

Consensus Changes in Bitcoin

(in 20 minutes)

LABITCONF, San Salvador
Nov 19th, 2021

John Newbery

brink
RESEARCH

Building Bitcoin





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

Loaft. t. l. v. v. p. h. o. l.
t. k. tekny. i. p. n. d. h. a. allz
p. i. n. g. i. v. l. d. allt. s. l. e. m. h. a.
h. o. l. e. y. h. a. i. y. a. g. l. i. o. p.
m. w. g. r. 2. m. g. m. i. 2. v. i. l. l. d. i.
n. a. t. h. e. j. r. a. e. y. o. l. v. i. t. k. t.
p. o. e. o. l. p. a. v. l. d. allt. 2. l. a. g. d.
v. i. s. i. t. a. t. i. o. n. e. s.

2012 : Pay to Script Hash (P2SH)

Allow arbitrary spending conditions to be encoded as an address

Reduce storage requirements for full nodes

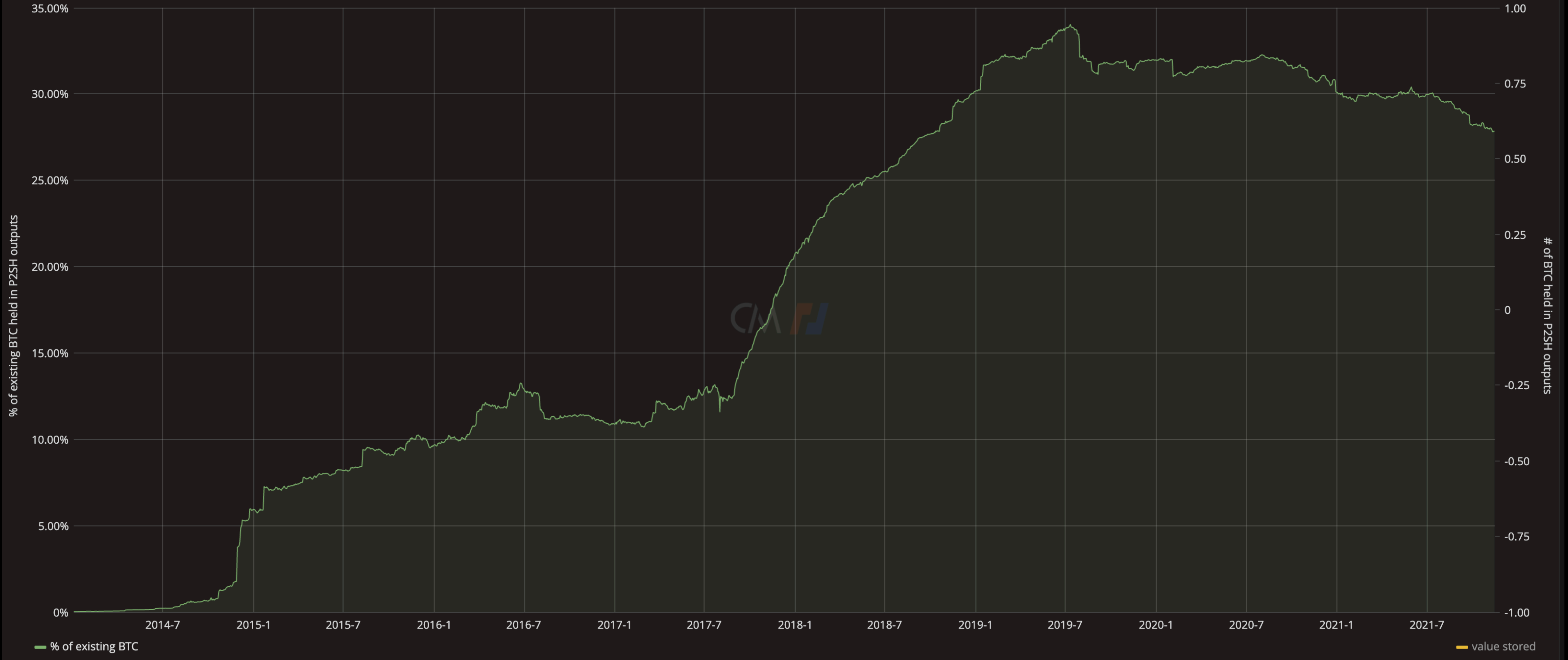


Hide spending conditions (until spend)





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

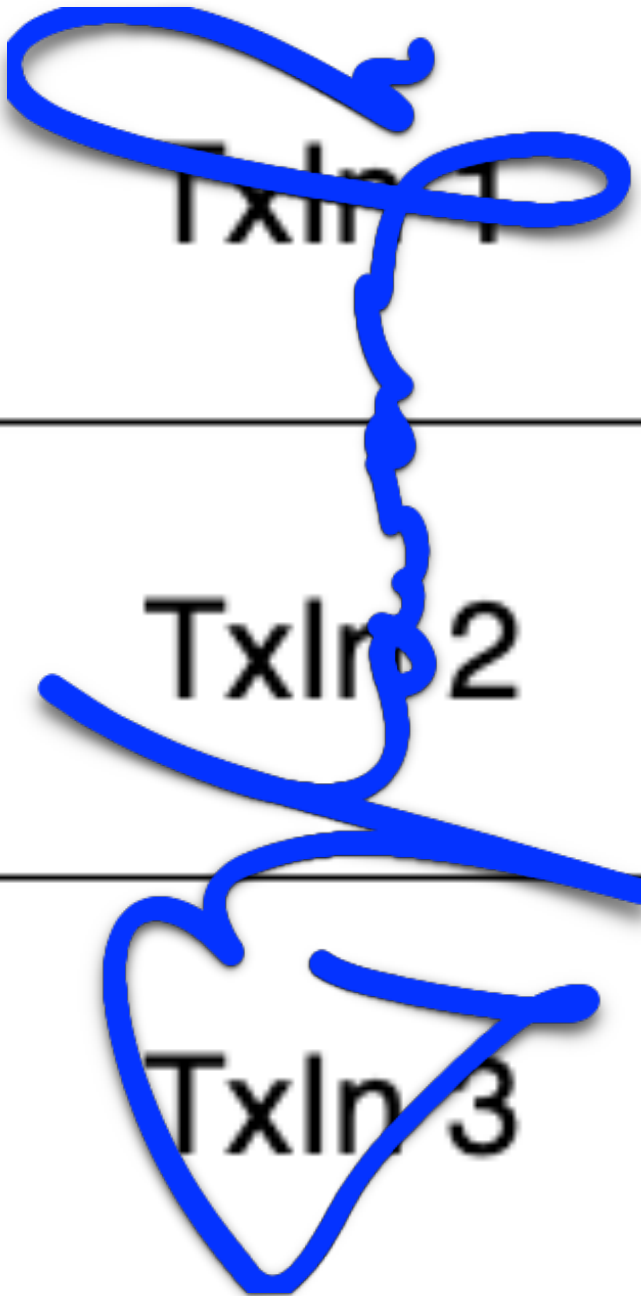


Future Consensus Changes

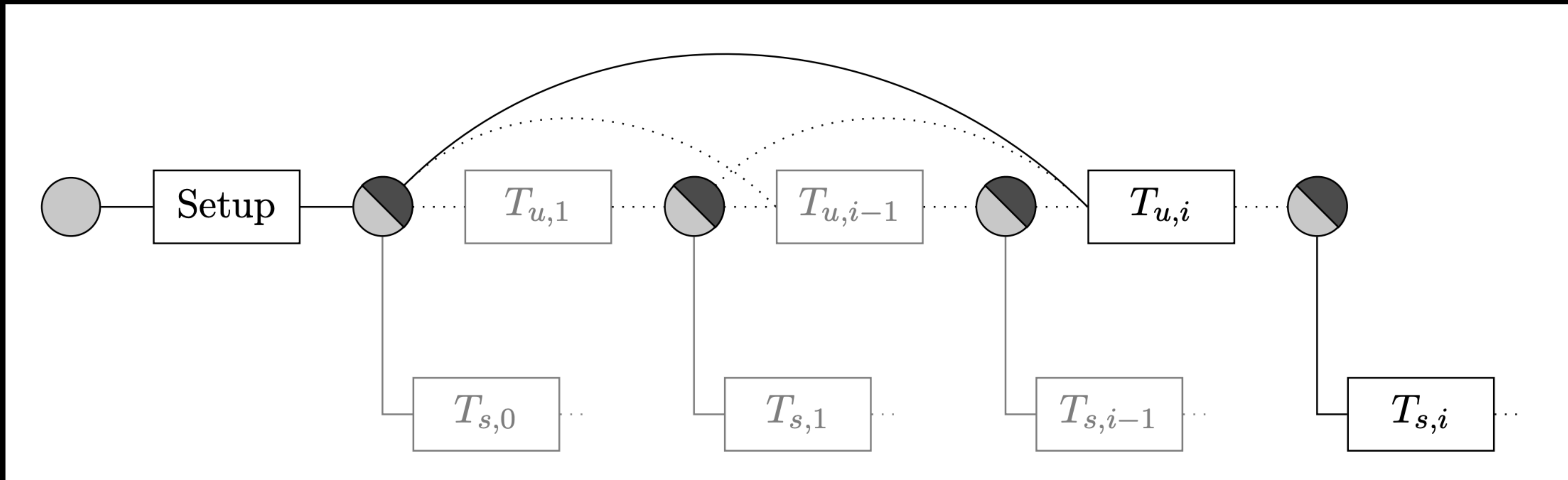


Signature Aggregation

 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

28/12/1980

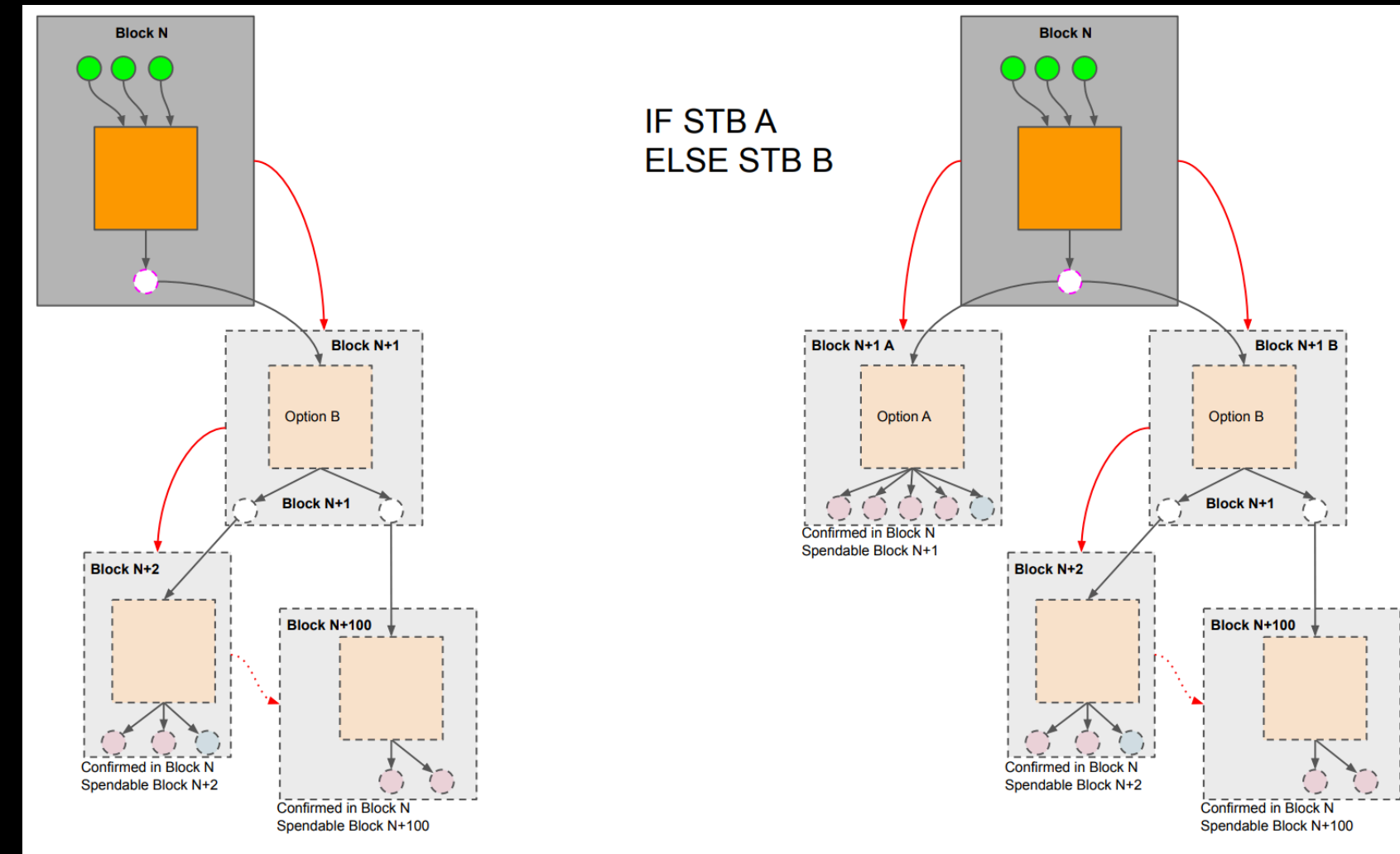
INLAND REVENUE
30 DEC 1980

THIS LEASE is made this 28th day of December One thousand nine hundred and eighty BETWEEN BRUCE WALEY SWALCLIFFE LEA BANBURY in the County of Oxford Mary WINIFRED DOROTHY GRIFFIN of "Sea Garden" Hope Cove in the County of Devon TQ7 3HE Married Woman and JOHN FINCH of Ridgeway Totland Bay Isle of Wight (hereinafter called "the Lessors" which expression where the context admits includes the Trustees of the Will of the late John Jenkins deceased and other the estate owner for the time being of the premises hereby demised expectant on the term mentioned) of the one part and LAURA LEWAL of 9 Redfield Lane (hereinafter called "the Tenant" which expression where the context admits includes the Executors Administrators and assigns of the Tenant) of the other part.

WHEREAS the Lessors are the present Trustees of the Will dated the First day of April One thousand nine hundred and twenty one of John Jenkins deceased and under such Will the necessary additional powers to grant leases for Ninety Nine years and such Trustees are the Registered Proprietors of the Land Registry with an Absolute Title under Title No. 1025 of various properties including the land edged red on the plan annexed hereto being the building (hereinafter called "the Building") comprising five flats known as Nos.157, 157A, 157B, 157C and 157D Latchmere Road in the London Borough of Wandsworth and have agreed for the consideration hereinafter mentioned to demise to the Tenant the flat known as No.157B Latchmere Road being on the First Floor of the Building

NOW in consideration of the sum of SIXTEEN THOUSAND POUNDS now paid by the Tenant to the Lessors (the receipt whereof the Lessors hereby acknowledge) and also in consideration of the rent covenants and conditions hereinafter reserved and contained and on the part of the Tenant to be paid observed and performed THIS DEED WITNESSETH as follows:-

1. THE Lessors hereby demise unto the Tenant ALL THAT the flat comprising part of the first floor of the Building and coloured pink on the plan annexed hereto being parts of the Building on the first floor including the floor joists and ceiling of the said flat but not the floor joists of the upper flat or the ceiling of the lower flat and including the internal walls but excluding the main walls and other parts mentioned in Clause 4 (4) hereof all which said first floor flat is known as No.157B Latchmere Road aforesaid AND TOGETHER with the rights and privileges mentioned in the First Schedule hereto EXCEPT AND RESERVED unto the Lessors the rights and benefits mentioned in the Second Schedule hereto TO HOLD the demised premises unto the Tenant (except and reserved as aforesaid) for a term of NINETY NINE YEARS from the Twenty fifth day of December One thousand nine hundred and seventy-six YIELDING AND PAYING therefor during the first Thirty three years of the said term and proportionately for any less period than a year the yearly rent of TWENTY FIVE POUNDS during the second Thirty three years of the said term the yearly rent of FIFTY POUNDS and during the remainder of the said term the yearly rent of ONE HUNDRED



A grayscale photograph of a hand holding a pen and writing on a document. The document is held by a stapler. The background is dark and out of focus. The text "In Conclusion" is overlaid on the left side of the image.

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
RESEARCH

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-asexualvegetative-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)