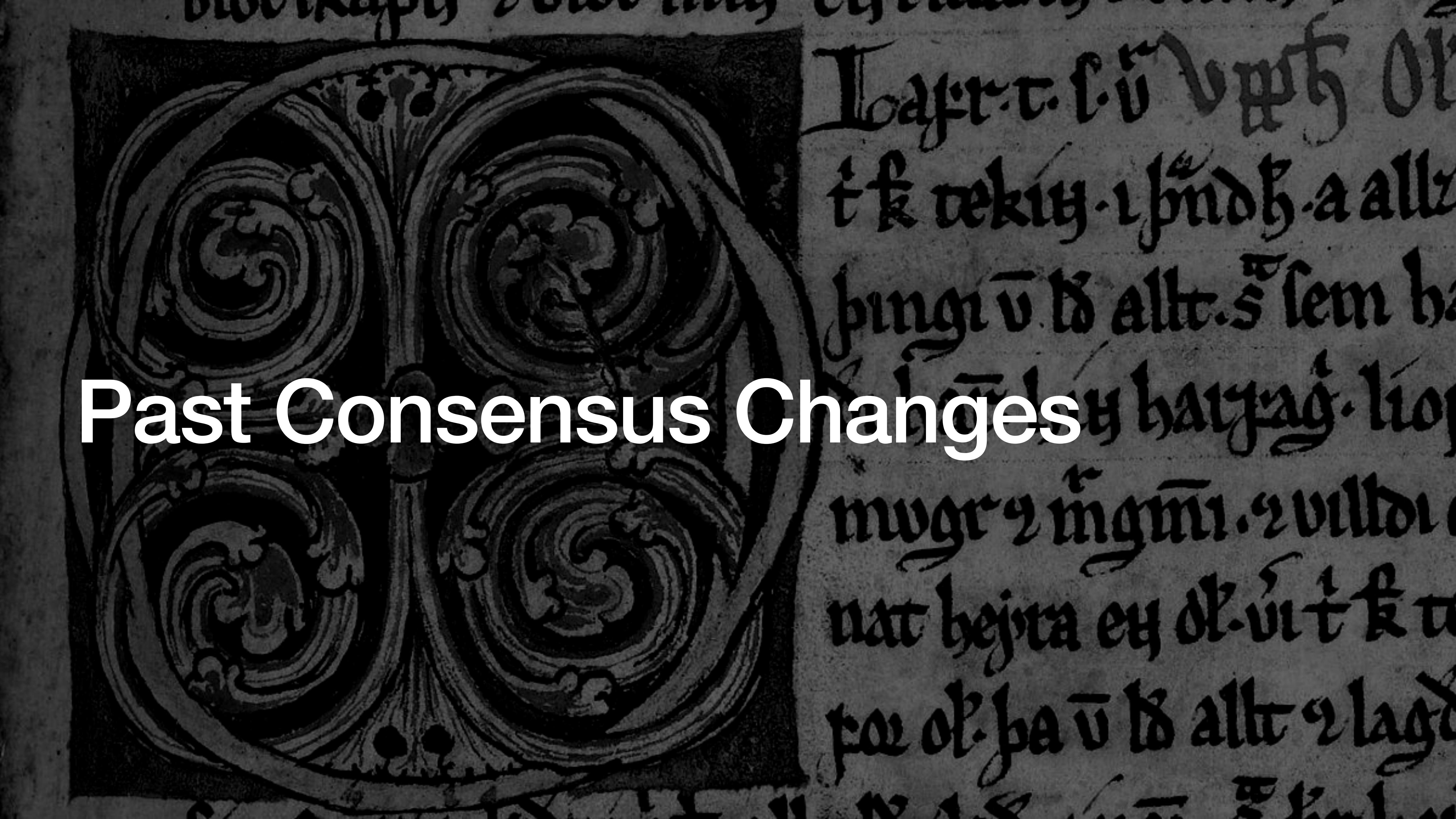
- Satoshi built a system that he didn't control
- Bitcoin does not exist through coercion or control
- Developers can't force users to use soft-fork features
- Soft-fork features **must** be incentive compatible



Incentive Compatibility

- What's good for the transactor is good for node operators
- Scarce block space and transaction fees provide incentive
- less data => better privacy and scalability





Past Consensus Changes

2012 : Pay to Script Hash (P2SH)

Allow arbitrary spending
conditions to be encoded
as an address

Reduce storage
requirements for full nodes



Hide spending conditions
(until spend)





BTC stored



2017 : Segregated Witness

Fixes txid malleability

Witness discount

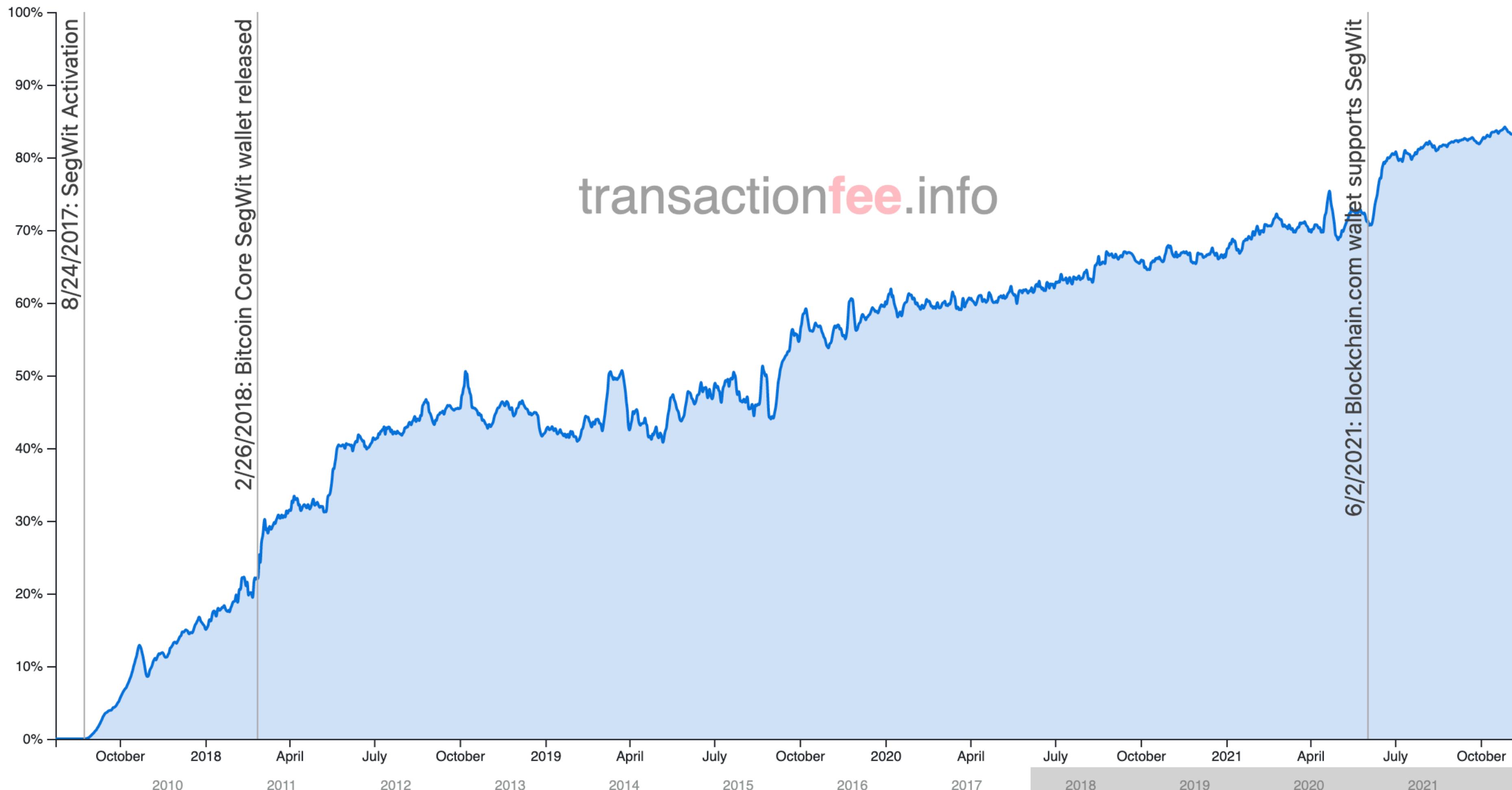


Allows chains of off-chain txs,
multi-owner UTXOs



SegWit spending Payments

Shows the percentage of payments spending SegWit per day.



2021 : Schnorr / Taproot

Multisignatures and
Threshold Signatures



Keypath spend is
one pubkey/one signature



Batch signature validation



Future Consensus Changes

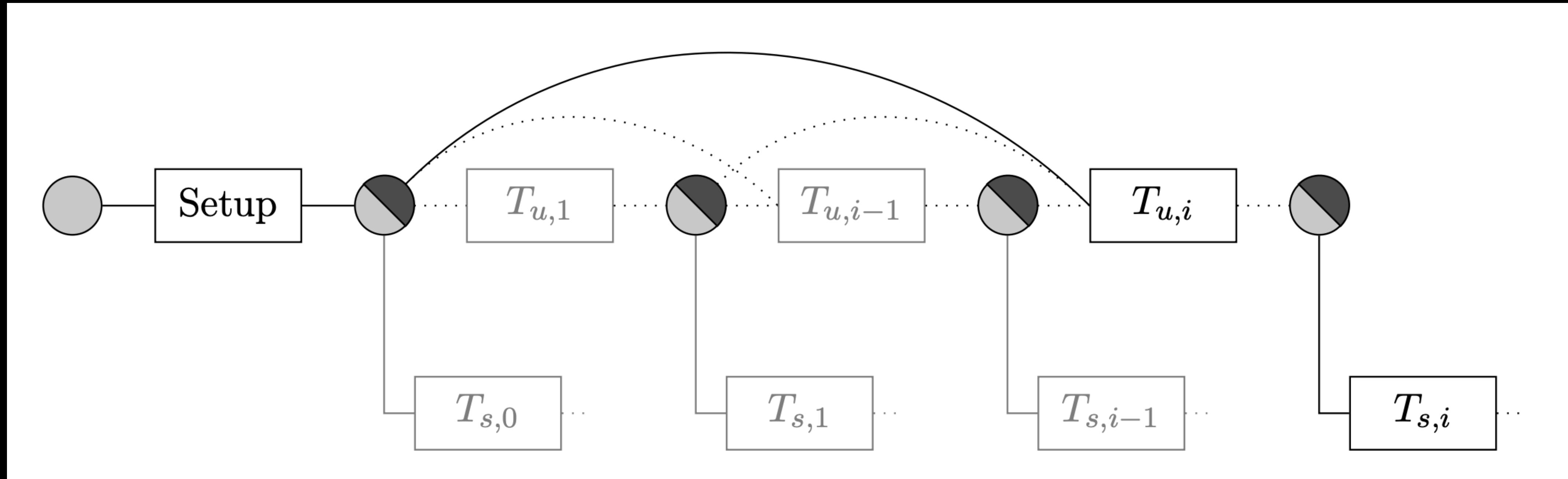


Signature Aggregation

TxIn 1 	TxOut 1
TxIn 2 	TxOut 2
TxIn 3 	TxOut 3

TxIn 1 	TxOut 1
TxIn 2 	TxOut 2
TxIn 3 	TxOut 3

SIGHASH_ANYPREVOUT



Delegation



graftroot

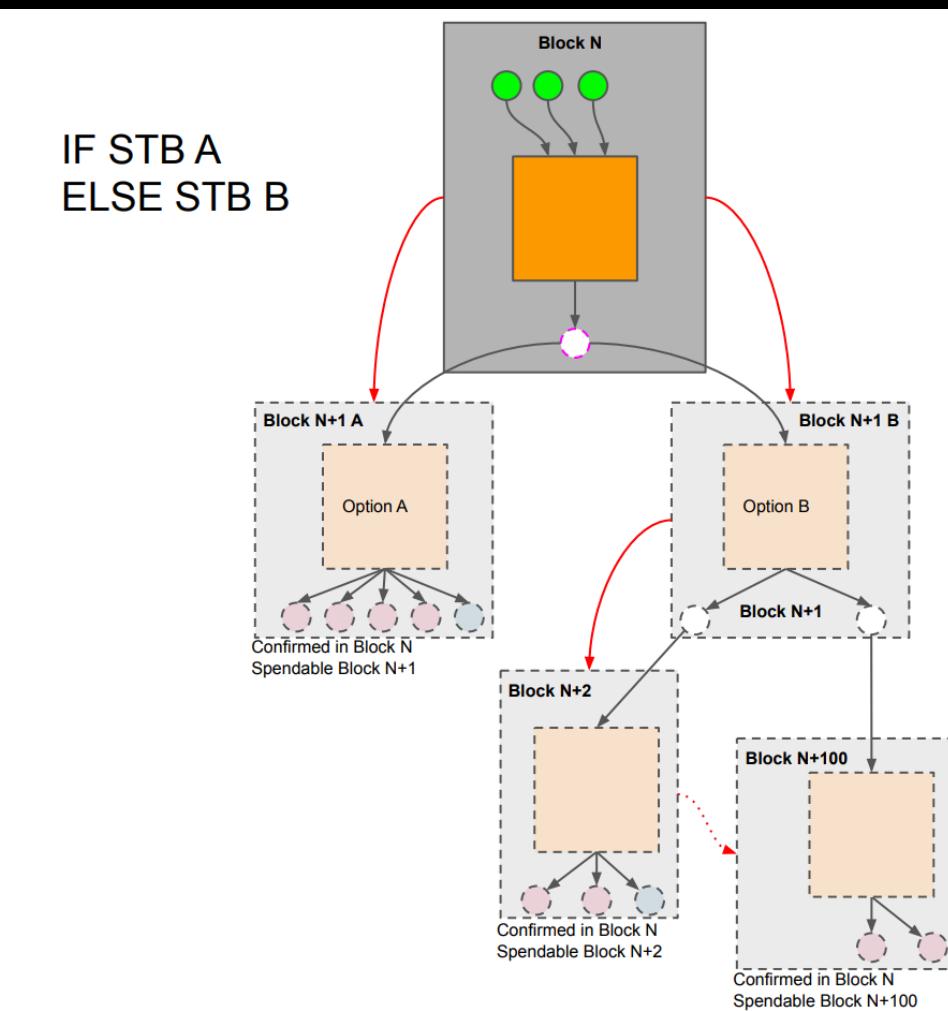
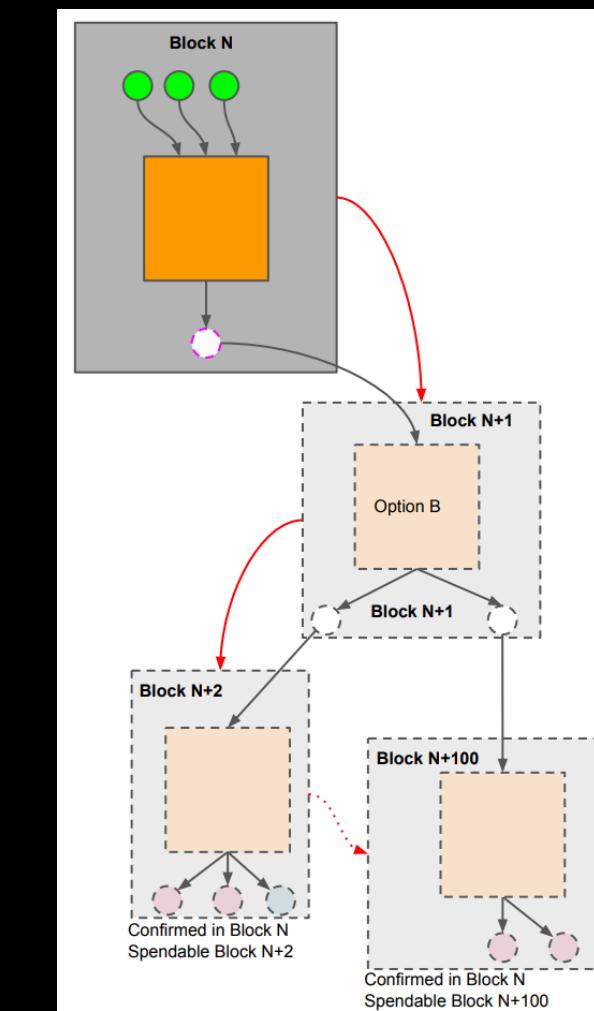
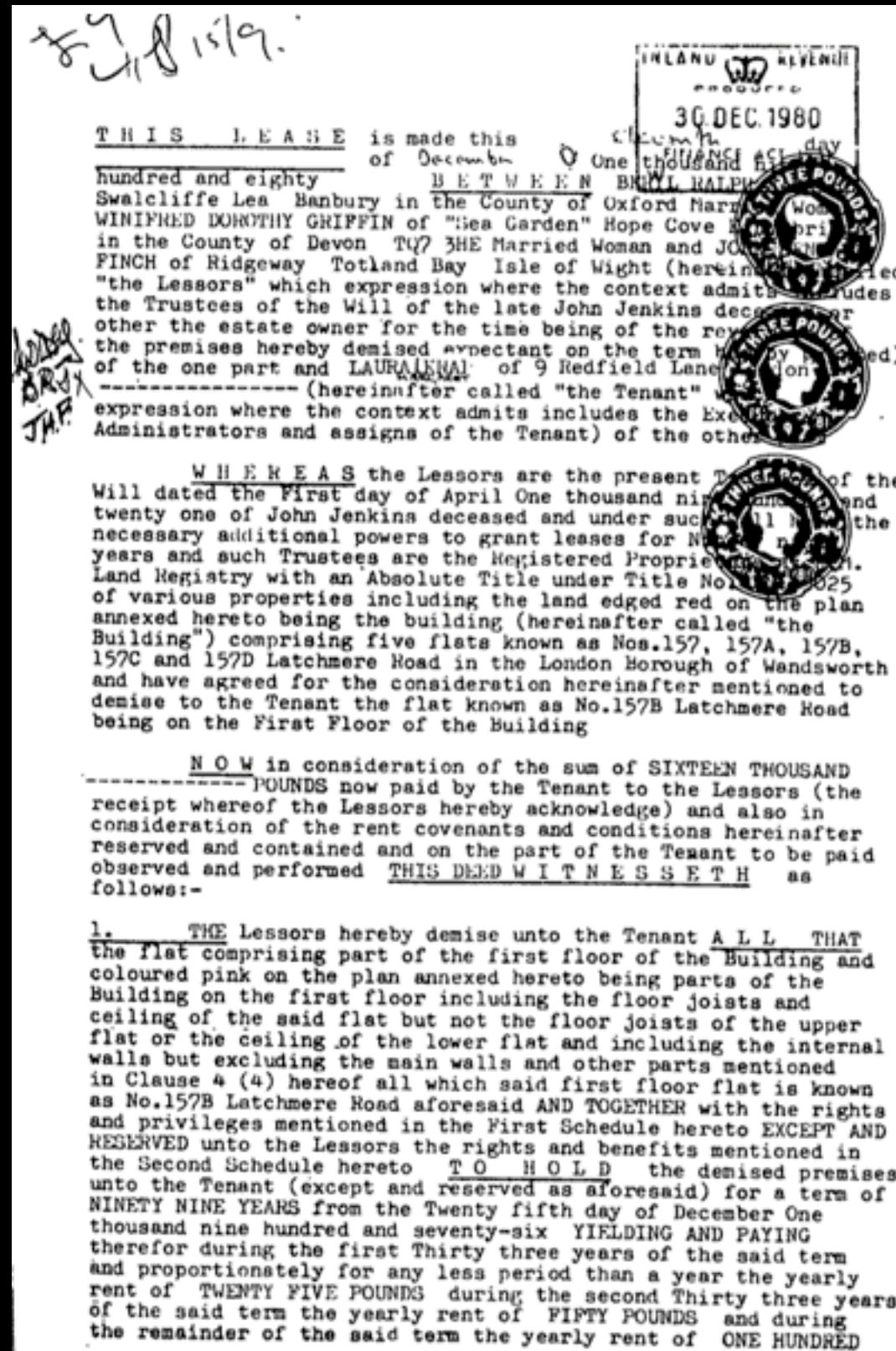


g'root



entroot

Covenants



In Conclusion





Protocol developers
provide tools



Tools must be
Incentive-compatible



Users benefit when
application developers
build products



Users must
demand better
products

Thank you!

John Newbery

brink

Learn More

- Future consensus changes: <https://bitcoinops.org/en/preparing-for-taproot/#future-consensus-changes>
- Cross-input signature aggregation: <https://github.com/ElementsProject/cross-input-aggregation>
- SIGHASH_ANYPREVOUT: https://bitcoinops.org/en/topics/sighash_anyprevout/
- eltoo: <https://blockstream.com/eltoo.pdf>
- Graftroot: <https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-February/015700.html>
- G'root: <https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-July/016249.html>
- Entroot: <https://gist.github.com/sipa/ca1502f8465d0d5032d9dd2465f32603>
- Covenants: <https://bitcoinops.org/en/topics/covenants/>
- OP_CTV: <https://github.com/bitcoin/bips/blob/master/bip-0119.mediawiki>
- TAPLEAF_UPDATE_VERIFY: <https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2021-September/019419.html>
- CoinPool: <https://thelab31.xyz/blog/coinpool>
- JoinPool: <https://gist.github.com/harding/a30864d0315a0cebd7de3732f5bd88f0>

Image credits

- p2 “Construction” <https://www.constructionexec.com/article/the-fundamentals-of-the-construction-industry-are-strong-but-lingering-workforce-concerns-need-industry-wide-action>
- p4 “decentralized” by Salvia Santos from the Noun Project
- p4 “Eye” by shwepes from the Noun Project
- p4 “Scale” by Adrien Coquet from the Noun Project
- p4 “Incentivize” by Matt Brooks from the Noun Project
- p5 “Incentives” <https://www.inc.com/bill-fotsch-and-john-case/why-your-incentive-plan-isnt-working.html>
- p7 “Incentives” <https://hrdailyadvisor.blr.com/2019/02/14/cons-of-team-based-incentives/>
- p10 <https://txstats.com/>
- p12 <https://transactionfee.info/>
- p16 <https://blockstream.com/eltoo.pdf>
- p18 grafting - <https://agriagrarian.blogspot.com/2020/09/grafting-a-sexual-vegetative-propagation.html>
- p18 groot - Marvel Studios
- p18 entroot - New Line Cinema
- p19 covenants - <https://utxos.org/uses/> by Jeremy Rubin
- p20 “insurance-policy-checklist-clipboard” - [https://www.mybarandrestaurant.com/insurance-policy-checkup-is-your-restaurant-covered/insurance-policy-checklist-clipboard/#prettyPhoto\[postimages\]/0](https://www.mybarandrestaurant.com/insurance-policy-checkup-is-your-restaurant-covered/insurance-policy-checklist-clipboard/#prettyPhoto[postimages]/0)