
LayerTwo Labs
Drivechains

Friends of Drivechain

Last Edited: 3/23/2023 | (Drivechain = BIP 300/301)

Bitcoiner	Statement	Source
Adam Back, Co-Founder and CEO of Blockstream	"**Drivechains...are pretty cool...and arguably could have been more important or useful than let's say Taproot.**" "**we're probably going to need sidechains / drivechains** where we're going, to onboard the next billion users. soon."	https://www.youtube.com/live/zp1B_i4JIXc?feature=share&t=7117 https://twitter.com/adam3us/status/1626563440054607872
Peter McCormack, Host of the What Bitcoin Did Podcast	"I like that fact that it just gives me one currency to go around and do all these other things, I like that a lot so that's cool."	https://www.whatbitcoindid.com/podcast/should-drivechains-come-to-bitcoin
Olaoluwa Osuntokun, CTO of Lightning Labs	"In the past year, the drivechain specs seem to have come a long way."	https://twitter.com/roasbeef/status/946036030590906368
Jameson Lopp, CTO & Co-founder of Casa	"...implementing Drivechains or Validity Rollups would not only improve overall network speed and capacity but would also **allow developers to test out various solutions in a way that keeps the underlying base layer safe**. This should massively speed up development time and thus fight against the looming ossification threat."	https://www.forbes.com/sites/digital-assets/2023/03/18/should-we-be-worried-about-bitcoin-ossification
Fiatjaf, Creator of Nostr	"Drivechain is our only hope." "We need Drivechain or all the work of thousands in the last 13 years will be in vain." Drivechain essay by Fiatjaf: https://fiatjaf.com/drivechain.html	https://twitter.com/fiatjaf/status/1380583953195749378 https://twitter.com/fiatjaf/status/1611138970850676739
Anton Kumaigorodski, Bitcoiner	"here's another project which I think is more critical than LN for bitcoin's long term survival"	https://t.me/lightningwallet/11374
Hampus Sjöberg, Creator of Blixt Lightning Wallet, Programmer, EDM producer, ₿itcoin fanatic	"We better work on actual real solutions (BIP300 drivechains) rather than nonsensical ones."	https://twitter.com/hampus_s/status/1620008878837751810
CalleBTC, Physicist, Programmer, Lightning dev	"I support BIP-300."	https://twitter.com/callebtc/status/1580157754660225024

Ruben Somsen, Bitcoin Sorcerer and Creator of Spacechains	"I would like to see Drivechains happen and run it as an experiment and see how it goes."	https://www.unhashedpodcast.com/episodes/2021/3/30/ep-129-l2-scaling-in-ethereum-and-bitcoin-w-eric-wall-amp-somsen
Aaron van Wirdum, Journalist at Bitcoin Magazine	"Surely you wouldn't prefer off-chain custodial accounts (eg. Coinbase) over sidechain balances (eg. Drivechain)?" "Custodial services can steal your bitcoin successfully 100% of the time. How can sidechains be worse than that?"	https://twitter.com/AaronvanW/status/1002919331758473217
Checkmate, Lead On-chain Analyst at Glassnode	"When will people start taking Drivechains seriously?"	https://twitter.com/_Checkmatey_/status/1344360650621947905
Super Testnet, Freelance Software Developer specializing in Bitcoin, Lightning, and Nostr	"There is already a fork of bitcoin with bip300 support. If 51% of bitcoiners run it then we have bip300. If anyone wants help setting it up, I'm happy to assist." "I'm not convinced it hurts anyone, but I am convinced **it brings us slightly better sidechains** than what we have today, and **helps miners make more in fees**." "Personally, I would not use drivechains if they existed [...] But I don't think that is a good reason to block the softfork. **You don't have to personally want to use something to support making it an option**."	https://twitter.com/super_testnet/status/1617205607617929217 https://twitter.com/super_testnet/status/1617226991710658562 https://twitter.com/super_testnet/status/1608967999532470272
Eric Wall, Investor and Software Engineer	"it's been 7 years since @Truthcoin wrote the original drivechain blog post. if you went back in time and told me that 7 years later no effort has been made towards merge-mined sidechains but that the same people who opposed them were upset ethereum existed i'd laugh in your face"	https://twitter.com/ercwl/status/1594449547689869319
Nic Carter, Founder and General Partner, Castle Island Ventures	"I agree with all of this"	https://twitter.com/nic__carter/status/1542176840726495232
Stewart Mackenzie, @sj_mackenzie, Host of the Stewart Mackenzie Indaba podcast	"The sooner BIP-300/1 happens the better."	https://twitter.com/sj_mackenzie/status/1580367565066358784

moonsettler @4moonsettler, stubborn self-sovereign money maximalist and aspiring cypherpunk	"it's entirely possible that drivechains could provide tremendous value with not a single current adopter using them, even once."	https://twitter.com/4moonsettler/status/1618307639817179136
Mario Gibney, Bitcoin promoter. Formerly at Ledn and Blockstream	"[If Drivechain is] ...incredibly useful... [it may] push toward greater total fees added to bitcoin."	https://twitter.com/Mario_Gibney/status/1457755740509245452
Andreas Brekken, Founder of SideShiftAI	"Activate BIP 300! This is how we get DeFi on Bitcoin." "**Monero should be a sidechain of Bitcoin using Drivechain**"	https://twitter.com/abrkn/status/1397456620439834628 https://twitter.com/abrkn/status/1403649701887365120
Mike In Space	"You mfers want ATH? Get BIP300 activated. You're welcome." "**I don't think we would see so much economic activity on other chains if we had Drivechain already**."	https://twitter.com/mikeinspace/status/1407549854646214656 https://twitter.com/mikeinspace/status/1475679698004975620
Michael Tidwell, Co-Founder of TABConf, Founder of The Atlanta BidDevs, and VP of Infrastructure at ZEBEDEE	"a sad unlikely future would be bip300 is done as a last ditch effort to take $ share% away from alts. i hope if/when bip300,.. it's done out of the love for btc innovation..."	https://twitter.com/miketwenty1/status/1466434096461197318
Kalle Alm, Bitcoin Core Contributor	"My understanding is there's some controversy/contention about drivechains, but the idea seems pretty cool, yep."	https://twitter.com/kallewoof/status/1404675811869806593
Vlad Costea, Host of the Bitcoin Takeover Podcast	"Drivechains are the purest form of Bitcoin maximalism. Anything else is conservatism in comparison."	https://twitter.com/thevladcostea/status/1615009368071720962
Torkel Rogstad, Co-Founder of Bare Bitcoin and Software Developer at Arcane Crypto	"We desperately need to take a long and hard look in the mirror, and start doing things differently. I think starting a more serious and thorough discussion about BIP300 (Drivechain) is the right place to start."	https://twitter.com/torkelrogstad/status/1512501111659409409

Sergio Demian Lerner, Chief of Innovation at IOV Labs and Designer of the RSK Rootstock Bitcoin sidechain	"[...] **migrate Rootstock to a drivechain when it is softforked into Bitcoin** [...] the destiny is to become fully decentralized." "[...] **sidechains are the natural extension of the Bitcoin finance stack** [...]. A sidechain is a blockchain that is highly incentive-aligned with the Bitcoin community."	https://twitter.com/SDLerner/status/1617188603267792897 https://medium.com/iovlabs-innovation-stories/bitcoin-sidechains-74a72ceba35d
Pete Rizzo, Editor of Bitcoin Magazine and Editor At Large of Kraken Digital Asset Exchange	"...I think anybody in the developer community will tell you, even if they don't want to do Drivechains, that they respect Paul Sztorc, because Paul Sztorc is trying to further Bitcoin as a technology."	https://www.whatbitcoindid.com/podcast/the-role-of-bitcoin-maximalism-part-2
Edan Yago, Cheerleader-In-Chief of Sovryn	"**The only thing missing from Bitcoin is that ability to adopt any feature or technology without changing main chain. BIP 300 fixes this**."	https://twitter.com/EdanYago/status/1402036078614306822?s=20&t=53YUb4h0GEpe01UpfeVa6Q
Guy Swann, Host of the Bitcoin Audible Podcast	"I feel like **sidechains are an inevitable part of the ecosystem** for multiple reasons, & I simply see BIP300 as a hashrate based sidechain rather than a federated multisig. I 100% agree on the alts issue, but that's not why i am interested in it."	https://twitter.com/TheGuySwann/status/1457557455127425030
John Light, Product at Sovryn and Bitcoin researcher	"I would like to see both validity rollups and drivechains offered as options for people on Bitcoin layer one. [...] I think **it would make sense to do drivechains first rather than wait until validity rollups are ready**. [...] What I call the "miners will steal hypothesis" has so far been proven to be false on blockchains that implement basically the same security model [as Drivechain]".	https://twitter.com/i/spaces/1LyGBqDkkYEKN?s=20
Giacomo Zucco, CEO of ZuckBucks, Bitcoiner, Entrepreneur, Consultant and Educator	"**I like drivehain but I'm skeptical they will ever have consensus**" "I'm not very convinced abour drivechains, I do like hashrate escrows, but I like status quo as default in case of any change less than obviously necessary." "Drivechains give lots of censoring power to miners. I'd prefer a coinwitness kind of 2WP. **But yes: a monero-like sidechain would be way better than Monero as a separate shitcoin, also for swaps (no slippage, less liquidity bottleneck)**."	https://t.me/lightningwallet/234397 https://twitter.com/giacomozucco/status/1612223050665328641 https://twitter.com/giacomozucco/status/1507377144237805572
Alexei Zamyatin, Founder @interlayHQ	"...make BTC interoperability easier (BIP300 or similar)..."	https://twitter.com/alexeiZamyatin/status/1594136409711218689

Andrew Bailey, Associate Professor of Humanities/Philosophy, Yale-NUS College	"A year later, I'm starting to have views. They're pretty pro-BIP300, I confess!"	https://twitter.com/resistancemoney/status/1614111587601874946
Troy Cross, Professor of Philosophy and Humanities at Reed College	"[...] long-term we need either a better fee market, something like drivechains, or else… mining at a loss by large stakeholders." "I agree." (In response to: "Building on bitcoin will increase in an exciting way once drivechain is adopted. #Hivemind")	https://twitter.com/thetrocro/status/1504493801003360258 https://twitter.com/thetrocro/status/1618112234533842944
Brad Mills, Investor, Entreprenuer, and Host of the Magic Internet Money Podcast	"I think it's time the Bitcoin community took a more serious look at @Truthcoin's drivechain proposal."	https://twitter.com/bradmillscan/status/1401981128328855555
Ari Paul, Founder and Chief Investment Officer of BlockTower Capital	"...Drivechains are at least 4 years old. The LN whitepaper was 2016. If there had been aggressive innovation (from the user functionality perspective) on this stuff, I'd agree it would have taken the wind out of many altcoin sails, but there wasn't so it didn't."	https://twitter.com/AriDavidPaul/status/1404803437313789965
J0E007, Cryptocurrency trader	"As a self-professed Bitcoin maximalist, I support #BIP300. **Enabling permissionless innovation on top of a stable and conservative Bitcoin base layer (rather than pushing them into shitcoinosphere) is a very important goalz**. That's how modern versatile Internet came into being."	https://twitter.com/J0E007/status/1408788553560117256
Paul Puey, Co-Founder at EdgeWallet	"I'm a fan."	https://twitter.com/paullinator/status/1620100865460957185
Sjors Provoost, Bitcoin Core contributor	"What I find most appealing about the Drivechain idea is the separation of funding second layer and using second layer. With Lighning everyone needs to open their own channels which is expensive, whereas Drivechain would allow economies of scale for those transfers. If it works."	https://twitter.com/provoost/status/946327279633911808
Sovryn Matt @SovrynM, Contributor to Sovryn	"BIP-300 fixes this. Rather than polluting the btc blockchain with NFTs, you give the NFT enthusiasts a bitcoin sidechain to do their NFT scamming. Smart bitcoin miners will secure and mine the NFT sidechain for additional revenue from fees generated."	https://twitter.com/SovrynM/status/1620271176303128576
Greg Slepak, Founder at Tao Effect LLC and President at okTurtles Foundation Inc.	"ACK'ing potential for safe operation of #Drivechain: [...]"	https://twitter.com/taoeffect/status/1620198161926193152

Isaac Fain, President at Krew Labs	"why its great: #Drivechain provides a canonical, easy to reuse pattern for launching sidechains with consistent security properties. This stimulates innovation and limit risk with experimental bridge / federated models."	https://twitter.com/isaacfain/status/1617229767777853445
Joel Kaartinen @jkaartinen, Lead Systems Architect @PrasosLtd	"I don't really see an argument against drivechain here. If 51% of miners are colluding hard enough and "willing to steal", Bitcoin is in deep trouble, drivechains or not."	https://twitter.com/jkaartinen/status/1412123740796821504
Alex Kravets, Founder and CEO at Satoshium	"I would personally love to see Drivechain soft fork adopted."	https://twitter.com/alexkravets/status/1000079544118738944
Timoleon Moraitis, Senior Researcher and Group Leader at Huawei (Machine Learning, Neuromorphic Computing, and Computational Neuroscience)	"Any sidechain replacing an altcoin increases BTC's security by 1. eliminating competitors with potential attack interests, 2. increasing the value of the token in which btc miners are paid. On top, 3. Drivechain brings more fees to btc miners, not changing mainchain fees or size."	https://twitter.com/timos_m/status/1190425914166906886
Post Capone @p0stc4p0n3, Ordinals Enthusiast/Influencer	"*If* BIP300/301 *could* fox it then there is *at least* one fix that doesn't require a modification of the supply cap."	https://twitter.com/p0stc4p0n3/status/1619605474390982658
Eric O'Reilly, liberty & #bitcoin	"Some thoughts on the Drivechain 1/ The premise is valid. #Bitcoin base layer is difficult to change, which is probably a good thing. At the same time, some use cases for blockchain beyond Bitcoin Script have emerged. 2/ Drivechain allows for faster iteration on second layers, while encouraging the use of BTC as the monetary unit on those layers. [...]"	https://twitter.com/ericohreilly/status/1568105801755279361
Vake @vakeraj	"drivechains —> prediction markets —> futarchy —> omniscience —> transcend death" "I really don't think @Truthcoin is malicious. Like the rest of us, he's seeing the growth of altcoins, and wishes that would take place within the Bitcoin ecosystem. Hence his passion for sidechains/drivechains."	https://twitter.com/vakeraj/status/1316430745926332422 https://twitter.com/vakeraj/status/959083699919884288
Gabriel Kurman, Co-founder of the Bitcoin Rootstock sidechain	"Absolutely we count on the Bitcoin Core Devs to implement the Drivechain softfork as soon as possible to make Sidechains 2.0 a reality!"	https://twitter.com/GabrielKurman/status/1121945970177191937

```
BIP: 300
Layer: Consensus (soft fork)
Title: Hashrate Escrows (Consensus layer)
Author: Paul Sztorc <truthcoin@gmail.com>
        CryptAxe <cryptaxe@gmail.com>
Comments-Summary: No comments yet.
Comments-URI: https://github.com/bitcoin/bips/wiki/Comments:BIP-0300
Status: Draft
Type: Standards Track
Created: 2017-08-14
License: BSD-2-Clause
Post-History: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-May/014364.html
```

Table of Contents

Abstract

In Bip300, txns are not signed via cryptographic key. Instead, they are "signed" by hashpower, over time. Like a big multisig, 13150-of-26300, where each block is a new "signature".

Bip300 emphasizes slow, transparent, auditable transactions which are easy for honest users to get right and very hard for dishonest users to abuse. The chief design goal for Bip300 is *partitioning* -- users may safely ignore Bip300 txns if they want to (or Bip300 entirely).

See this site for more information.

Motivation

As Reid Hoffman wrote in 2014: "Sidechains allow developers to add features and functionality to the Bitcoin universe without actually modifying the Bitcoin Core code...Consequently, innovation can occur faster, in more flexible and distributed ways, without losing the synergies of a common platform with a single currency."

Today, coins such as Namecoin, Monero, ZCash, and Sia, offer features that Bitcoiners cannot access -- not without selling their BTC to invest in a rival monetary unit. According to coinmarketcap.com, there is now more value *outside* the BTC protocol than within it. According to cryptofees.info, 15x more txn fees are paid outside the BTC protocol, than within it.

Software improvements to Bitcoin rely on developer consensus -- BTC will pass on a good idea if it is even slightly controversial. Development is slow: we are now averaging one major feature every 5 years.

Sidechains allow for competitive "benevolent dictators" to create a new sidechain at any time. These dictators are accountable only to their users, and (crucially) they are protected from rival dictators. Users can move their BTC among these different pieces of software, as *they* see fit.

BTC can copy every useful technology, as soon as it is invented; scamcoins lose their justification and become obsolete; and the community can be pro-creativity, knowing that Layer1 is protected from harmful changes.

Specification

Overview

Bip300 allows for six new blockchain messages (these have consensus significance):

- M1. "Propose New Sidechain"
- M2. "ACK Proposal"
- M3. "Propose Bundle"
- M4. "ACK Bundle"
- M5. Deposit -- a transfer of BTC from-main-to-side
- M6. Withdrawal -- a transfer of BTC from-side-to-main

Nodes organize those messages into two caches:

- D1. "The Sidechain List", which tracks the 256 Hashrate Escrows (Escrows are slots that a sidechain can live in).
- D2. "The Withdrawal List", which tracks the withdrawal-Bundles (coins leaving a Sidechain).

D1 (The Sidechain List)

D1 is a list of active sidechains. D1 is updated via M1 and M2.

Field No.	Label	Type	Description / Purpose
1	Escrow Number	uint8_t	The escrow's ID number. Used to uniquely refer to each sidechain.
2	Version	int32_t	Version number.
3	String KeyID	string	Used to derive all sidechain deposit addresses.
4	Sidechain Private Key	string	The private key of the sidechain deposit script.
5	ScriptPubKey	CScript	Where the sidechain coins go. This always stays the same, even though the CTIP (UTXO) containing the coins is always changing.
6	Sidechain Name	string	A human-readable name of the sidechain.
7	Sidechain Description	string	A human-readable name description of the sidechain.
8	Hash1 - tarball hash	uint256	Intended as the sha256 hash of the tar.gz of the canonical sidechain software. (This is not enforced anywhere by Bip300, and is for human purposes only.)

9	Hash2 - git commit hash	uint160	Intended as the git commit hash of the canonical sidechain node software. (This is not enforced anywhere by Bip300, and is for human purposes only.)
10	Active	bool	Does this sidechain slot contain an active sidechain?
11	"CTIP" -- Part 1 "TxID"	uint256	The CTIP, or "Critical (TxID, Index) Pair" is a variable for keeping track of where the sidechain's money is (ie, which member of the UTXO set).
12	"CTIP" -- Part 2 "Index"	int32_t	Of the CTIP, the second element of the pair: the Index. See #11 above.

D2 (The Withdrawal List)

D2 lists withdrawal-attempts. If these attempts succeed, they will pay coins "from" a Bip300-locked UTXO, to new UTXOs controlled by the withdrawing-user. Each attempt pays out many users, so we call these withdrawal-attempts "Bundles".

D2 is driven by M3, M4, M5, and M6. Those messages enforce the following principles:

1. The Bundles have a canonical order (first come first serve).
2. From one block to the next, every "Blocks Remaining" field decreases by 1.
3. When "Blocks Remaining" reaches zero the Bundle is removed.
4. From one block to the next, the value in "ACKs" may either increase or decrease, by a maximum of 1 (see M4).
5. If a Bundle's "ACKs" reach 13150 or greater, it "succeeds" and its corresponding M6 message can be included in a block.
6. If the M6 of a Bundle is paid out, it is also removed.
7. If a Bundle cannot possibly succeed (13500 - "ACKs" > "Blocks Remaining"), it is removed immediately.

Field No.	Label	Type	Description / Purpose
1	Sidechain Number	uint8_t	Links the withdrawal-request to a specific hashrate escrow.
2	Bundle Hash	uint256	A withdrawal attempt. Specifically, it is a "blinded transaction id" (ie, the double-Sha256 of a txn that has had two fields zeroed out, see M6) of a txn which could withdraw funds from a sidechain.

3	ACKs (Work Score)	uint16_t	The current ACK-counter, which is the total number of ACKs (the PoW that has been used to validate the Bundle).
4	Blocks Remaining (Age)	uint16_t	The number of blocks which this Bundle has remaining to accumulate ACKs

The Six New Bip300 Messages

First, how are new sidechains created?

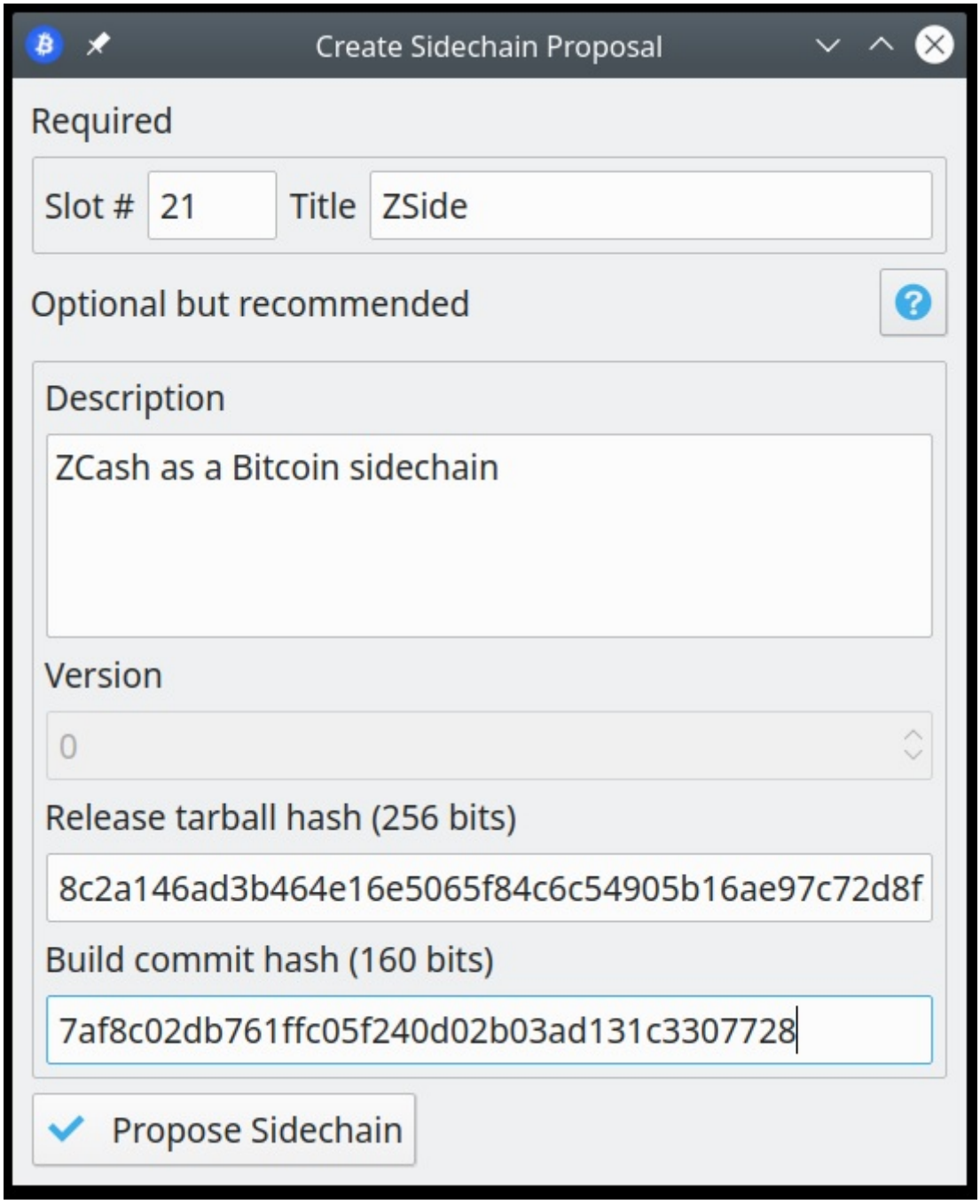
They are first proposed (with M1), and later acked (with M2). This process resembles Bip9 soft fork activation.

M1 -- Propose Sidechain

M1 is a coinbase OP Return output containing the following:

```
1-byte - OP_RETURN (0x6a)
4-byte - Message header (0xD5E0C4AF)
N-byte - The serialization of the sidechain.
  1-byte nSidechain
  4-byte nVersion
  x-byte strKeyID
  x-byte strPrivKey
  x-byte scriptPubKey
  x-byte title
  x-byte description
  32-byte hashID1
  20-byte hashID2
```

Examples


Create Sidechain Proposal
Required
Slot # 21
Title ZSide
Optional but recommended
Description
ZCash as a Bitcoin sidechain
Version
0
Release tarball hash (256 bits)
8c2a146ad3b464e16e5065f84c6c54905b16ae97c72d8f
Build commit hash (160 bits)
7af8c02db761ffc05f240d02b03ad131c3307728
Propose Sidechain

```
cryptaxe@hal:~/Drivechain$ ./src/drivechain-cli help createsidechainproposal
createsidechainproposal
Generates a sidechain proposal to be included in the next block mined by this node.
Note that this will not broadcast the proposal to other nodes. You must mine a block which includes your proposal to complete the process.
Pending proposals created by this node will automatically be included in the soonest block mined possible.

Arguments:
1. "nsidechain"   (numeric, required) sidechain slot number
2. "title"        (string, required) sidechain title
3. "description"  (string, optional) sidechain description
4. "version"      (numeric, optional) sidechain / proposal version
5. "hashid1"      (string, optional) 256 bits used to identify sidechain
6. "hashid2"      (string, optional) 160 bits used to identify sidechain

Examples:
> drivechain-cli createsidechainproposal 1 "Namecoin" "Namecoin as a Bitcoin sidechain" 0 78b140259d5626e17c4bf339c23cb4fa8d16d138f71d9803ec394bb01c051f0b 90869d013
db27608c7428251c6755e5a1d9e9313

> curl --user myusername --data-binary '{"jsonrpc": "1.0", "id":"curltest", "method": "createsidechainproposal", "params": [1 "Namecoin" "Namecoin as a Bitcoin side
chain" 0 78b140259d5626e17c4bf339c23cb4fa8d16d138f71d9803ec394bb01c051f0b 90869d013db27608c7428251c6755e5a1d9e9313] }' -H 'content-type: text/plain;' http://127.0.0
.1:8332/

cryptaxe@hal:~/Drivechain$ ./src/drivechain-cli createsidechainproposal 1 "Namecoin" "Namecoin as a Bitcoin sidechain" 0 78b140259d5626e17c4bf339c23cb4fa8d16d138f71
d9803ec394bb01c051f0b 90869d013db27608c7428251c6755e5a1d9e9313
{
  "nSidechain": 1,
  "title": "Namecoin",
  "description": "Namecoin as a Bitcoin sidechain",
  "privatekey": "5JPjosnCe69m5S6JFahcc6AQsDEoRadjE4LZj4dmGkv2EfPFKma",
  "keyid": "c6fbd9b51c3883fb3d5f41a3d930fadca7ca3483",
  "version": 0,
  "hashID1": "78b140259d5626e17c4bf339c23cb4fa8d16d138f71d9803ec394bb01c051f0b",
  "hashID2": "90869d013db27608c7428251c6755e5a1d9e9313"
}
```

M2 -- ACK Sidechain Proposal

M2 is a coinbase OP Return output containing the following:

```
1-byte - OP_RETURN (0x6a)
4-byte - Message header (0xD6E1C5BF)
32-byte - sha256D hash of sidechain's serialization
```

Notes

The new M1/M2 validation rules are:

1. Any miner can propose a new sidechain (M1) at any time. This procedure resembles BIP 9 soft fork activation: the network must see a properly-formatted M1, followed by "acknowledgment" of the sidechain (M2) in 90% of the following 2016 blocks.
2. Bip300 comes with only 256 sidechain-slots. If all are used, it is possible to "overwrite" a sidechain. This requires vastly more M2 ACKs -- 50% of the following 26300 blocks must contain an M2. The possibility of overwrite, does not change the Bip300 security assumptions (because we already assume that the sidechain is vulnerable to miners, at a rate of 1 catastrophe per 13150 blocks).

Notes on Withdrawing Coins

Bip300 withdrawals ("M6") are very significant.

For an M6 to be valid, it must be first "prepped" by one M3 and then 13,150+ M4s. M3 and M4 are about "Bundles".

What are Bundles?

Sidechain withdrawals take the form of “Bundles” -- named because they "bundle up" many individual withdrawal-requests into a single rare layer1 transaction.

Sidechain full nodes aggregate the withdrawal-requests into a big set. The sidechain calculates what M6 would have to look like, to pay all of these withdrawal-requests out. Finally, the sidechain calculates what the hash of this M6 would be. This 32-byte hash identifies the Bundle.

This 32-byte hash is what miners will be slowly ACKing over 3-6 months, not the M6 itself (nor any sidechain data, of course).

A bundle either pays all its withdrawals out (via M6), or else it fails (and pays nothing out).

Bundle Hash = Blinded TxID of M6

The Bundle hash is static as it is being ACKed. Unfortunately, the M6 TxID will be constantly changing -- as users deposit to the sidechain, the input to M6 will change.

To solve this problem, we do something conceptually similar to AnyPrevOut (BIP 118). We define a "blinded TxID" as a way of hashing a txn, in which some bytes are first overwritten with zeros. These are: the first input and the first output. Via the former, a sidechain can accept deposits, even if we are acking a TxID that spends from it later. Via the latter, we can force all of the non-withdrawn coins to be returned to the sidechain (even if we don't yet know how many coins this will be).

M3 -- Propose Bundle

M3 is a coinbase OP Return output containing the following:

```
1-byte - OP_RETURN (0x6a)
4-byte - Commitment header (0xD45AA943)
32-byte - The Bundle hash, to populate a new D2 entry
```

The new validation rules pertaining to M3 are:

1. If the network detects a properly-formatted M3, it must add an entry to D2 in the very next block. The starting "Blocks Remaining" value is 26,299. The starting ACKs count is 1.
2. Each block can only contain one M3 per sidechain.

Once a Bundle is in D2, how can we give it enough ACKs to make it valid?

M4 -- ACK Bundle(s)

M4 is a coinbase OP Return output containing the following:

```
1-byte - OP_RETURN (0x6a)
4-byte - Commitment header (0xD77D1776)
1-byte - Version
n-byte - The vector describing the "upvoted" bundle-choice, for each sidechain.
```

Version 0x01 uses one byte per sidechain, and applies in most cases. Version 0x02 uses two bytes per sidechain and applies in unusual situations where at least one sidechain has more than 256 distinct withdrawal-bundles in progress at one time. Other interesting versions are possible: 0x03 might say "do exactly what was done in the previous block" (which could consume a fixed 6 bytes total, regardless of how many sidechains). 0x04 might say "upvote everyone who is clearly in the lead" (which also would require a mere 6 bytes), and so forth.

If a sidechain has no pending bundles, then it is skipped over when M4 is created and parsed.

The upvote vector will code "abstain" as 0xFF (or 0xFFFF); it will code "alarm" as 0xFE (or 0xFFFE). Otherwise it simply indicates which withdrawal-bundle in the list, is the one to be "upvoted". For example, if there are two sidechains, and we wish to upvote the 7th bundle on sidechain #1 plus the 4th bundle on sidechain #2, then the vector would be 0x0704.

The M4 message will be invalid (and invalidate the block), if it tries to upvote a Bundle that doesn't exist (for example, trying to upvote the 7th bundle on sidechain #2, when sidechain #2 has only three bundles). If there are no Bundles at all (no one is trying to withdraw from any sidechain), then *any* M4 message present in the coinbase will be invalid. If M4 is NOT present in a block, then it is treated as "abstain".

The ACKed withdrawal will gain one point for its ACK field. Therefore, the ACK-counter of any Bundle can only change by (-1,0,+1).

Within a sidechain-group, upvoting one Bundle ("+1") requires you to downvote all other Bundles in that group. However, the minimum ACK-counter is zero. While only one Bundle can be upvoted at once; the whole group can all be unchanged at once ("abstain"), and they can all be downvoted at once ("alarm").

Finally, we describe Deposits and Withdrawals.

M5 -- Deposit BTC to Sidechain

Both M5 and M6 are regular Bitcoin txns. They are distinguished from regular txns (non-M5 non-M6 txns), when they select one of the special Bip300 CTIP UTXOs as one of their inputs (see D1).

All of a sidechain’s coins, are stored in one UTXO, called the "CTIP". Every time a deposit or withdrawal is made, the CTIP changes. Each deposit/withdrawal will select the sidechains CTIP, and generate a new CTIP. (Deposits/Withdrawals never cause UTXO bloat.) The current CTIP is cached in D1 (above).

If the **quantity of coins**, in the from-CTIP-to-CTIP transaction, goes **up**, (ie, if the user is adding coins), then the txn is treated as a Deposit (M5). Else it is treated as a Withdrawal (M6). See here.

As far as mainchain consensus is concerned, all deposits to a sidechain are always valid.

M6 -- Withdraw BTC from a Sidechain

We come, finally, to the critical matter: where users can take their money *out* of the sidechain.

First, M6 must obey the same CTIP rules of M5 (see immediately above).

Second, an M6 is only valid for inclusion in a block, if its blinded TxID matches an "approved" Bundle hash (ie, one with an ACK score of 13150+). In other words, an M6 can only be included in a block, after the 3+ month (13150 block) ceremony.

Third, M6 must meet two accounting criteria, lest it be invalid:

1. "Give change back to Escrow" -- The first output, TxOut0, must be paid back to the sidechain's Bip300 script. In other words, all non-withdrawn coins must be paid back into the sidechain.
2. "No traditional txn fee" -- For this txn, the sum of all inputs must equal the sum of all outputs. No traditional tx fee is possible. (Of course, there is still a txn fee for miners: it is paid via an OP TRUE output in the Bundle.) We want the withdraw-ers to set the fee "inside" the Bundle, and ACK it over 3 months like everything else.

Backward compatibility

As a soft fork, older software will continue to operate without modification. Non-upgraded nodes will see a number of phenomena that they don't understand -- coinbase txns with non-txn data, value accumulating in anyone-can-spend UTXOs for months at a time, and then random amounts leaving these UTXOs in single, infrequent bursts. However, these phenomena don't affect them, or the validity of the money that they receive.

(As a nice bonus, note that the sidechains themselves inherit a resistance to hard forks. The only way to guarantee that all different sidechain-nodes will always report the same Bundle, is to upgrade sidechains via soft forks of themselves.)

Deployment

This BIP will be deployed via UASF-style block height activation. Block height TBD.

Reference Implementation

See: https://github.com/drivechain-project/mainchain

Also, for interest, see an example sidechain here: https://github.com/drivechain-project/sidechains/tree/testchain

References

https://github.com/drivechain-project/mainchain https://github.com/drivechain-project/sidechains/tree/testchain See http://www.drivechain.info/literature/index.html

Credits

Thanks to everyone who contributed to the discussion, especially: ZmnSCPxj, Adam Back, Peter Todd, Dan Anderson, Sergio Demian Lerner, Chris Stewart, Matt Corallo, Sjors Provoost, Tier Nolan, Erik Aronesty, Jason Dreyzehner, Joe Miyamoto, Ben Goldhaber.

Copyright

EthSide -- An Ethereum Drivechain

09 Oct 2022

VIDEO WALKTHROUGH on YouTube (https://youtu.be/PsaSGZ0yulQ).

In This Guide

We show how to use Eth's software stack, but with BTC. (Ie, without buying Ether). This requires Bip300, but we can still demonstrate via DriveNet (a version of Bitcoin Core with Bip300 activated).

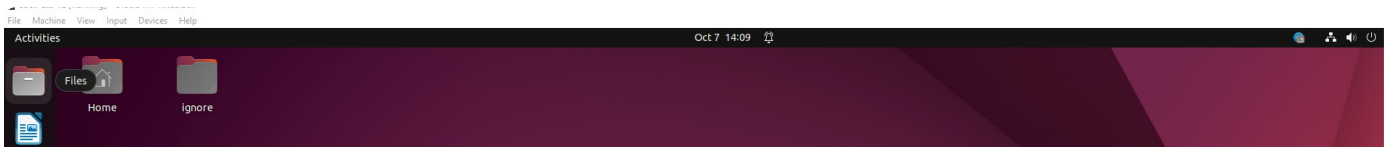
Specifically, we do 5 steps:

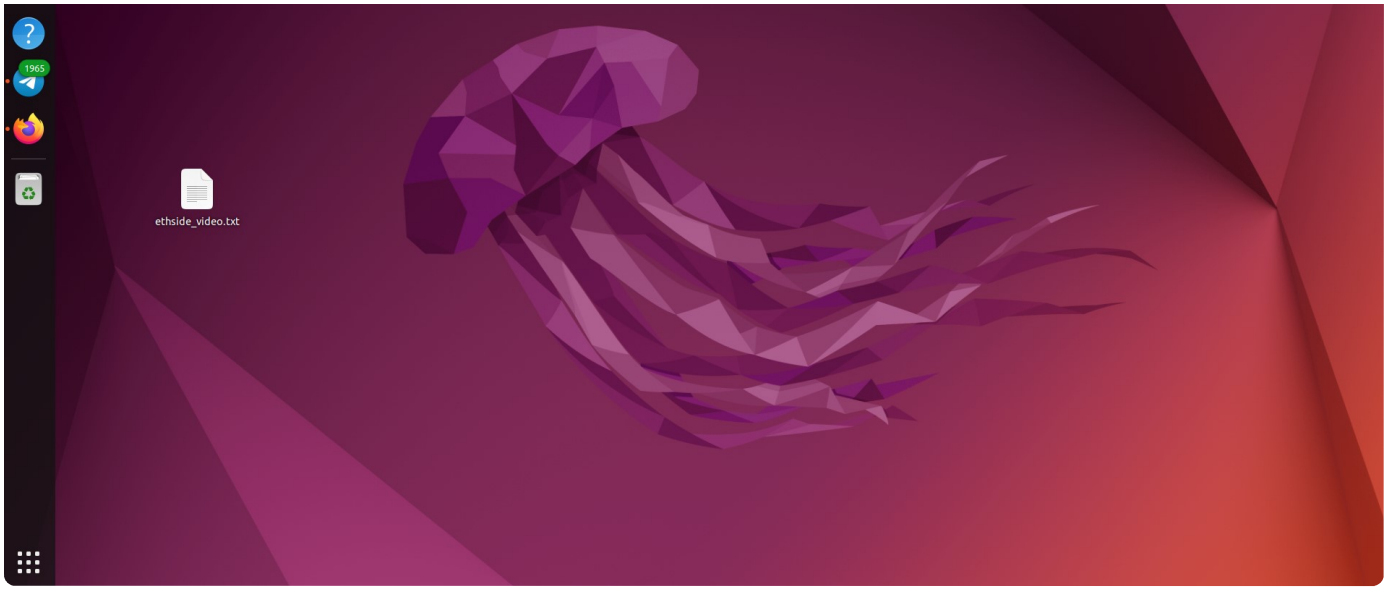
1. Open Linux, open three terminal windows, and make a project folder.
2. Use the first terminal window to: download the mainchain full node software, run it in regtest mode, force it to find 1 block every 5 seconds (for our convenience), and activate the ethereum sidechain on it.
3. Use the second terminal window to download, build, run, and connect "ethSide" (our ethereum sidechain clone). Via blind merged mining, it will also find a block every 5 seconds.
4. Use the third terminal window to play with ethereum – make accounts, use Eth functions, and especially: deposit 10 BTC from the mainchain to the Eth Sidechain.
5. Finally, we will go to remix.ethereum.org and plug our sidechain seamlessly into ETH's infrastructure. There we can run contracts.

Step 1: Set Up

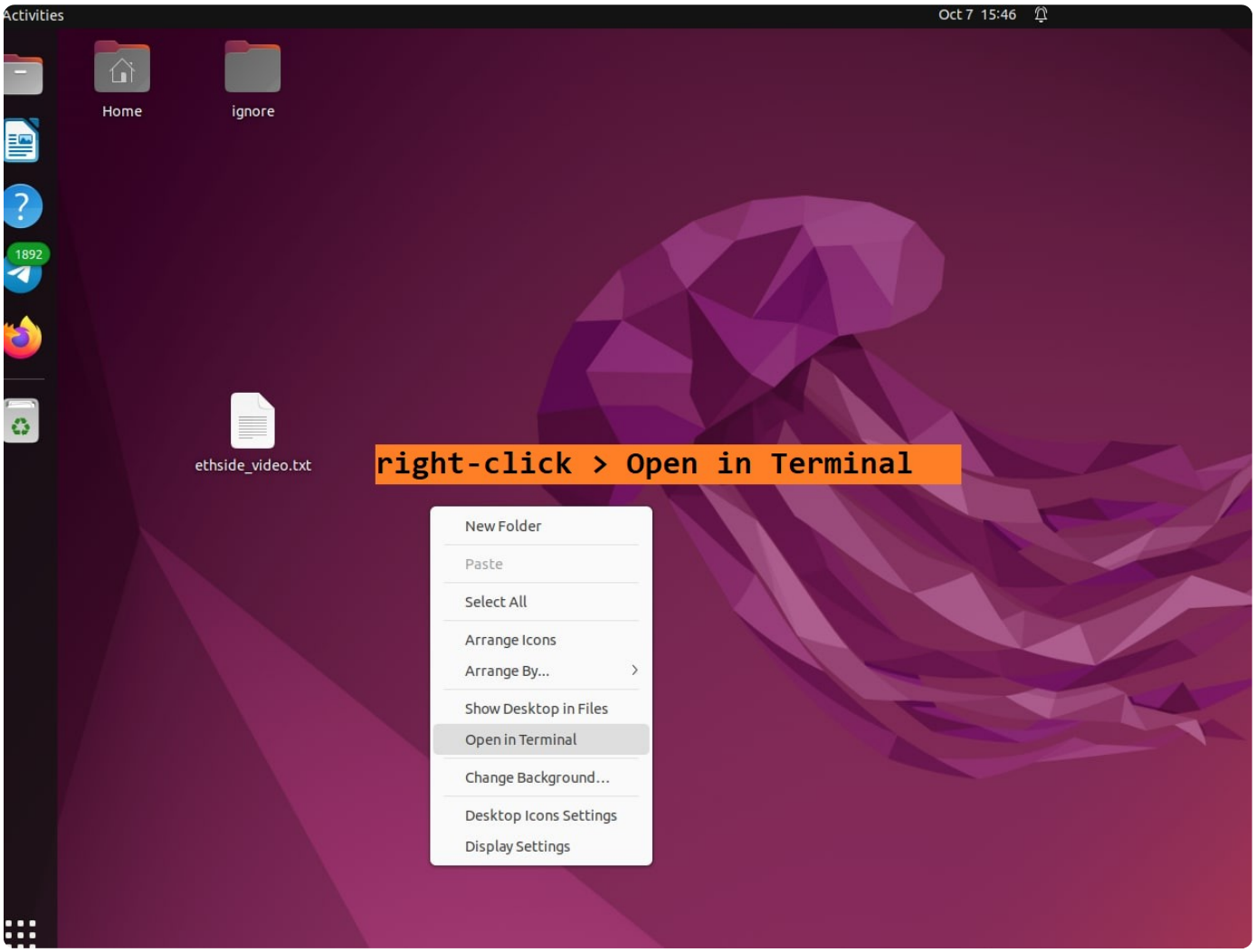
LINUX is needed. Mac/Windows users can run Linux for free, by using software such as VirtualBox (https://www.virtualbox.org/) or VMWare (https://www.vmware.com/products/fusion.html) – see these (https://www.wikihow.com/Install-Ubuntu-on-VirtualBox) guide (https://graspingtech.com/vmware-fusion-ubuntu-20.04/). This is easy & secure - it stops DriveNet from touching the rest of your computer.

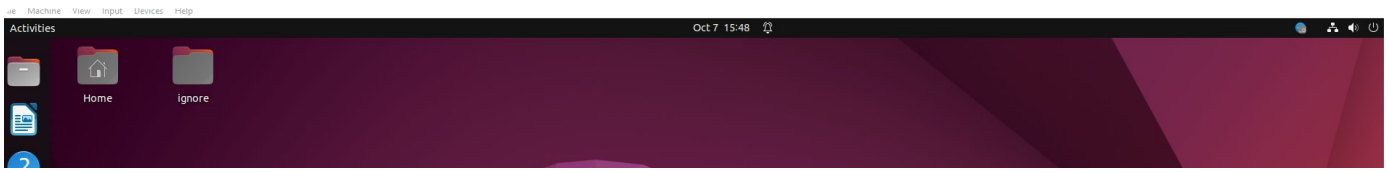
Below: you are looking at an Ubuntu desktop.

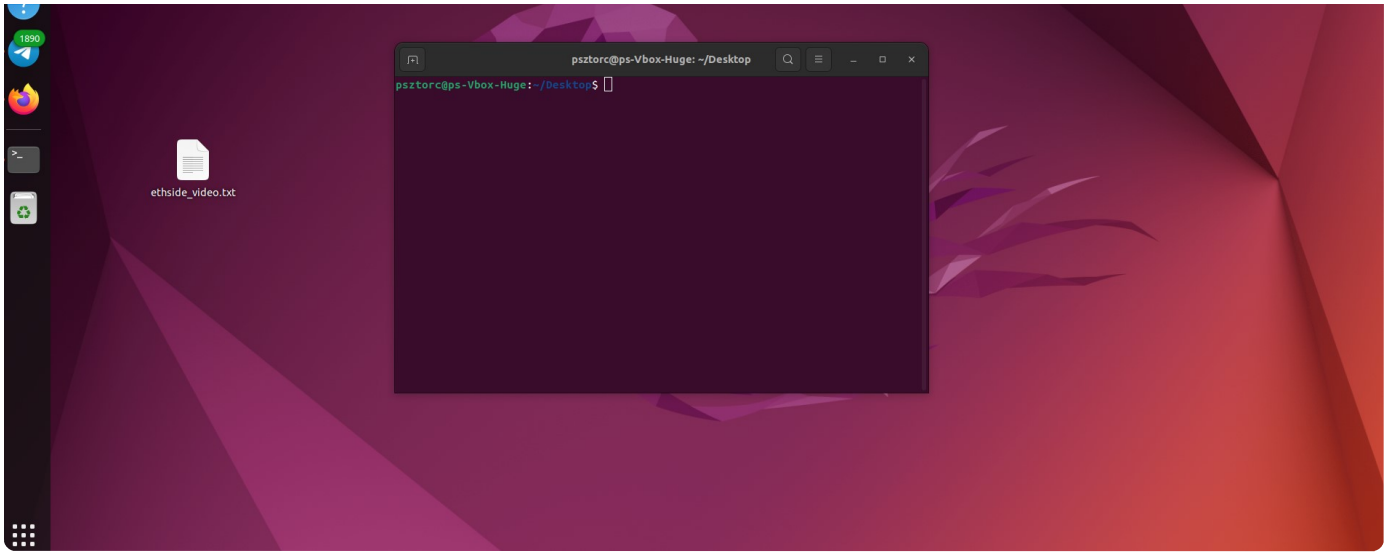




Open a terminal – (right-click -> “Open in Terminal”).





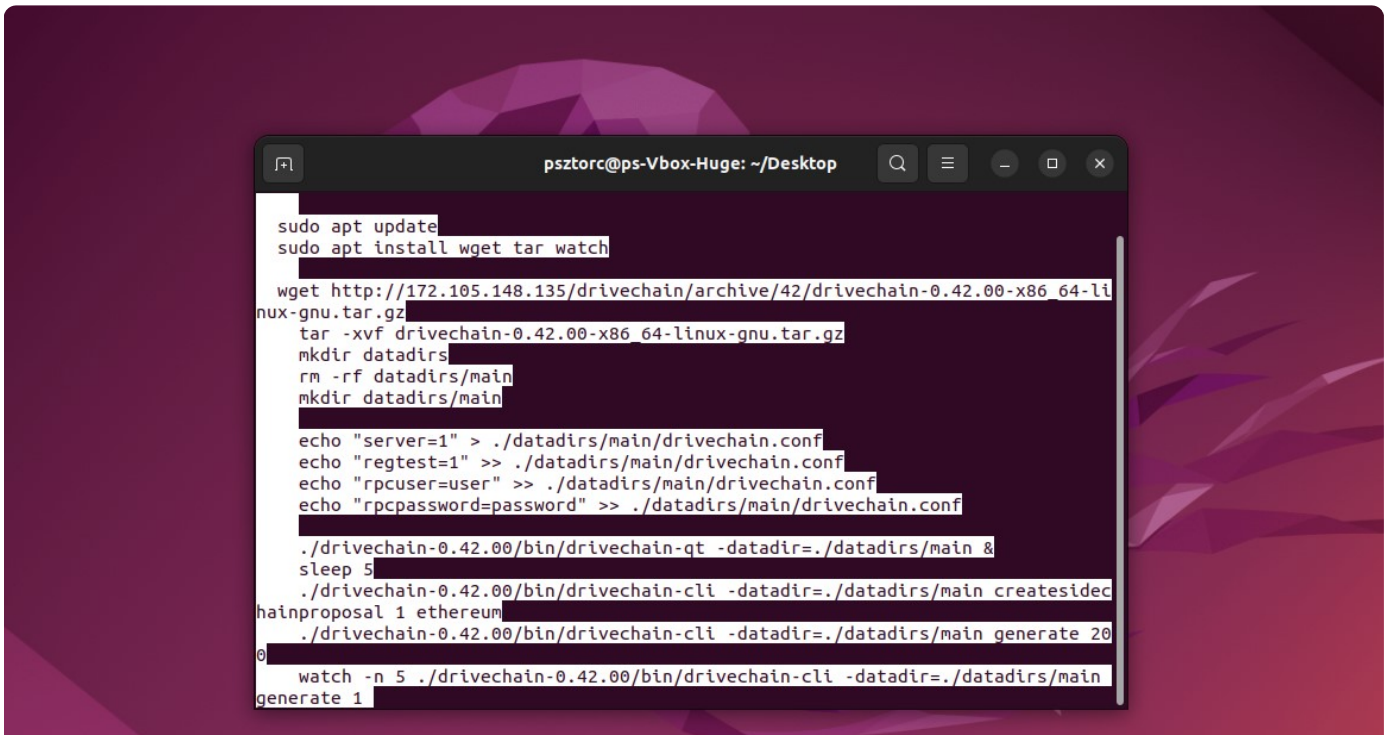


Step 2: Download & Use Mainchain

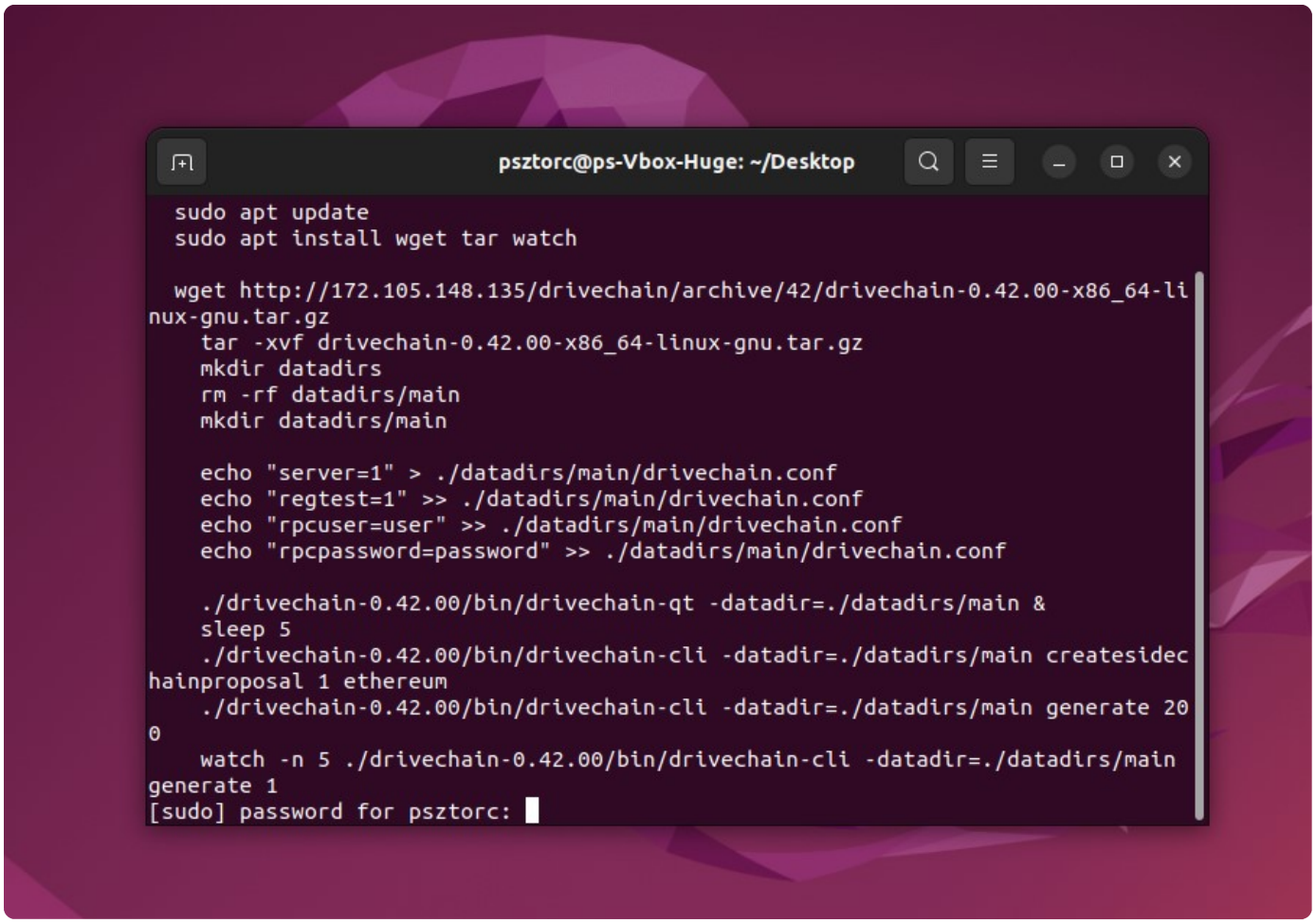
Now we want to do a bunch of steps: make a project folder, perform updates and install dependencies, download DriveNet-42, make a special directory for its blockchain to live (inside the project folder, where it won't bother any of your other files), turn DriveNet on (in regtest mode, so that we can do our testing unencumbered by proof-of-work), propose and then activate the ethereum sidechain (in sidechain slot #1), and finally order the regtest blockchain to find a block every 5 seconds.

In the terminal, run the following (copy/paste, with [cntrl + c], [cntrl + shift + v]:

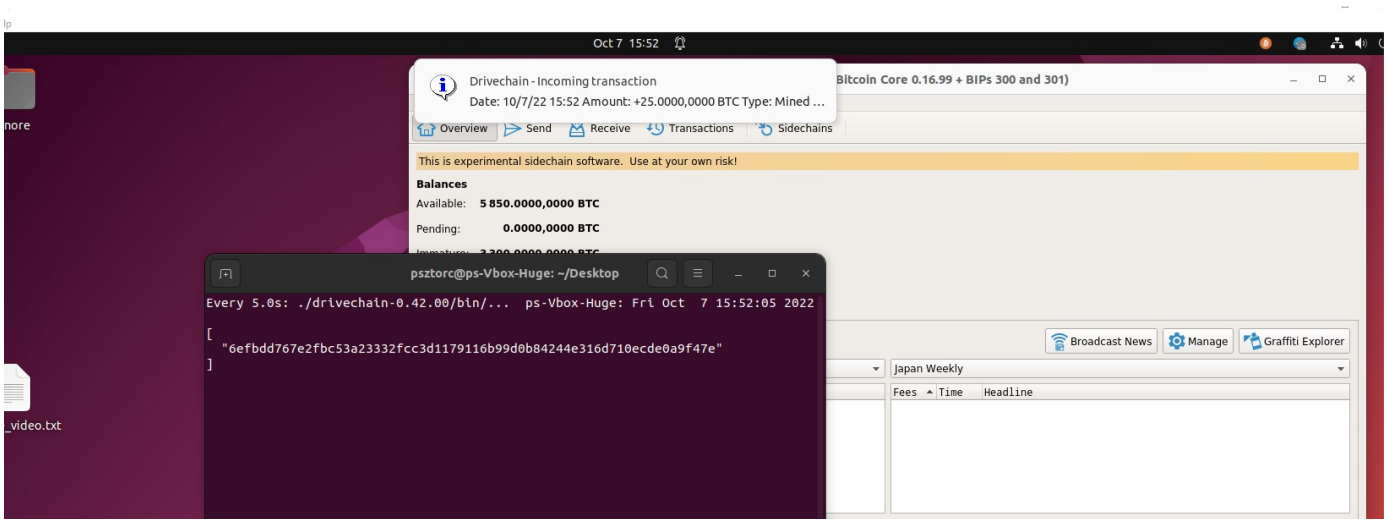
```
mkdir ethside_video
cd ethside_video

sudo apt update
sudo apt install wget tar watch

wget http://172.105.148.135/drivechain/archive/42/drivechain-0.42.00-x86_64-linux-gnu.ta
tar -xvf drivechain-0.42.00-x86_64-linux-gnu.tar.gz
mkdir datadirs
rm -rf datadirs/main
mkdir datadirs/main

echo "server=1" > ./datadirs/main/drivechain.conf
echo "regtest=1" >> ./datadirs/main/drivechain.conf
echo "rpcuser=user" >> ./datadirs/main/drivechain.conf
echo "rpcpassword=password" >> ./datadirs/main/drivechain.conf

./drivechain-0.42.00/bin/drivechain-qt -datadir=./datadirs/main &
sleep 6
./drivechain-0.42.00/bin/drivechain-cli -datadir=./datadirs/main createsidechainproposal
./drivechain-0.42.00/bin/drivechain-cli -datadir=./datadirs/main generate 200
watch -n 5 ./drivechain-0.42.00/bin/drivechain-cli -datadir=./datadirs/main generate 1
```

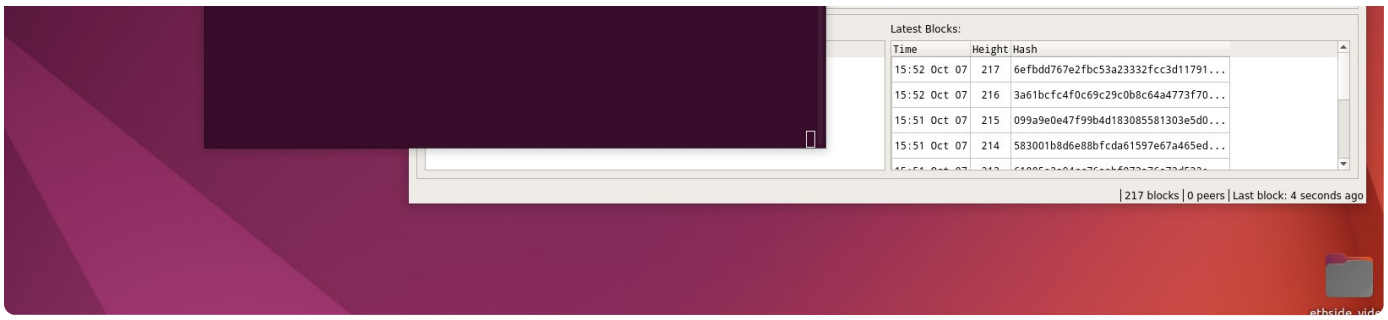


Because of "sudo", you may need your Ubuntu password (to give permission to install the updates):



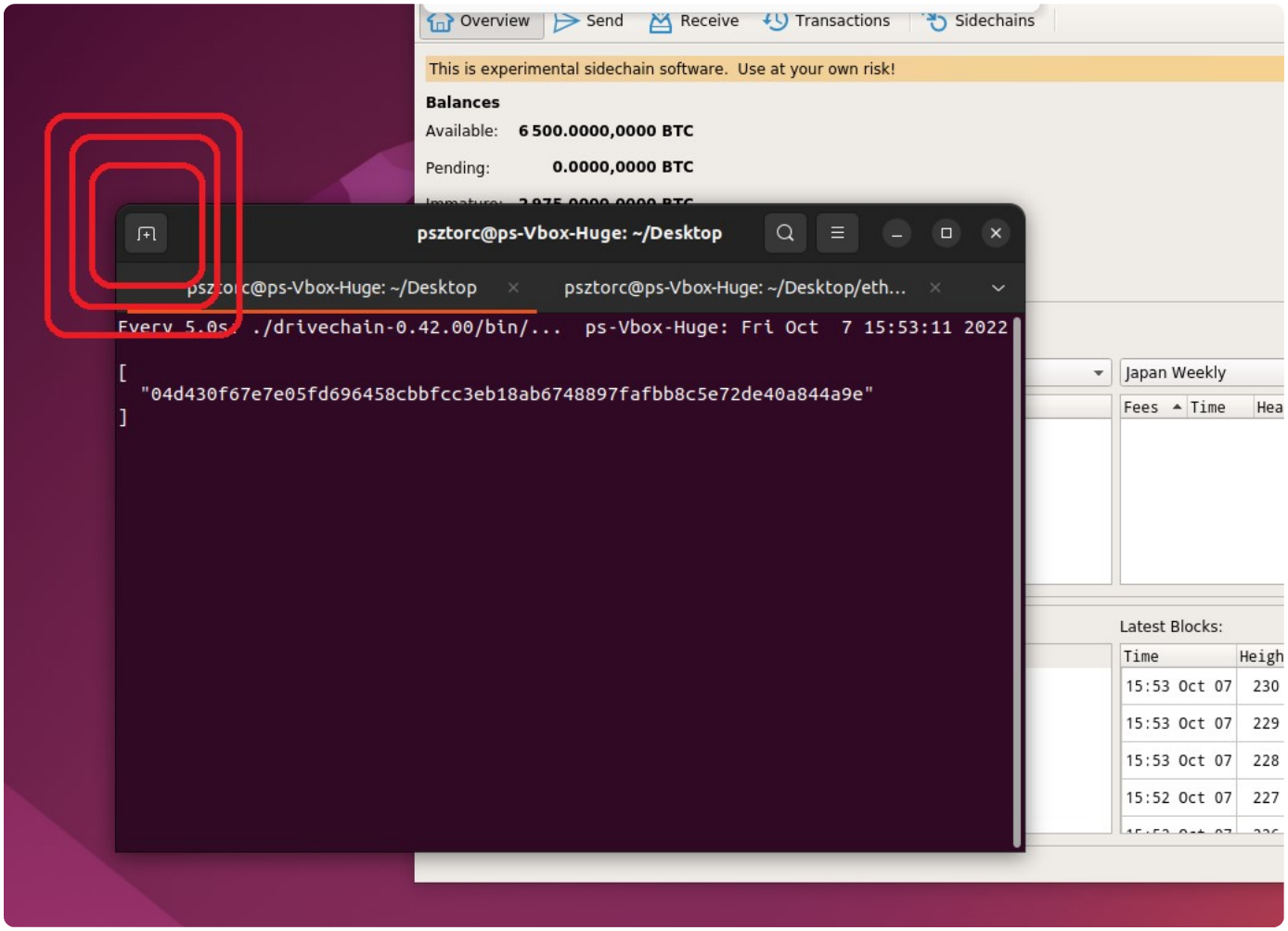
Below, we are finished: DriveNet is running in regtest mode, and finding a new block every 5 seconds:





Step 3: Download & Use EthSide

Now open a second terminal tab.



Now we want to download, build, run and connect EthSide (our sidechain-clone of Ethereum).

In the new terminal tab run:

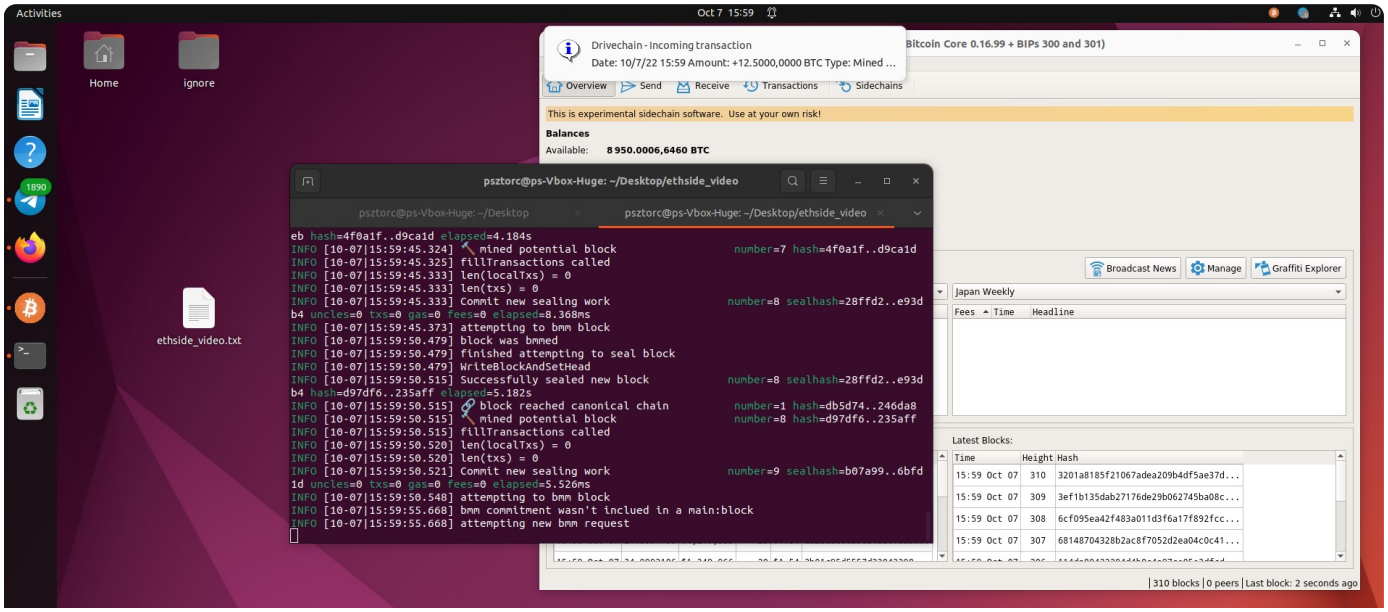
```
sudo apt update
sudo apt install git curl build-essential golang

curl --proto '=https' --tlsv1.2 -sSf https://sh.rustup.rs (https://sh.rustup.rs) | sh

git clone https://github.com/nchashch/ethereum-sidechain (https://github.com/nchashch/et
cd ethereum-sidechain
make

cd ..

rm -rf datadirs/eth
mkdir datadirs/eth
./ethereum-sidechain/build/bin/geth --datadir ./datadirs/eth init ./ethereum-sidechain/g
./ethereum-sidechain/build/bin/geth --http --http.api eth,web3,personal,net \
    --http.corsdomain "https://remix.ethereum.org (https://remix.ethereum.org)" \
    --datadir=./datadirs/eth --maxpeers 0 --dev
```

(It may ask you for your Ubuntu password again).

(It may also complain about Rust being already installed, if Rust is already installed for some reason, then there is no need to install it again.)

(The "Building" step can take a little while – 3 minutes or so.)

You should now be mining EthSide blocks:



Step #4: Playing Around With Ethereum

Open a third terminal tab.

And in it, fire up ethereum:

```
./ethereum-sidechain/build/bin/geth attach http://127.0.0.1:8545 (http://127.0.0.1:8545)
```

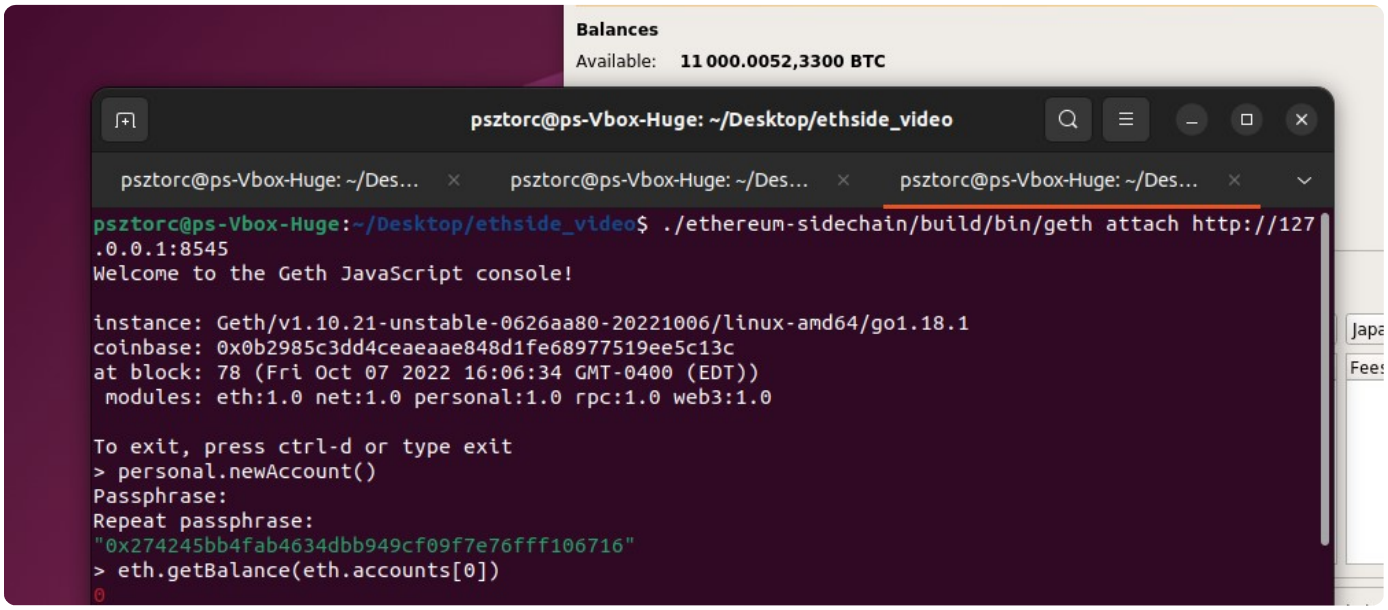
The Eth terminal is now on! You can now user Ethereum.

Try making a new “wallet”:

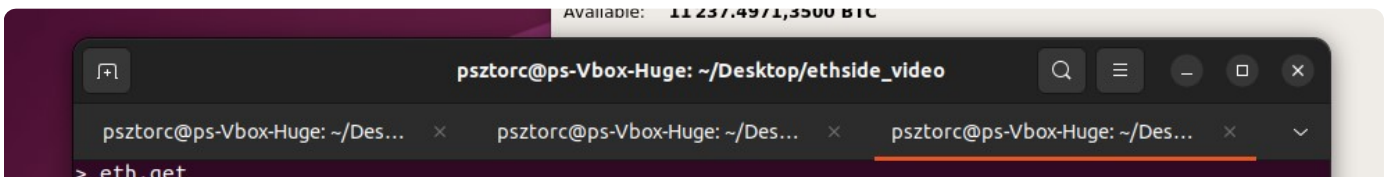
```
personal.newAccount()
```

Try checking your wallet balance – zero coins... for now.

```
eth.getBalance(eth.accounts[0])
```



Or use “help” (or Tab key), to see what you can try:



Finally, make sure that you run the following:

```
eth.deposit(eth.accounts[0], web3.toSatoshi(10), web3.toSatoshi(0.0001))
eth.getBalance(eth.accounts[0])
```

That command will take 10 of your BTC from the mainchain (since you've been mining this whole time), and sends them over to the ETH sidechain.

(Coin divisibility is different in ETH-world, so instead of getting 10,0000,0000 "sats", you instead get 10000000000000000000 aka 10 quintillion units 10,0000,0000,,00,0000,0000 of "side-gwei" (kind of like sats-squared). Isn't Ethereum fun!?)

(When the coins are sent back to the mainchain they will return to their original "sat"-level of divisibility.)

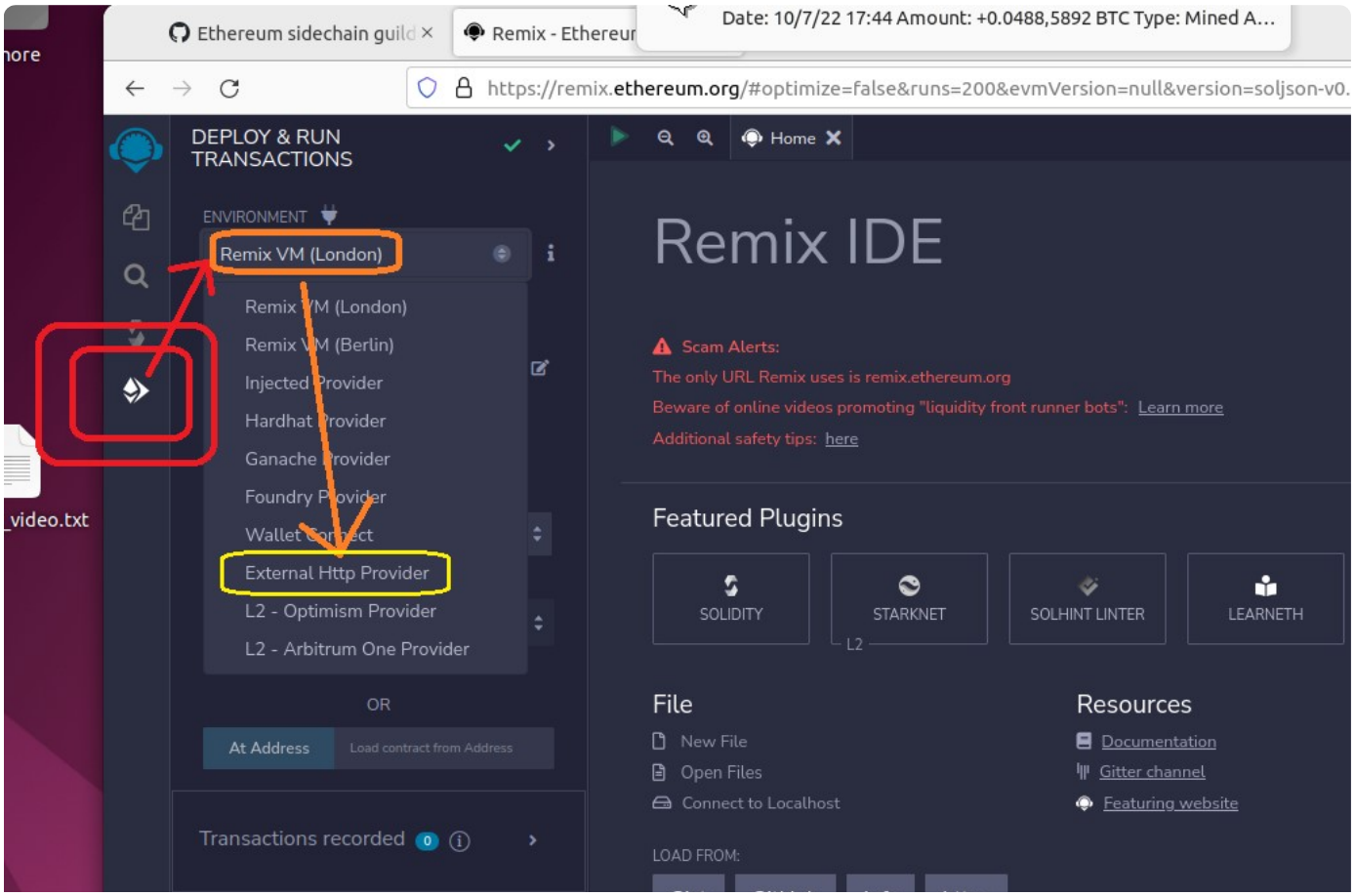
Now, take a break! You earned it!

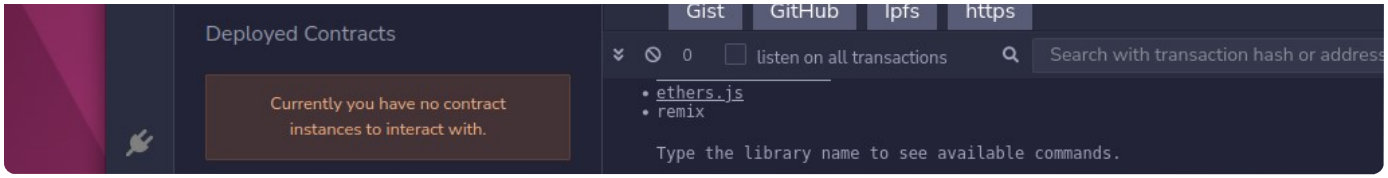
When we come back, we will take advantage of "remix.ethereum.org" (a dev website built by the ETH community).

Step #5: Hijacking Remix

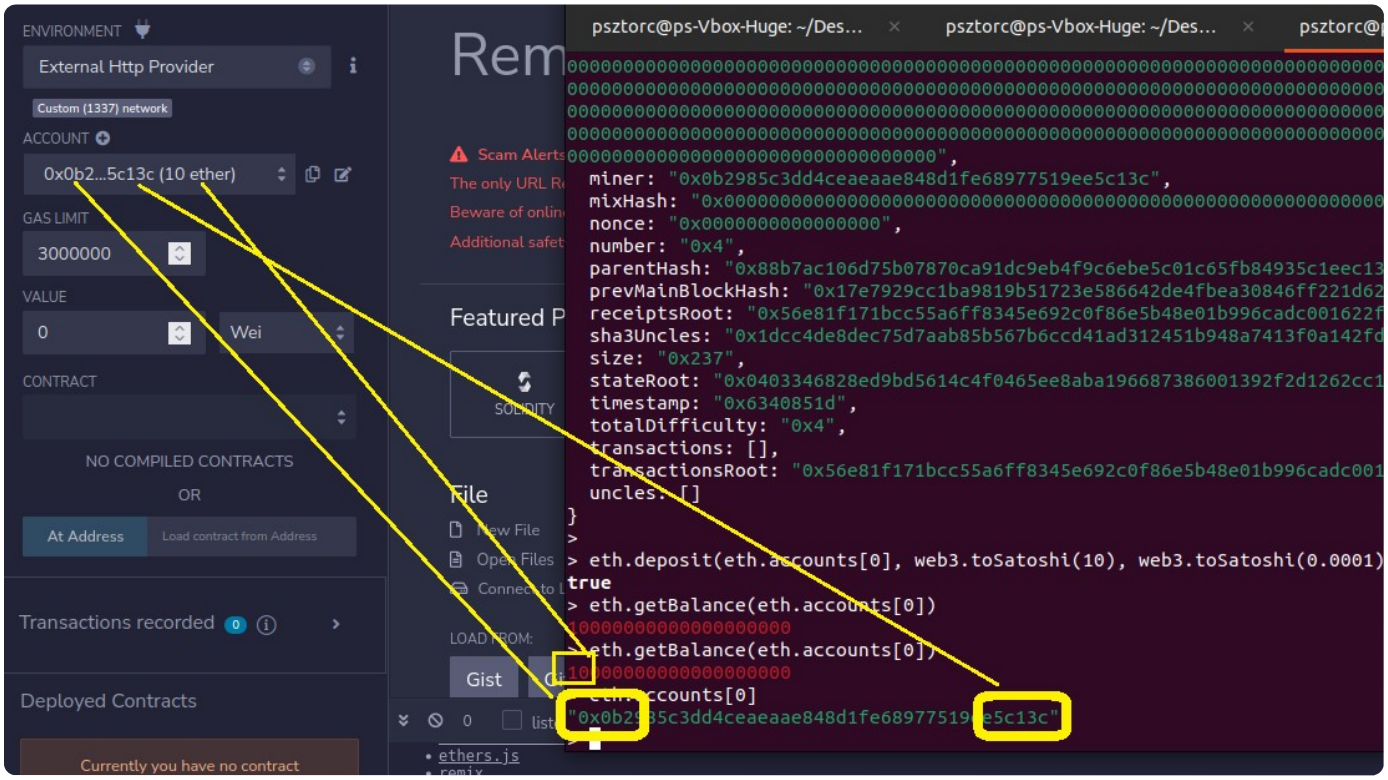
Now to invade the wider world of ETH – visit https://remix.ethereum.org/ (https://remix.ethereum.org/).

Like a wolf among sheep, click on the sidebar's ETH logo, then change "Remix VM (London)", to "External Http Provider".

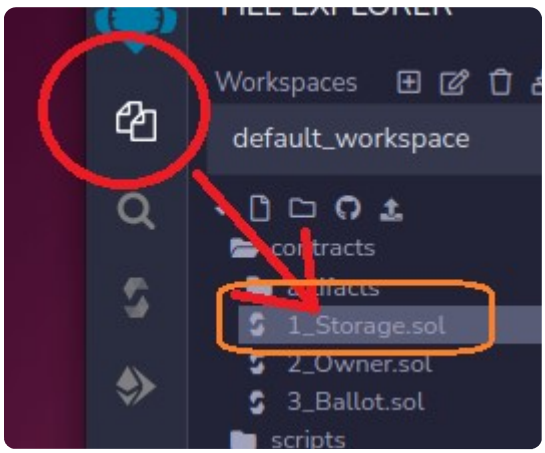




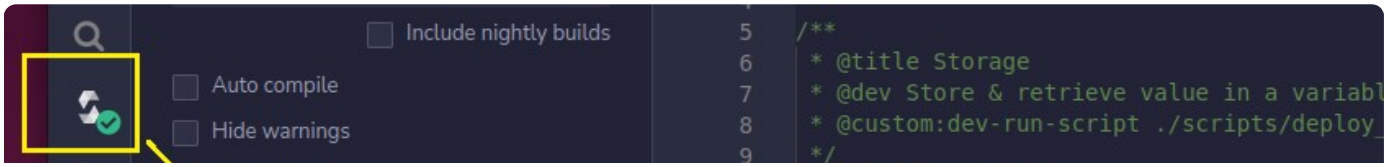
It will automatically connect to your EthSide node. It will even display the 10 "Ether" (that you deposited, from the mainchain).

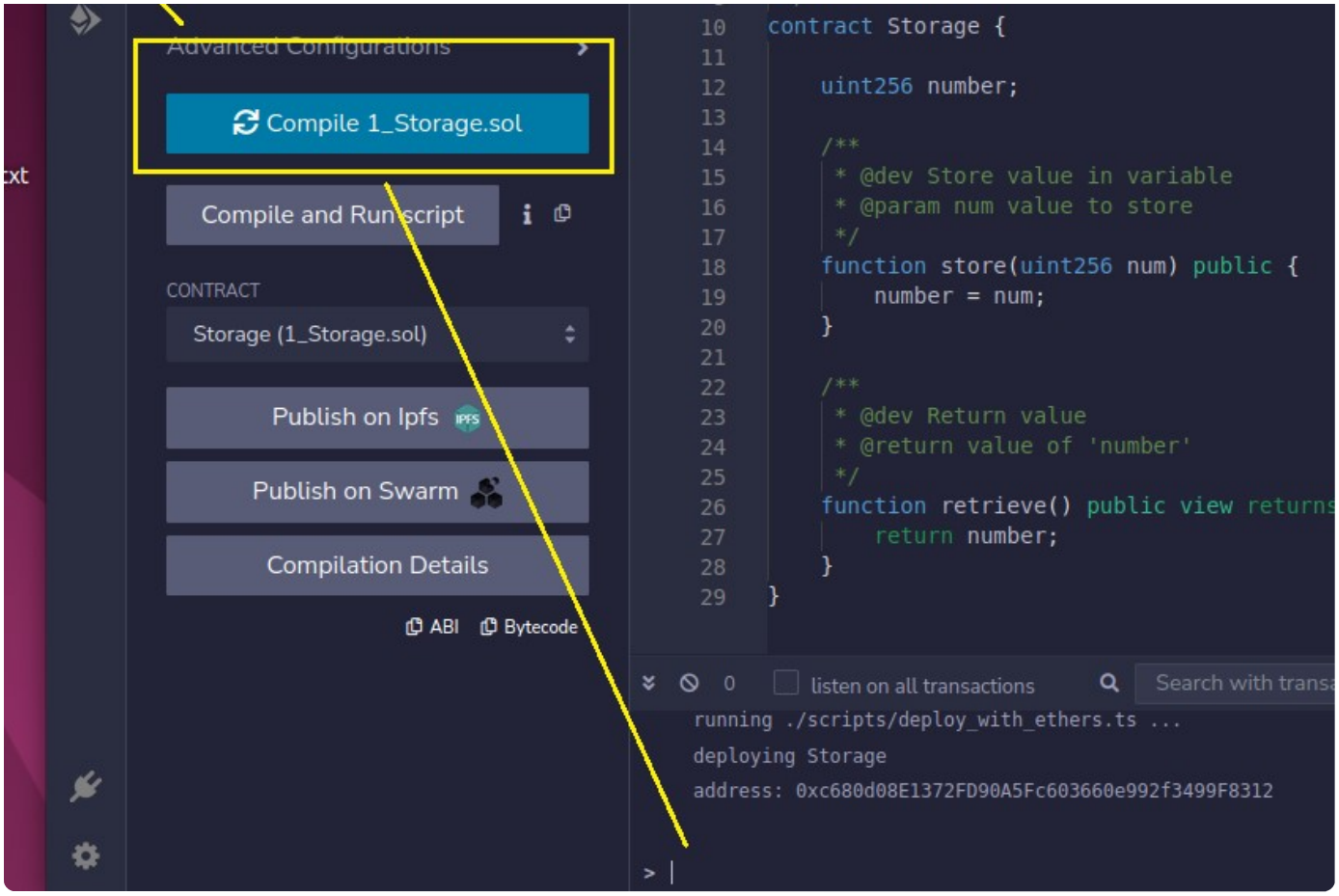


Now we can run the contracts on this site. For example, the "Storage" contract...

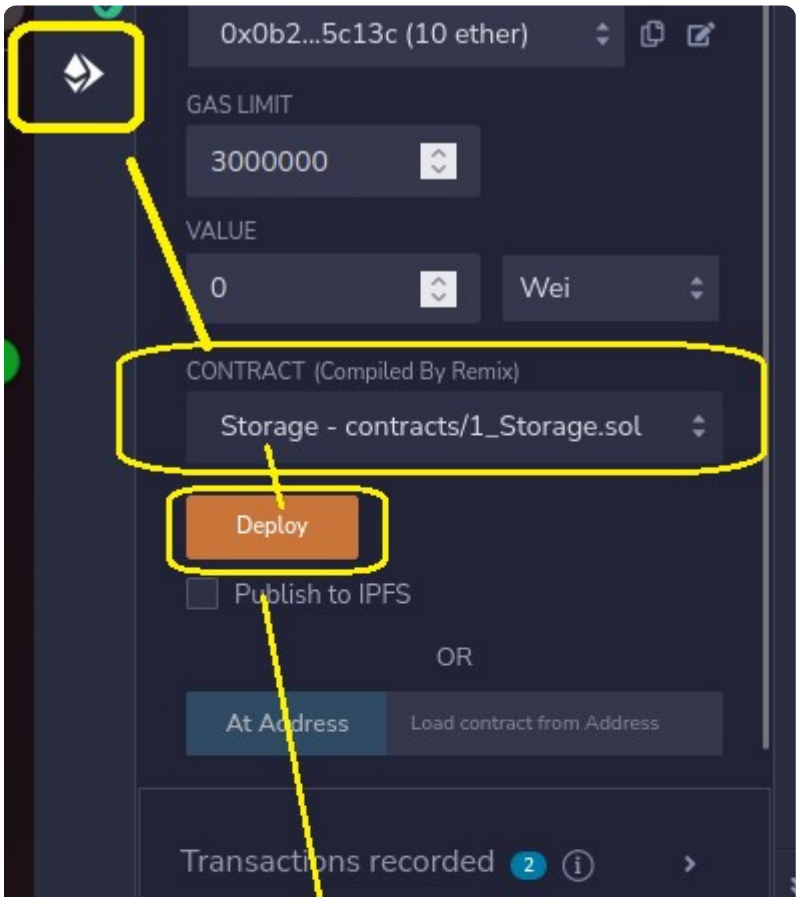


Once we select "1_Storage.sol", we can Compile it (on the third sidebar tab).

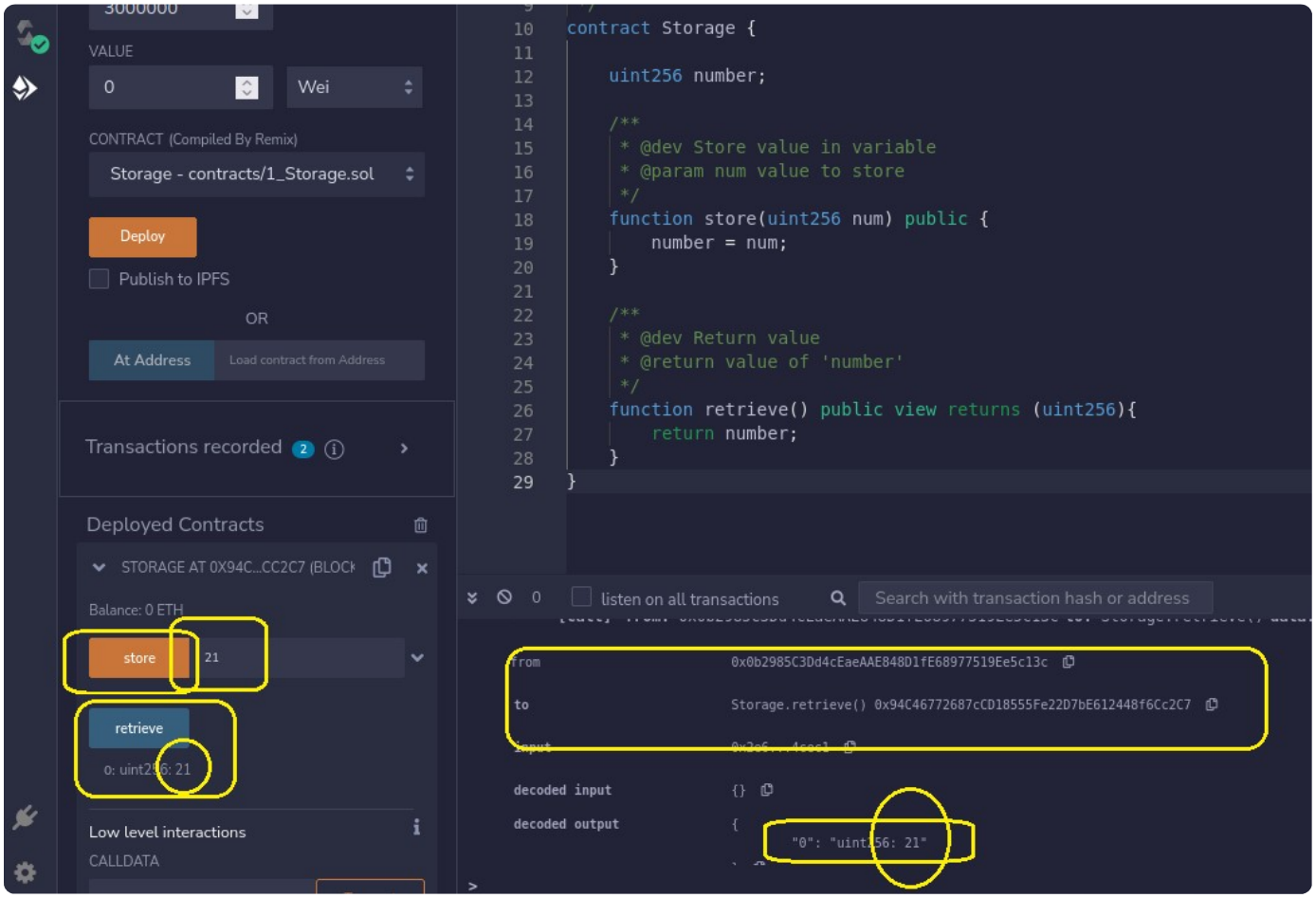




Once we Compile it, we can Deploy it on the fourth tab.



Once we Deploy it, we can make use of it! Specifically, in this case, we can use "1_Storage.sol" to store a number, and then retrieve it! The "magic" of Ethereum!



The walkthrough we did is very similar to the one advocated for on this site (https://geth.ethereum.org/docs/getting-started/dev-mode). You can explore the site and see how well the other guides apply!

In Conclusion

We ran an ETH contract... on top of BTC. We didn't buy any Ether! And we left Layer1 alone – our layer1 Bitcoin mainchain full node, knew nothing of Ethereum's rules.

This guide didn't cover withdrawals (ie: when coins move from sidechain to mainchain). But that's only because Bip300 withdrawals have already been covered to death.

OLDER · VIEW ARCHIVE (8) (HTTP://WWW.DRIVECHAIN.INFO/ARCHIVE)

Bip300: Getting to 100% Bitcoin Dominance (and Beyond)

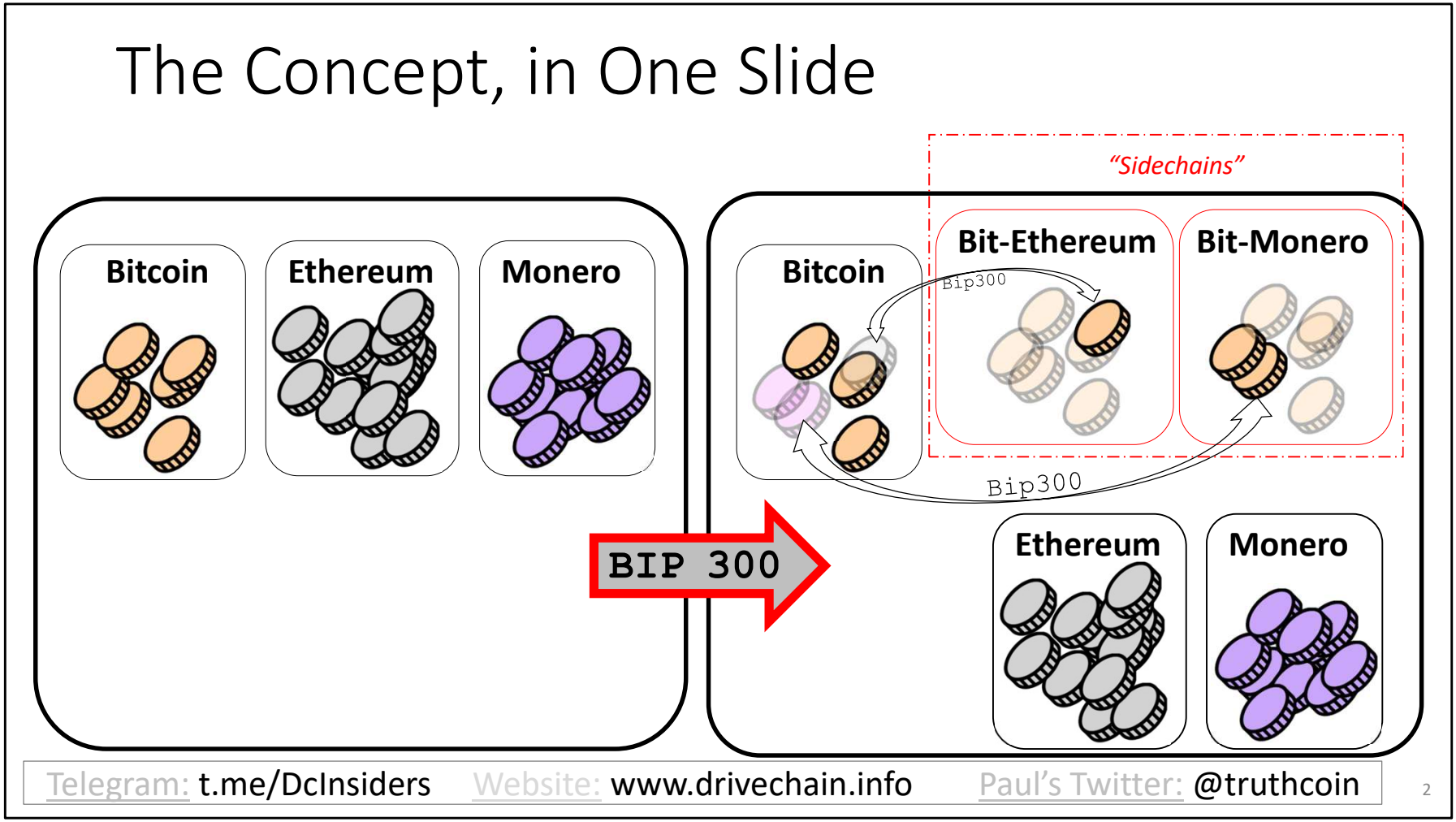
Paul Sztorc

TabConf 2021 -- November 5th

Telegram: t.me/DcInsiders Website: www.drivechain.info Paul's Twitter: @truthcoin

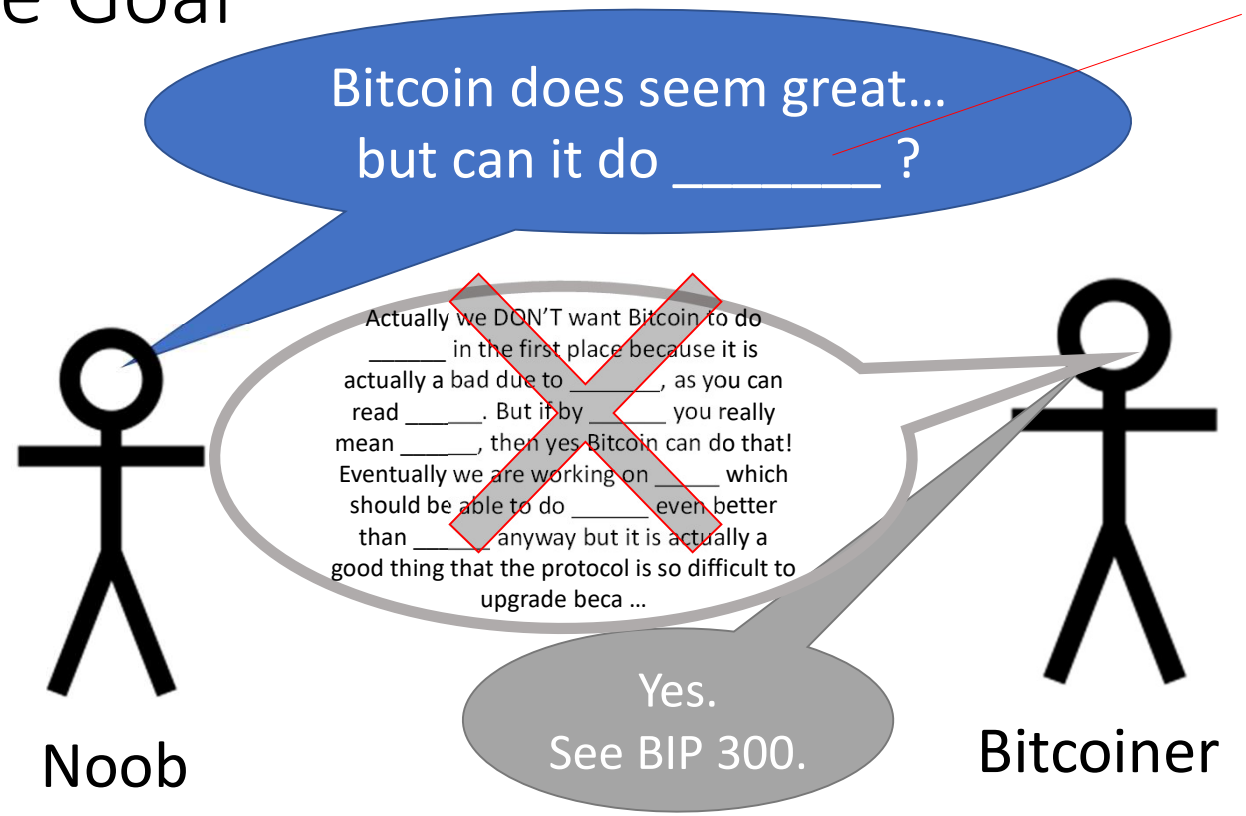
1

TRANSCRIPT OF SPEECH, 11/5/2021: Okay, hello. I've been invited to speak about Bip300 ... which is one of my ideas for taking Bitcoin to the next level. ...



Bip300 proposes these new layer2s, that some call "sidechains". Sidechains are a response to the threat of Altcoins, but they're also a response to the desire of Bitcoiners for creativity, and innovation – -- you know: the desire to try new things without asking for anyone's permission. How can we let everyone try the ideas that they like? And how do I keep other people's bad ideas away from me? So here you see we have the world of Altcoins on the left, but then, the revenge of Bip300 on the right. We have copied Ethereum and Monero into our own projects that respect the 21M coin limit of BTC. No inflation.

The Goal

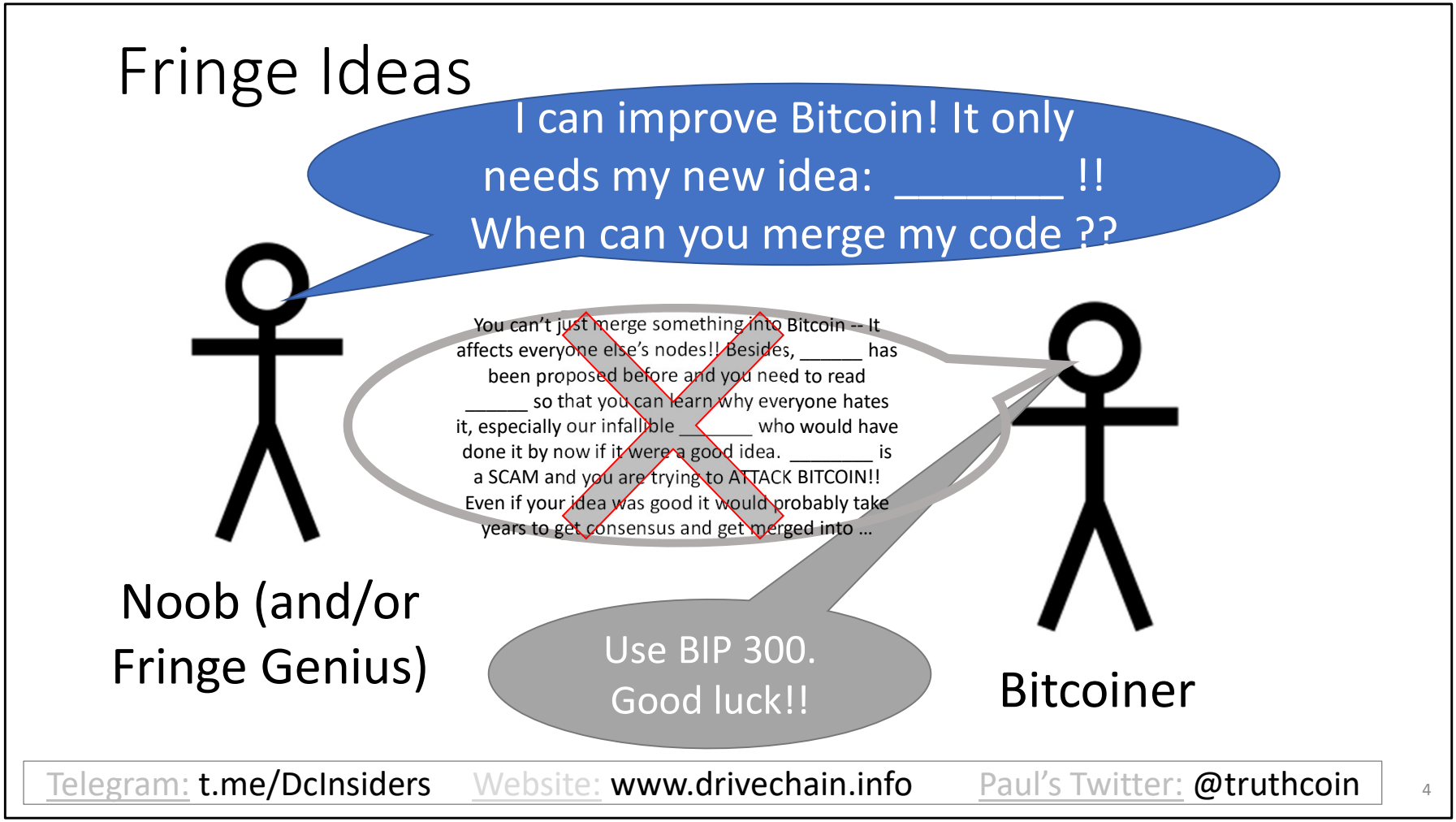


Smart Contracts
DeFi
Turing Completeness
Ring Signatures
zk-Snarks
Large Blocksizes
NFTs
Oracles
Mimblewimble
…(etc)

Telegram: t.me/DcInsiders Website: www.drivechain.info Paul's Twitter: @truthcoin

3

Ideally, with Bip300, if some annoying person asks "Sure Bitcoin seems great, but can it do .... smart_contracts, DeFI, zk-snarks, blah blah, you just say "Yes, Bitcoin can do that – see Bip300".



Similarly, if some innovator dreams up a crazy idea, "Hey I can improve Bitcoin, it only needs my new idea ... larger blocksizes, Turing Completeness, KYC-miner-coins?" Then: similarly, they now can do that without anyone's permission. They just don't do it on Bitcoin base layer, they do it on a Bip300 sidechain.

So: that's the goal – FREEDOM. Developers can write whatever code they want, users can use that code if they like. Everyone gets what they want. But how is it accomplished?

Three Aspects

1. Full Autonomy
2. Protect Base Layer
3. Improve Miner Incentives

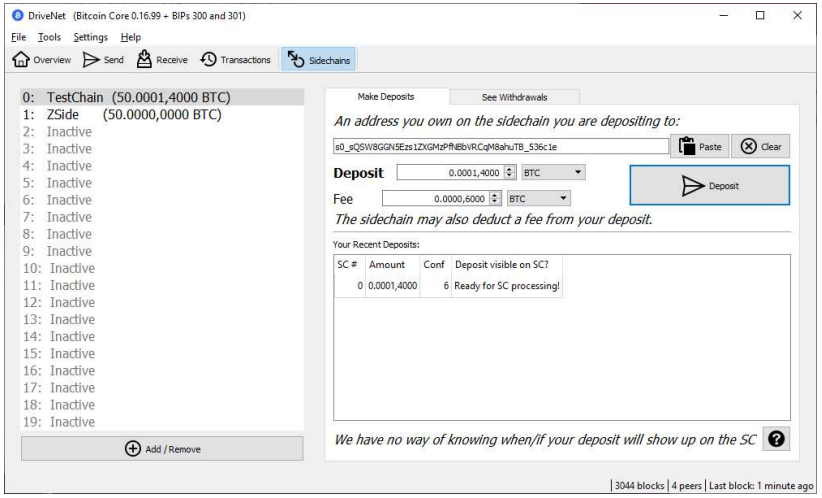
Releases

Download Latest Version (v40)

Software	Linux	Windows	Mac	Source
Mainchain v40.01	tar.gz	.exe	dmg, tar.gz	Github
Testchain v14	tar.gz	.exe	n/a	Github
Trainchain v77	tar.gz	.exe	n/a	Github
Thunder v5	tar.gz	.exe	n/a	Github
zSide v5	tar.gz	n/a	n/a	GitLab

Click here for CHECKSUMs

Not Vaporware



YouTube

Bitcoin-ZCash Sidechain (Regtest Demo)

489 views • Mar 1, 2021

ivechain.info Paul's Twitter: @truthcoin

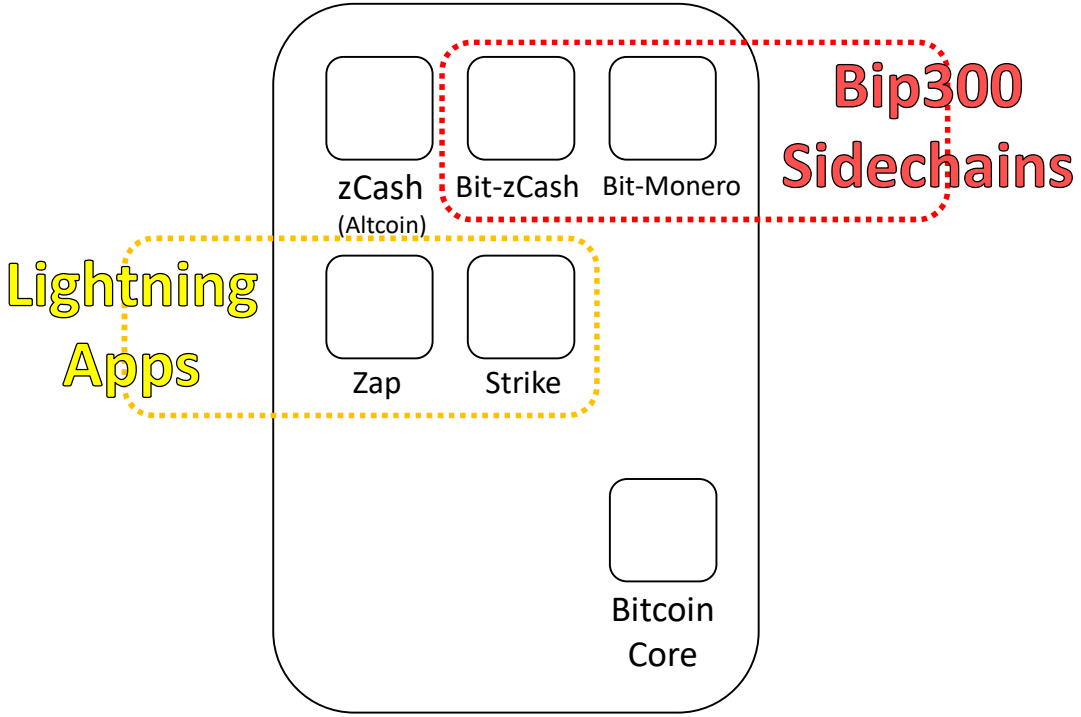
5

I will break the idea down, into three aspects. These are: Full Autonomy ; Protect the Base Layer ; and Improve Miner Incentives.

Before continuing, however, I did want to mention, that this project is not vaporware. The code is open source (on Github, right now!), there's downloads with a GUI (we have Windows/Mac versions now), and there's even a YouTube video of me, using Bip300 on testnet, to copy the zCash Altcoin. So the software is very use-able, you can download it right now. Ok now back to these three aspects.

(#1) Full Autonomy

Metaphor



Telegram: t.me/DcInsiders Website: www.drivechain.info Paul's Twitter: @truthcoin

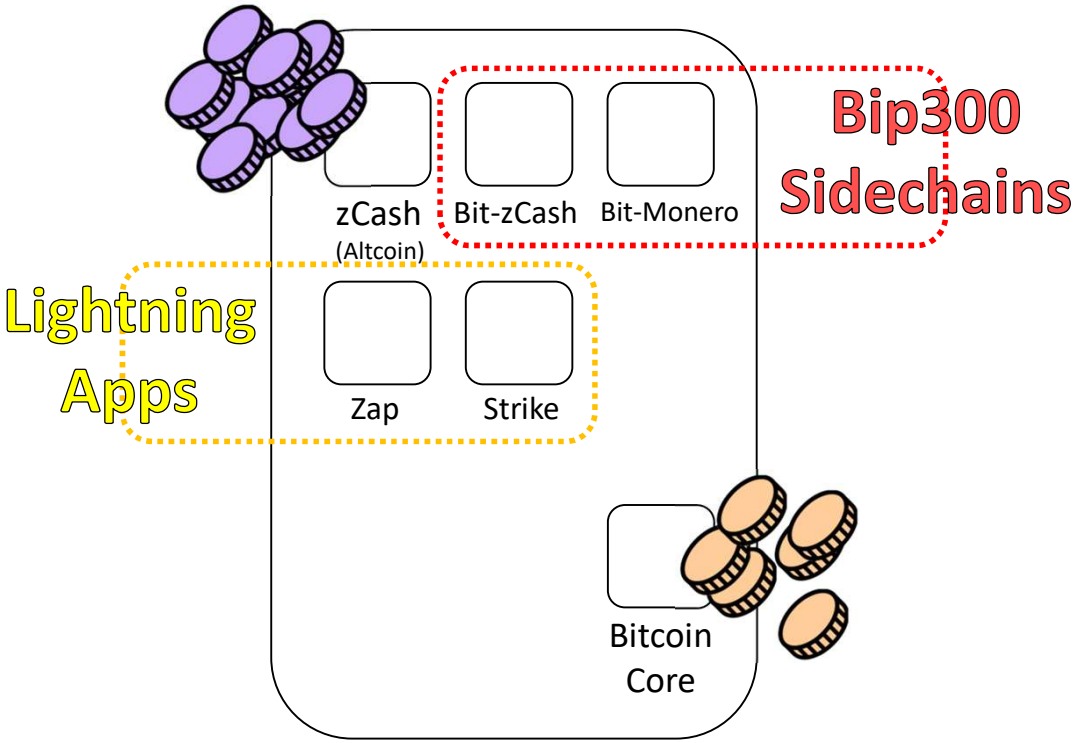
6

Aspect number one: full autonomy. Each new Bip300 sidechain is its own 'app' and you can change the sidechain software however you like. It's just like making a new iPhone app: each "app" has its own development team, the software they write can have any validation rules, (!) or no validation rules.

But, for example, they could add: zk-snarks, higher Blocksize, turing complete scripts, Taproot, mimblewimble, Monero ring-signatures, whatever you like. Any idea –good or bad— can be done and no one can stop them. It's just like releasing a new iPhone app. Each project starts with zero Bit-coins on them. No coins.

(#1) Full Autonomy

Metaphor

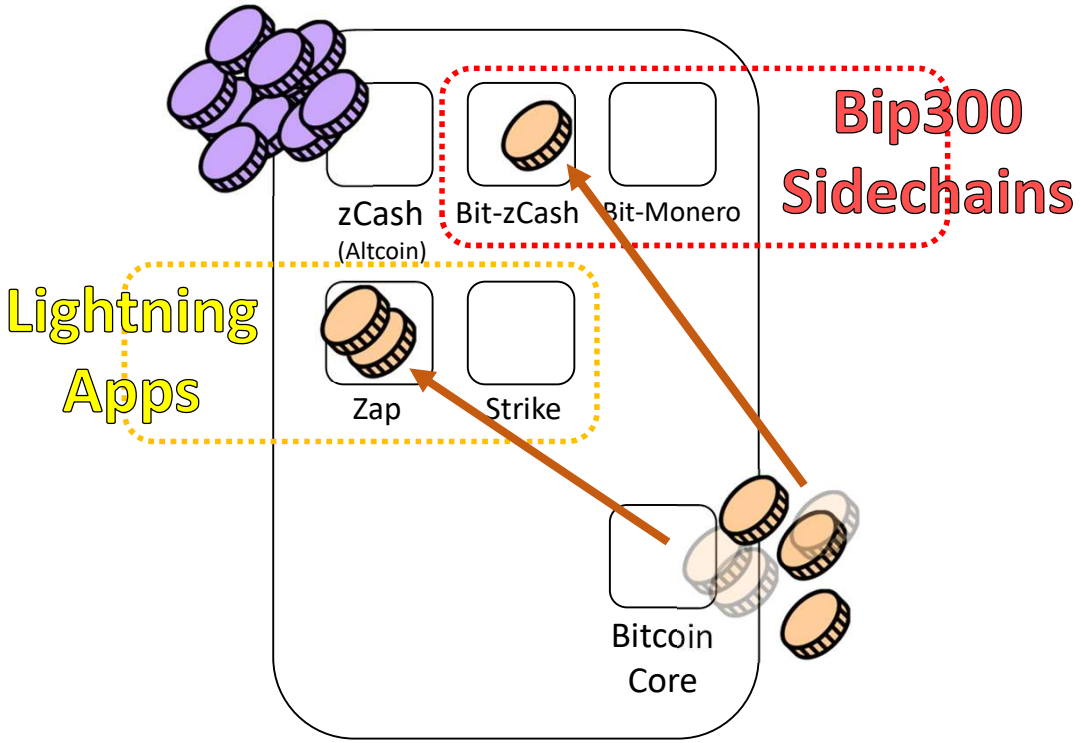


Telegram: t.me/DcInsiders Website: www.drivechain.info Paul's Twitter: @truthcoin 7

Coins travel from layer1, to these other networks. Users have to voluntarily choose to send their BTC over. To your software. Just like a lighting App. (So it's a good comparison). Those purple coins are Altcoins ... we don't like those. But next to it is a sidechain that does the exact same thing. So....

(#1) Full Autonomy

Metaphor

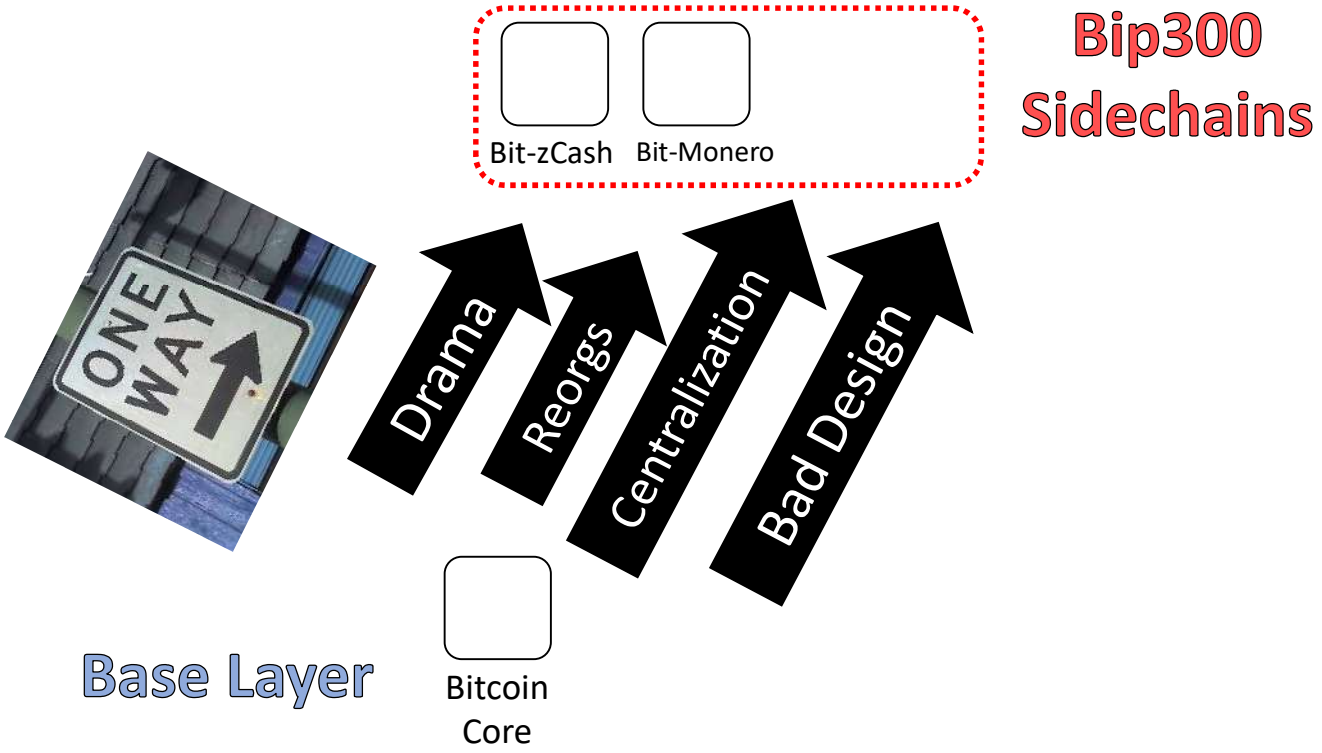


Telegram: t.me/DcInsiders Website: www.drivechain.info Paul's Twitter: @truthcoin

8

here you see the coins move over. Two coins to Zap, in the lightning world; and one coin to Bit-ZCash, in the Bip300 world. Still 21 million coins total.

(#2) Base Layer is Safe

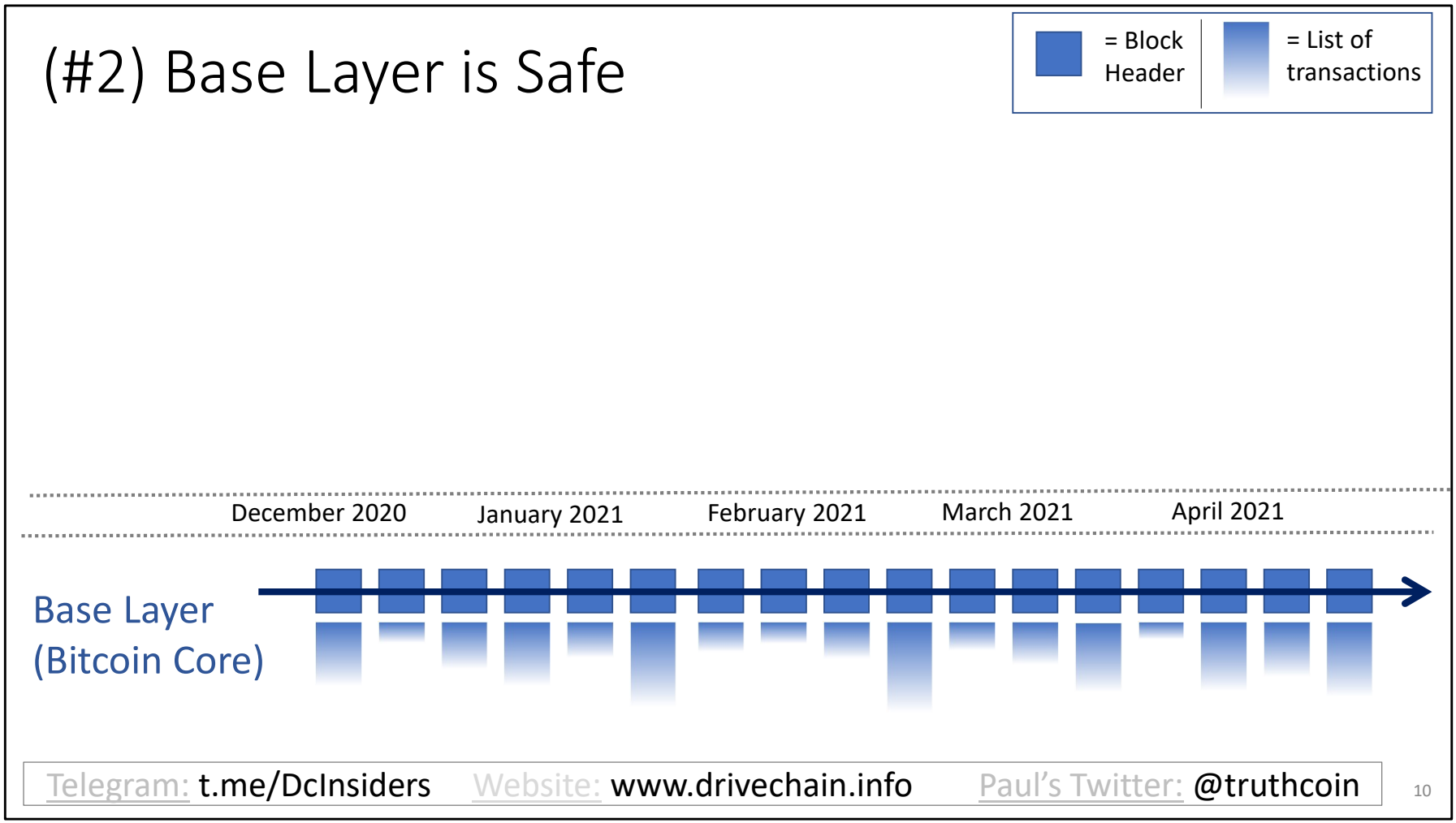


Telegram: t.me/DcInsiders Website: www.drivechain.info Paul's Twitter: @truthcoin

9

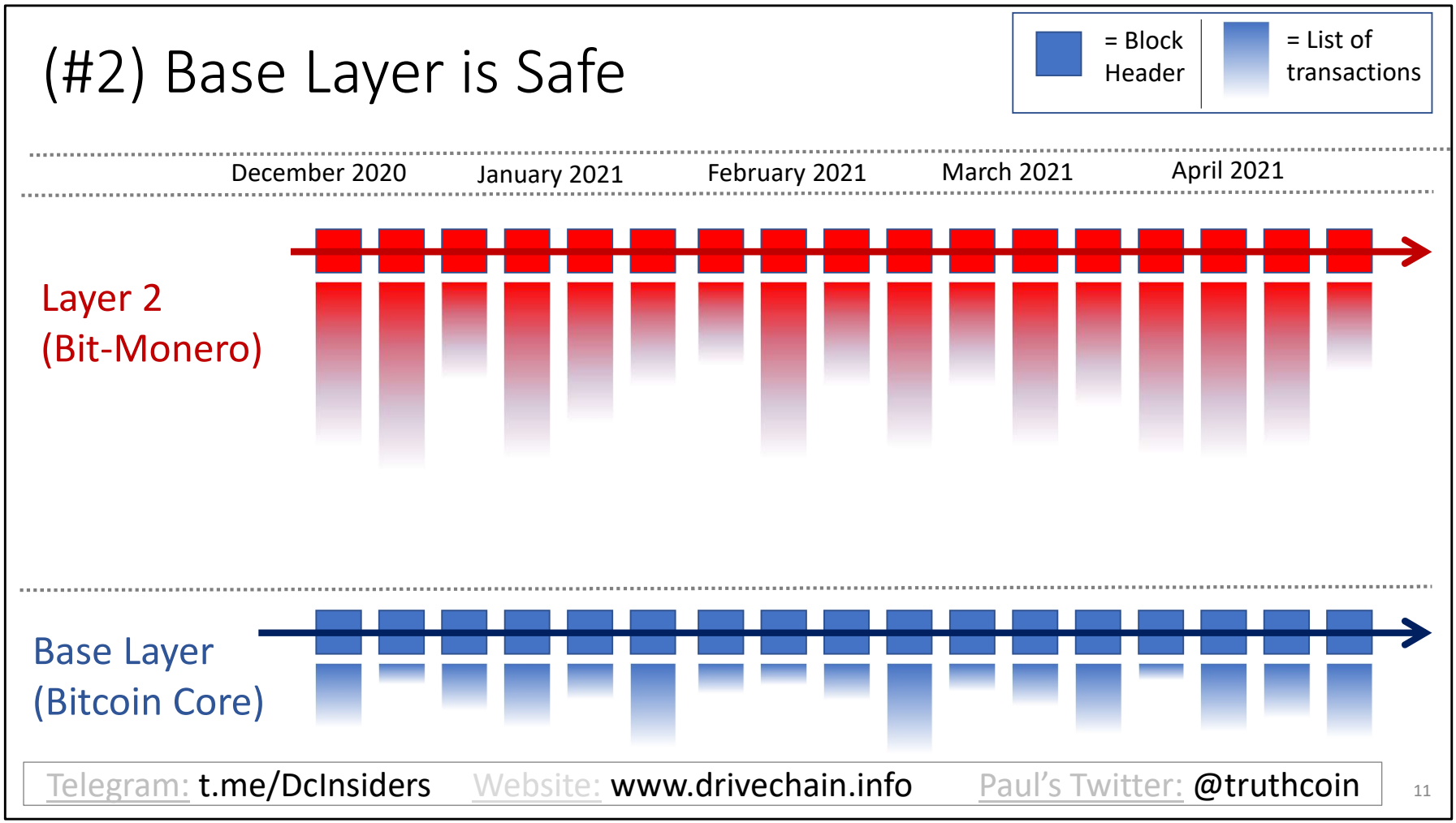
Ok, aspect two – the base layer (ie, Bitcoin Core, ie the mainchain, ie "layer1") that – your Bitcoin node -- is unaffected by problems on the sidechain. Even under very extreme adversarial conditions where the sidechain experiencing all sorts of chaos, Layer1 is just going to solider on, and ignore all of that. The drama can only go one way. So, let me try to explain this.

(#2) Base Layer is Safe

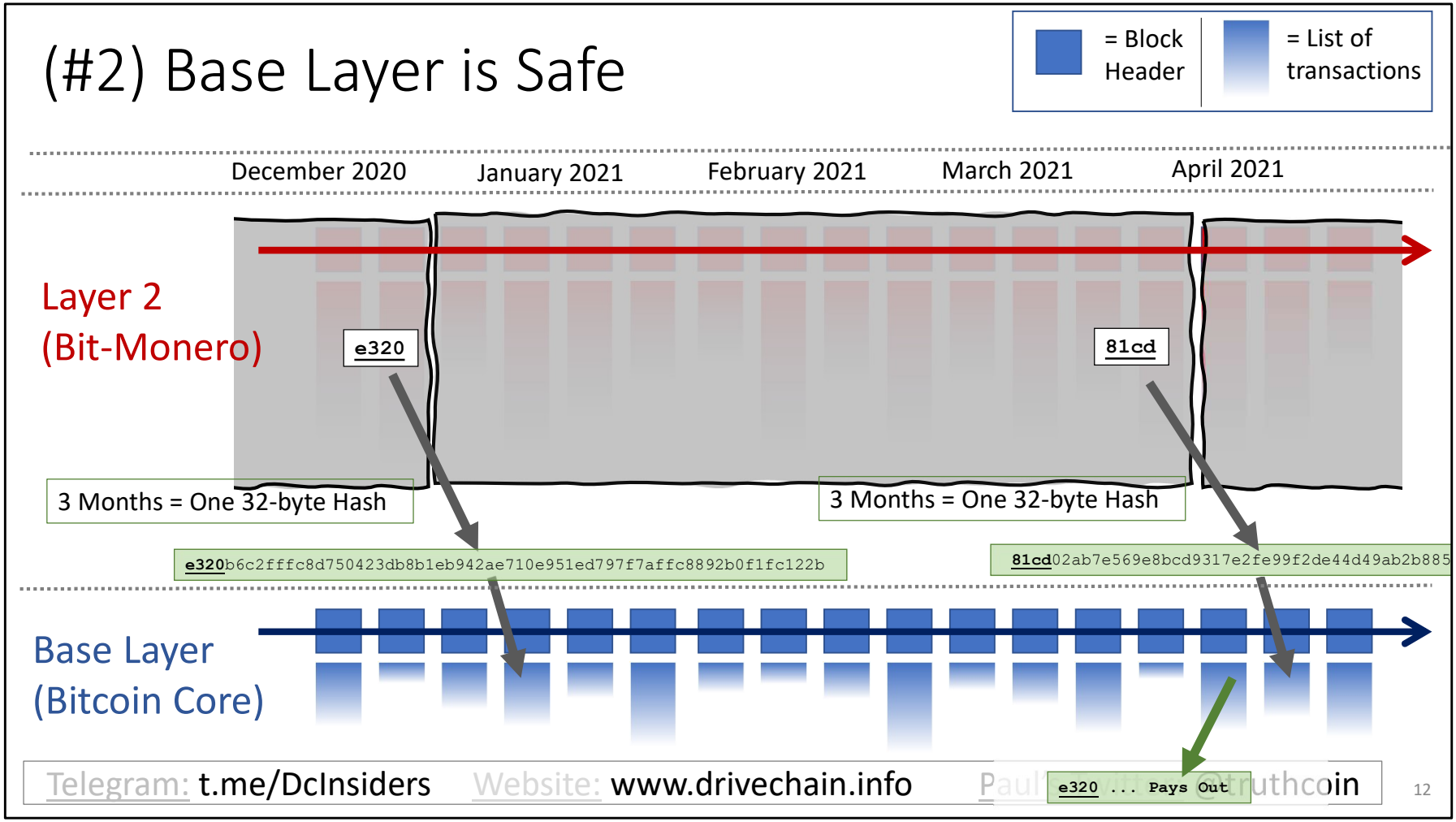


Here is a representation of Bitcoin's blockchain. The squares are block headers, and the trailing rectangles are the list of transactions in each block. (Because blocks aren't always the same size, of course.) And time is flowing from left to right. You can see across the top I'm going from Dec to April. Normally, of course, there would be tens of thousands of blocks (from Dec to April), that wouldn't have *FIT on the slides* so there's only seventeen.

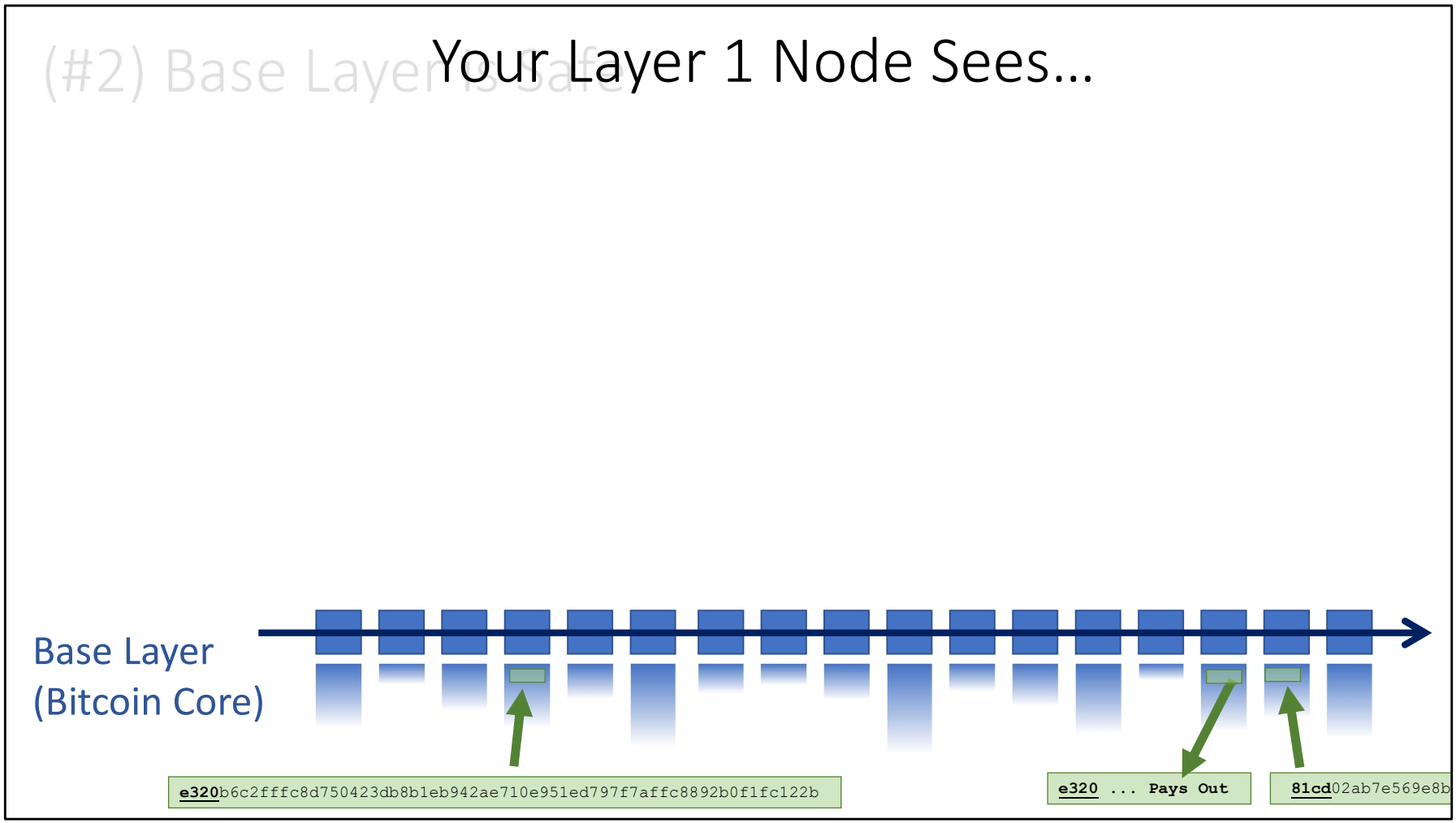
Now, what if there was a sidechain, activated, this whole time? Like a clone of Monero, or something. Well, we'll put it up...



Here it is. It has its own blocks, and its own block headers, and its own block chain, from December (on the left) to April (on the right). Now, the idea is ... that ...



... Three months of sidechain activity are compressed into one little 64-character string here. And that string is the only thing inserted into Layer1. Ever. So, no matter what Bit-Monero over here is doing, *this* is all that layer1 will see.. ready ?

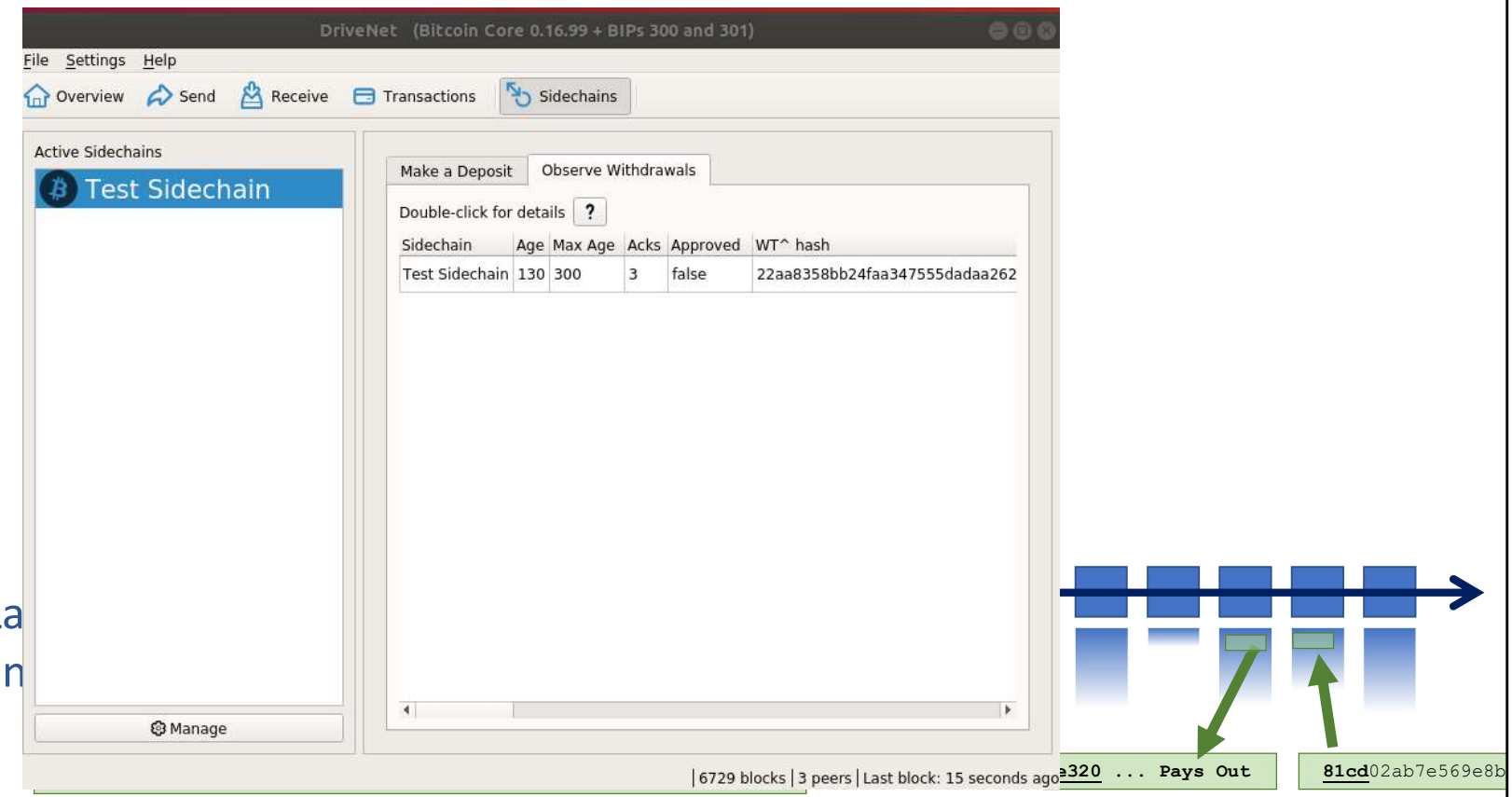


This.

Therefore, full nodes (on Layer1, down here in blue); they do not check anything that is happening on the sidechain (where there can be, theoretically, unlimited complexity). The sidechain doesn't need to be a blockchain, it doesn't need to be written in c++, it can make all kinds of mistakes. Etc. Bip300 operates entirely off of this one little string (here in green). (!) It does *a lot of logic* to that 4 little string, and assumptions and engineering, game theory economics, etc. I don't have time to explain all of it. But the point is that Layer1 can't be harmed by Layer2 because it really is ignoring Layer2.

I feel compelled to drive this point even further, so...

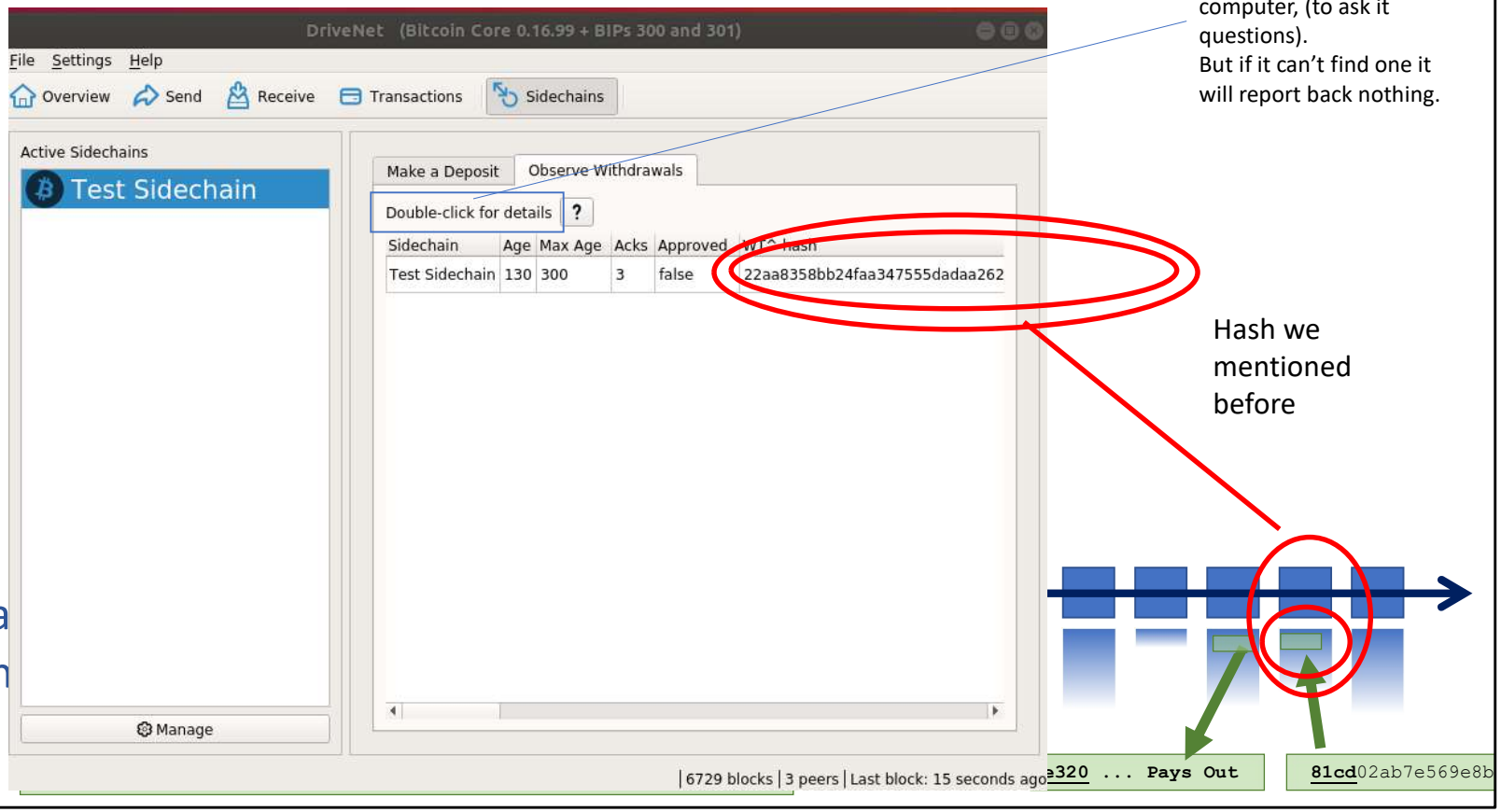
Your Layer 1 Node Sees…



Base La
(Bitcoin

Here is our software. –Just two more slides to finish this point, with a real-world example-- We are looking all the Bip300 withdrawals, there's only one right now. Which is this little row here.

Your Layer 1 Node Sees...



Now, the software says "double-click for details", up here. But for the purposes of this talk, that is misleading. Because what the "double-click" does, is try to find a sidechain node on your computer, with rpc-access, so that it can ask questions about the withdrawal. But if you don't have a sidechain full node (on this computer), then if you "double-click" it will just tell you that it knows absolutely nothing whatsoever. So, this little row here, is the entire Bip300 idea.

(#3) Improve Mining Incentives (Bip 301)

- Get all of the fees, on all of the chains!
- Miners can ignore Sidechain / Altcoin software.

Upon finding a sidechain block worth $2000...		
Item	Layer1 Miner ("Mary")	Sidechain User ("Simon")
Runs a sidechain node?	No	Yes
How much hashing?	100%	0%
Coins collected, on Layer2	$0	$2000
Coins paid out, on Layer1	$0	$1999
Coins rec'd, on Layer1	$1999	$0
d(Net Worth)	+$1999	+$1

Security Budget in the Long Run
14 Feb 2019 https://www.truthcoin.info/blog/security-budget/

Security Budget II, Low Fees, and Merged Mining
www. 15 Oct 2021 https://www.truthcoin.info/blog/security-budget-ii-mm/

4, 2021
coin
16

Okay third aspect. This one is only this one slide here. Third aspect is that we want to improve Mining Incentives (Bip301).

This is technically Bip301, now. I separated the two BIPs, to make them easier to read. But I think anyone with a brain who uses Bip300, would use Bip301 also – but you don't have to. Anyway, with Blind Merged Mining (BIP 301), *miners* don't need to pay attention to Sidechains, at all. So, layer1 *users* already weren't paying attention, now layer1 miners can also ignore Sidechains (if they want). They *still* collect all of the transaction fee-revenues from the sidechain's txn! How? Well, they contract with someone else who is running a sidechain full node, and the miner sells *them* the block- rights, basically.

(#3) Improve Mining Incentives (Bip 301)

- Get all of the fees, on all of the chains!
- Miners can ignore Sidechain / Altcoin software.

Upon finding a sidechain block worth $2000...		
Item	Layer1 Miner ("Mary")	Sidechain User ("Simon")
Runs a sidechain node?	No	Yes
How much hashing?	100%	0%
Coins collected, on Layer2	$0	$2000
Coins paid out, on Layer1	$0	$1999
Coins rec'd, on Layer1	$1999	$0
d(Net Worth)	+$1999	+$1

Crypto Fees

There's tons of crypto projects.
Which ones are people actually paying to use?

Layer 1 × | Share | Filters 1 | Yesterday

Name	▼ 1 Day Fees	7 Day Avg. Fees
Ethereum	$8,740,188.92	$7,864,461.27
Binance Smart Chain	$2,033,849.09	$1,643,743.19
Bitcoin	$1,970,350.71	$1,809,454.32
Dogecoin	$32,366.20	$24,394.61
Terra	$18,666.89	$19,434.10
Cardano	$14,645.96	$13,656.48
		$27,636.72

Security Budget in the Long Run

14 Feb 2019 https://www.truthcoin.info/blog/security-budget/

Security Budget II, Low Fees, and Merged Mining

www. 15 Oct 2021 https://www.truthcoin.info/blog/security-budget-ii-mm/

4, 2021

coin

17

Here's the important part – Miners don't run a sidechain node, but they still get all the money.

Therefore, if miners just do what they normally do, today, and include the txns which pay the highest total fees, then they will automatically mine all sidechain blocks and collect revenue from all the 5 sidechain transactions. Ultimately, I think this concept could boost fee-revenues by 1000x, if not much more. But I don't have time to tell you about it -- I did write two articles about "Security Budget" that you can look up if you want.

Something I want to mention, is that I gave this talk at Bitcoin2021 in June, using these little numbers over here; (on the right). And yesterday I updated the slide…

(#3) Improve Mining Incentives (Bip 301)

- Get all of the fees, on all of the chains!
- Miners ca

Item
Runs a sidechai
How much hash
Coins collected,
Coins paid out,
Coins rec'd, on
d(Net Worth)

Crypto Fees

There's tons of crypto projects.
Which ones are people actually paying to use?

Layer 1 × | Share | Bundle | Filters 1 | Yesterday

Name	▼ 1 Day Fees		7 Day Avg. Fees
Ethereum	$75,669	+846%	$74,428,911.16
Binance Smart Chain	$5,848	+216%	$5,198,367.48
Bitcoin	$1,035	-52%	$863,839.49
Avalanche	$105,316.62		$86,451.49
Fantom	$92,087.08		$92,517.89
Polygon	$65,296.89		$74,457.60
Terra	[illegible]		$14,118.19

November 4, 2021

Crypto Fees

There's tons of crypto projects.
Which ones are people actually paying to use?

Layer 1 × | Share | Filters 1 | Yesterday

Name	▼ 1 Day Fees	7 Day Avg. Fees
Ethereum	$8,740,188.92	$7,864,461.27
Binance Smart Chain	$2,033,849.09	$1,643,743.19
Bitcoin	$1,970,350.71	$1,809,454.32
Dogecoin	$32,366.20	$24,394.61
Terra	$18,666.89	$19,434.10
Cardano	$14,645.96	$13,656.48
xDai	$13,951.33	$27,636.72

Taken from https://cryptofees.info/ June 4, 2021

Telegram: t.me/DcInsiders Website: www.drivechain.info Paul's Twitter: @truthcoin

18

Bitcoin revenues are down, ETH revenues are way up.

Maybe that was unlucky timing, *shrug*. Just something to think about.

Outline

- Title / Summary (2)
- Bip300 -- Goal, Three Aspects (16)
- Outline (1) -- *YOU ARE HERE*
- Altcoins We Should Copy (15)
- The Supposed "Drawbacks" of Bip300 (2)
- Ending (1)

Telegram: t.me/DcInsiders Website: www.drivechain.info Paul's Twitter: @truthcoin

19

Ok, here's the rest of the talk. We already made it more than halfway thought. Now I'm going to talk about the Altcoins we should copy. Then I will discuss two supposed Drawbacks of Bip300. And then it'll be over.

What do we use BIP 300 for…?

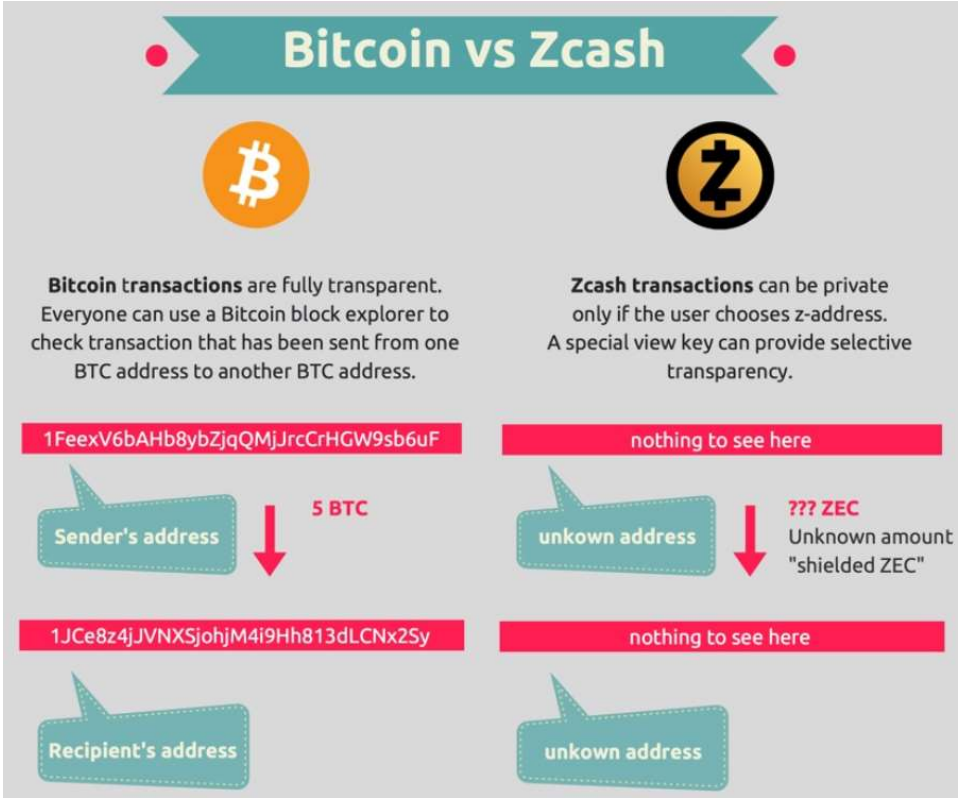
(In other words: Which altcoins are worth copying?)

Art: “When I paint my masterpiece” – Nick Kenrick (?) - Creative commons license

Ok, so we covered *the idea*. Now, the *concrete use-cases*.
Here are some Altcoins that I think we should consider ripping-off

Altcoins we should copy (?): zCash

Image from blockchainhub.net :
https://blockchainhub.net/blog/infographics/zcash-explained/



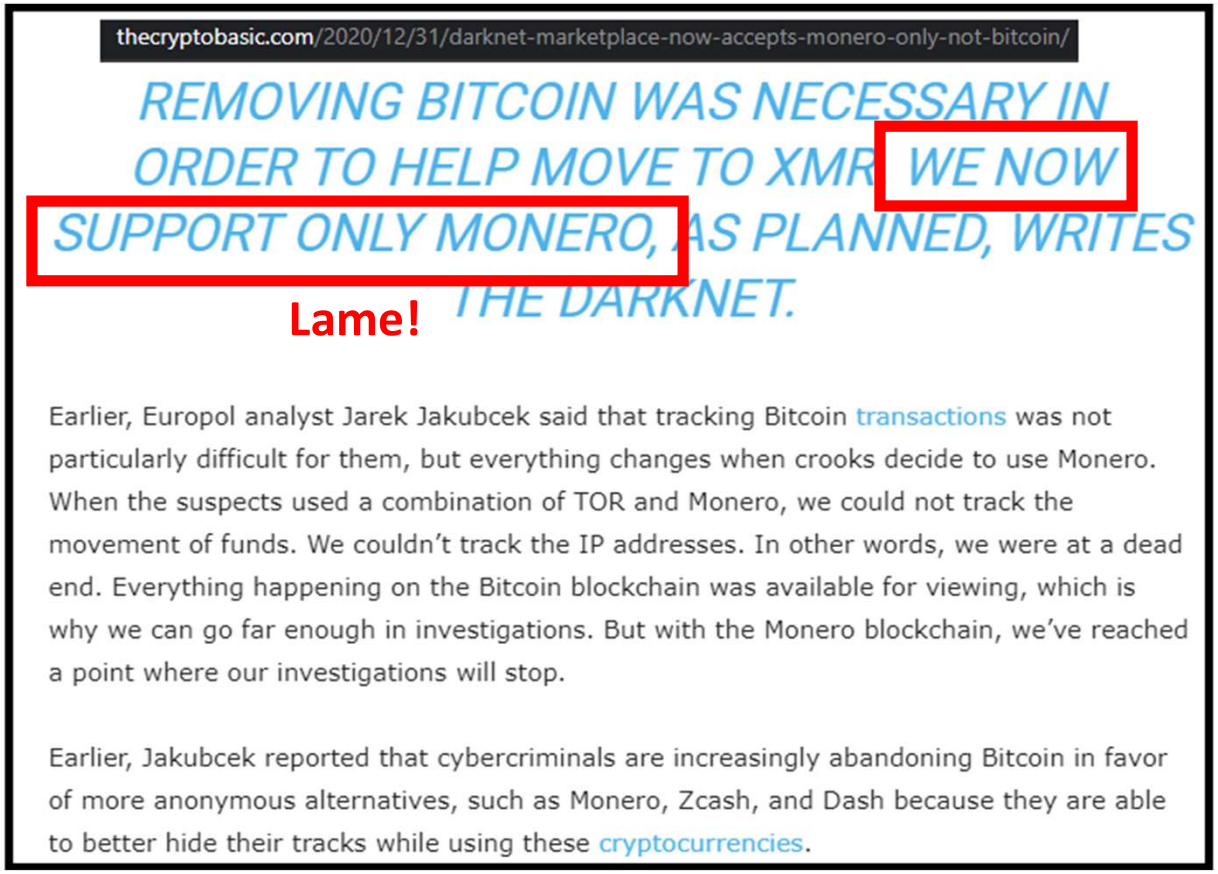
Telegram: t.me/DcInsiders Website: www.drivechain.info Paul's Twitter: @truthcoin

21

Obviously, zCash I mentioned at the beginning. ZCash has transactions where the sender, receiver, and the amount are all private. So then we Bitcoiners have to put up with comparisons like this. Where someone puts something up and says "Bitcoin vs Zcash". If we had Bip300, this infographic wouldn't make any sense at all. In fact all debates about one coin vs another coin would make no sense at all. Which brings me to my related point...

Losing Customers to Monero (?)

"White House Market" Retired (not exit scam) on Oct 4, 2021 [last month]



Telegram: t.me/DcInsiders Website: www.drivechain.info Paul's Twitter: @truthcoin

22

...there is a darknet market that, in Dec of last year, decided to *only* accept Monero. So that's kind of a slap to the face. If we had Bip300, then there would be no reason for them to accept Monero at all, let alone *exclusively*.

Altcoins we should copy (?): NameCoin

satoshi
Founder
Sr. Member
Activity: 364
Merit: 2754

Re: BitDNS and Generalizing Bitcoin
December 10, 2010, 05:29:28 PM
Merited by BitcoinFX (1), darosior (1)
#246

Piling every proof-of-work quorum system in the world into one dataset doesn't scale.

BitDNS users may not want to download everything the next several unrelated networks decide to pile in either.

The networks need to have separate fates. BitDNS users might be completely liberal about adding any large data features since relatively few domain registrars are needed, while Bitcoin users might get increasingly tyrannical about limiting the size of the chain so it's easy for lots of users and small devices.

Fears about securely buying domains with Bitcoins are a red herring. It's easy to trade Bitcoins for other non-repudiable commodities.

If you're still worried about it, it's cryptographically possible to make a risk free trade. The two parties would set up transactions on both sides such that when they both sign the transactions, the second signer's signature triggers the release of both. The second signer can't release one without releasing the other.

Re: BitDNS and Generalizing Bitcoin
December 10, 20
Merited by Aveatr

Quote from: Hal on De
additional block chain
on exchanges? These
purchase some kinds

satoshi
Founder
Sr. Member
Activity: 364
Merit: 2754

Right, the exchange

Re: BitDNS and Generalizing Bitcoin
December 09, 2010, 10:46:50 PM
Merited by ImHash (1)

Quote from: nanotube on December 09, 2010, 09:20:40 PM
seems that the miner would have to basically do "extra work". and if there's nc
(which of course, slows down the main bitcoin work), what would be a miner's
chains) ?

The incentive is to get the rewards from the extr side chains also fo

A longer interval than 10 minutes would be appropriate for BitDNS.

much easier if you can freely use all the space you need without worrying about paying
fees for expensive space in Bitcoin's chain. Some transactions:

Fun facts -- in this thread, Satoshi:
* Invents what is now known as Merged Mining.
* Assumes that there will be many separate blockchains that pay different fees (as if this were non-controversial!).
* The term “side chain” is used numerous times!

Telegram: t.me/DcInsiders Website: www.drivechain.info Paul’s Twitter: @truthcoin

23

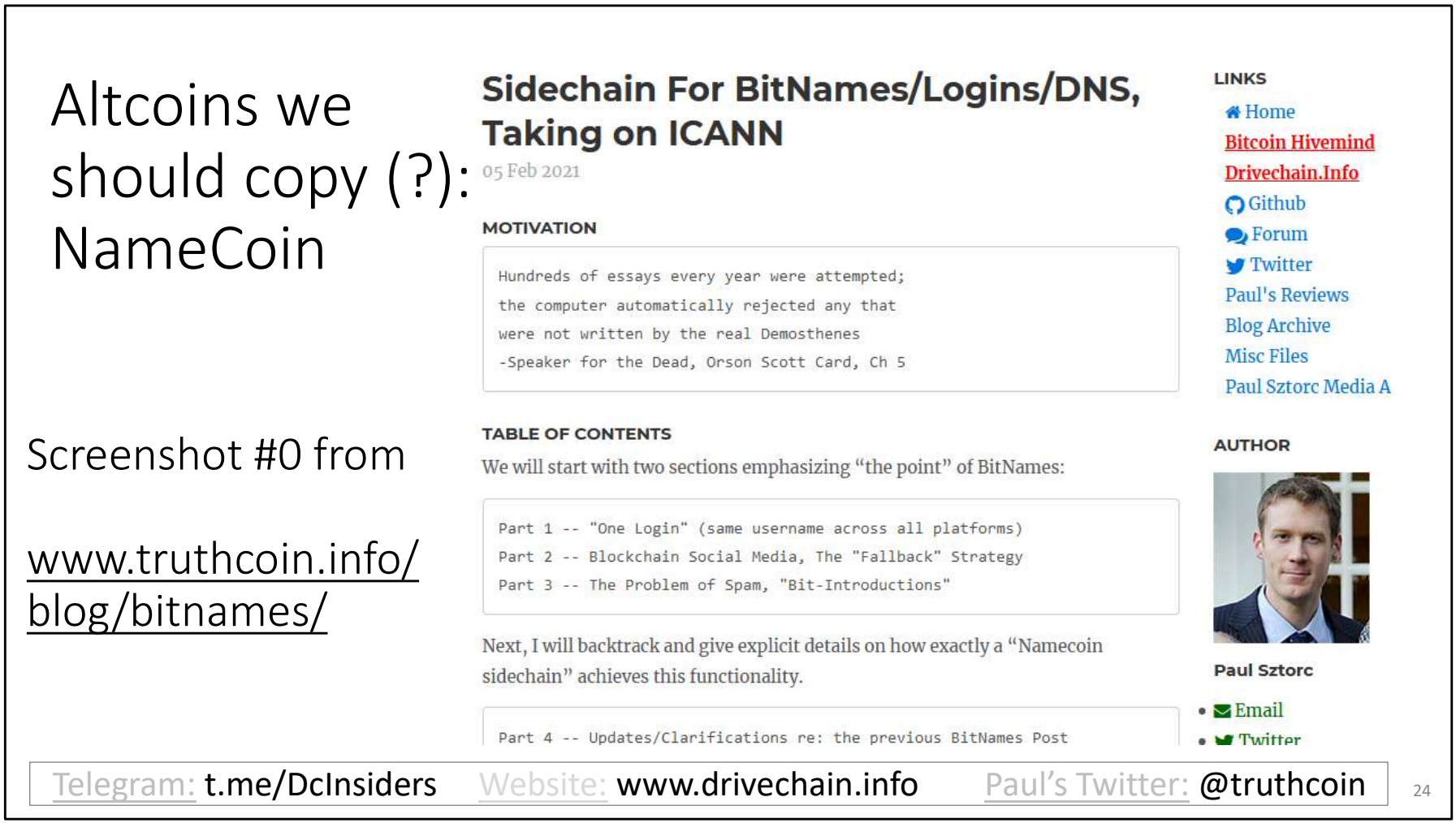
BitDNS was an idea proposed on bitcointalk, which later became the Altcoin Namecoin. This thread -where it’s proposed- is something that absolutely everyone should look up and read, if they have the time. Lots of cool history here. ... Satoshi invents Merged Mining, he coins the term “side chain”, he writes about how there will be lots of different chains, all back in 2010. It’s really cool.

Anyway, this concept, “BitDNS” is a weird idea, but I think it has tremendous potential. Again, I don’t have enough time to talk about it. But I did write a big article…

Altcoins we should copy (?): NameCoin

Screenshot #0 from

www.truthcoin.info/blog/bitnames/



Sidechain For BitNames/Logins/DNS, Taking on ICANN

05 Feb 2021

MOTIVATION

> Hundreds of essays every year were attempted;
> the computer automatically rejected any that
> were not written by the real Demosthenes
> -Speaker for the Dead, Orson Scott Card, Ch 5

TABLE OF CONTENTS

We will start with two sections emphasizing "the point" of BitNames:

```
Part 1 -- "One Login" (same username across all platforms)
Part 2 -- Blockchain Social Media, The "Fallback" Strategy
Part 3 -- The Problem of Spam, "Bit-Introductions"
```

Next, I will backtrack and give explicit details on how exactly a "Namecoin sidechain" achieves this functionality.

```
Part 4 -- Updates/Clarifications re: the previous BitNames Post
```

LINKS

- Home
- Bitcoin Hivemind
- Drivechain.Info
- Github
- Forum
- Twitter
- Paul's Reviews
- Blog Archive
- Misc Files
- Paul Sztorc Media A

AUTHOR

Paul Sztorc

- Email
- Twitter

Telegram: t.me/DcInsiders Website: www.drivechain.info Paul's Twitter: @truthcoin

24

…in Feburary –"BitNames, there's the url", and I will now give you a *FEW* of the images from that article. And you can read the article if you are interested.

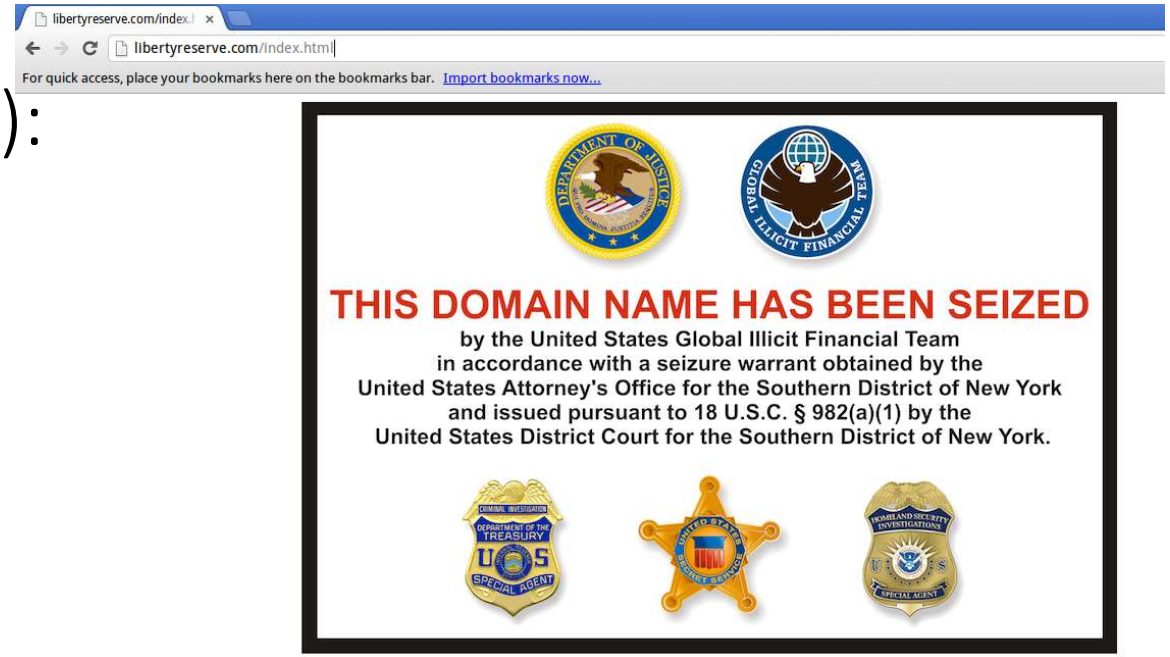
Altcoins we should copy (?): NameCoin

Screenshot #1 from

www.truthcoin.info/blog/bitnames/

…this is someone pretending to be Elon Musk, on Twitter…

Altcoins we should copy (?): NameCoin



Screenshot #2 from

www.truthcoin.info/blog/bitnames/

…this is the Liberty Reserve website domain_name being seized…

Altcoins we should copy (?): NameCoin

Screenshot #3 from

www.truthcoin.info/blog/bitnames/

…this is a guy on YouTube who, in the bottom-right, has to list out all of his screennames ... and they aren't all identical, his Facebook name is different.

With BitDNS everyone would just have one login, for every service. No one could seize your account, anywhere. And people would always be able to find you.

Altcoins we should copy (?): XCP / BitAssets / ERC20

Non-fungible token

From Wikipedia, the free encyclopedia

"NFT" redirects here. For other uses, see NFT (disambiguation).

This article **may contain wording that promotes the subject through exaggeration of unnoteworthy facts**. Please help improve it by removing or replacing such wording. *(May 2021) (Learn how and when to remove this template message)*

A **non-fungible token** (**NFT**) is a unit of data stored on a digital ledger, called a blockchain, that certifies a digital asset to be unique and therefore not interchangeable.[1] NFTs can be used to represent items such as photos, videos, audio, and other types of digital files. Access to any copy of the original file, however, is not restricted to the buyer of the NFT. While copies of these digital items are available for anyone to obtain, NFTs are tracked on blockchains to provide the owner with a proof of ownership that is separate from copyright.

In 2021, there has been increased interest in using NFTs. Blockchains like Ethereum, Flow, and Tezos have their own standards when it comes to supporting NFTs, but each works to ensure that the digital item represented is authentically one-of-a-kind. NFTs are now being used to commodify digital assets in art, music, sports, and other popular entertainment. Most NFTs are part of the Ethereum blockchain; however, other blockchains can implement their own versions of NFTs.[2] The NFT market value tripled in 2020, reaching more than $250 million.[3]

So lame!!

Contents [hide]

1 Description

Logo used to represen

Telegram: t.me/DcInsiders Website: www.drivechain.info Paul's Twitter: @truthcoin

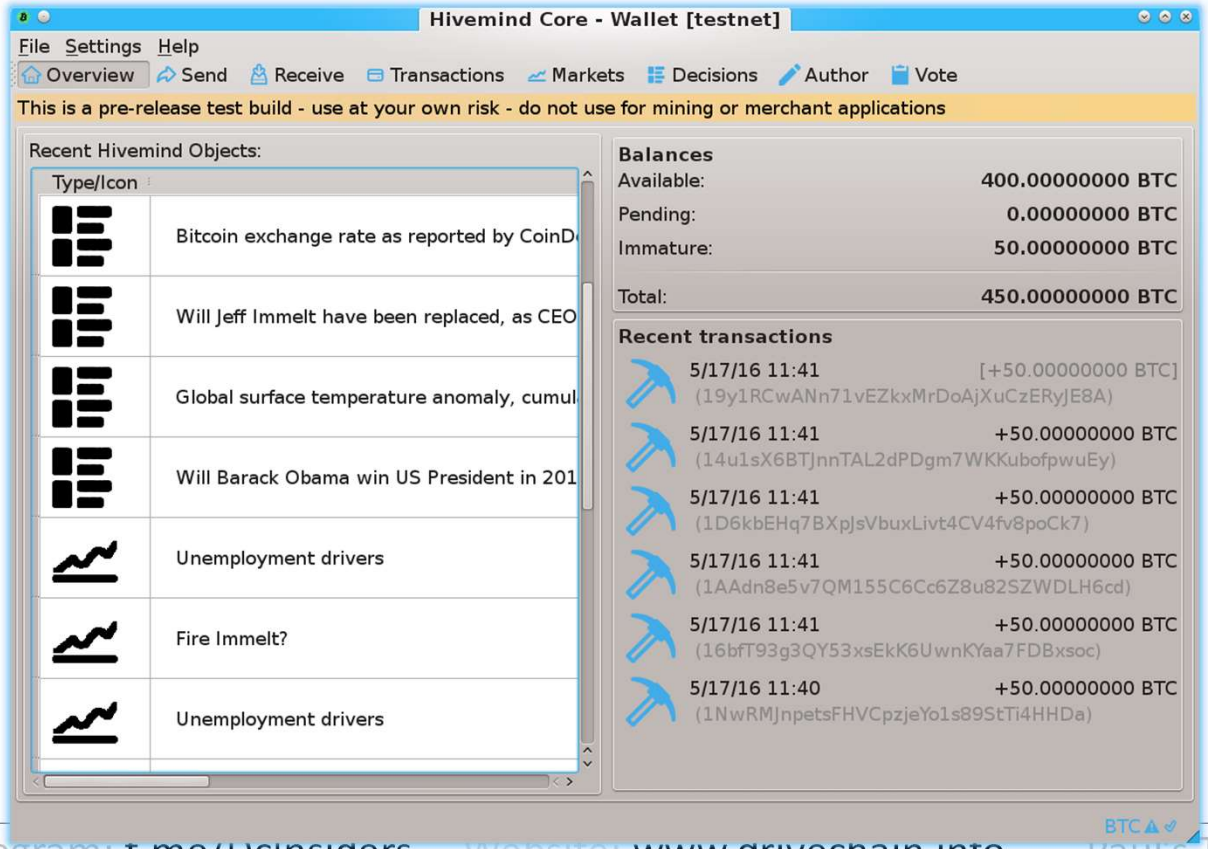
28

Ok lets talk about digital assets, now. Erc20/NFTs. They're basically digital baseball cards. Except they are unforgeable and indestructible, and unseizable. Anyways, a lot of people have fun collecting things. Most NFTs are on Ethereum, which is really lame. Because we Bitcoiners started all that, with counterparty and colored coins, etc. If we had Bip300, we could have a whole, special ERC20 chain or something. That would domesticate all of this energy in Bitcoin. Instead of having it compete against Bitcoin.

Prediction Markets

- Screenshots from my own BTC sidechain project

www.BitcoinHivemind.com



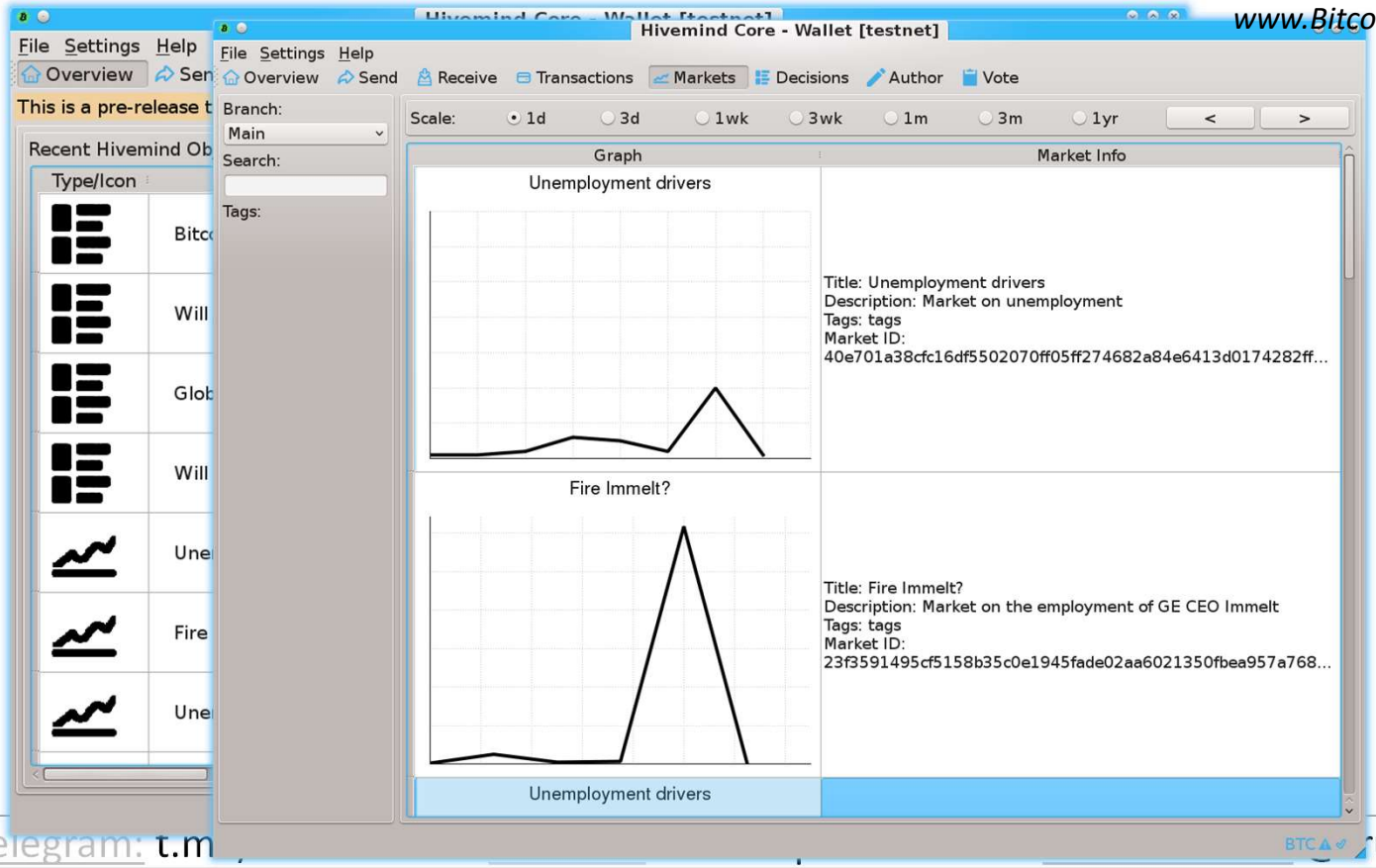
Telegram: t.me/DCinsiders Website: www.drivechain.info Paul's Twitter: @truthcoin

This is one of my other projects, BitcoinHivemind.com, check it out. I designed it to be a sidechain from the very beginning. Here are some screenshots…

Prediction Markets

- Screenshots from my own BTC sidechain project

www.BitcoinHivemind.com

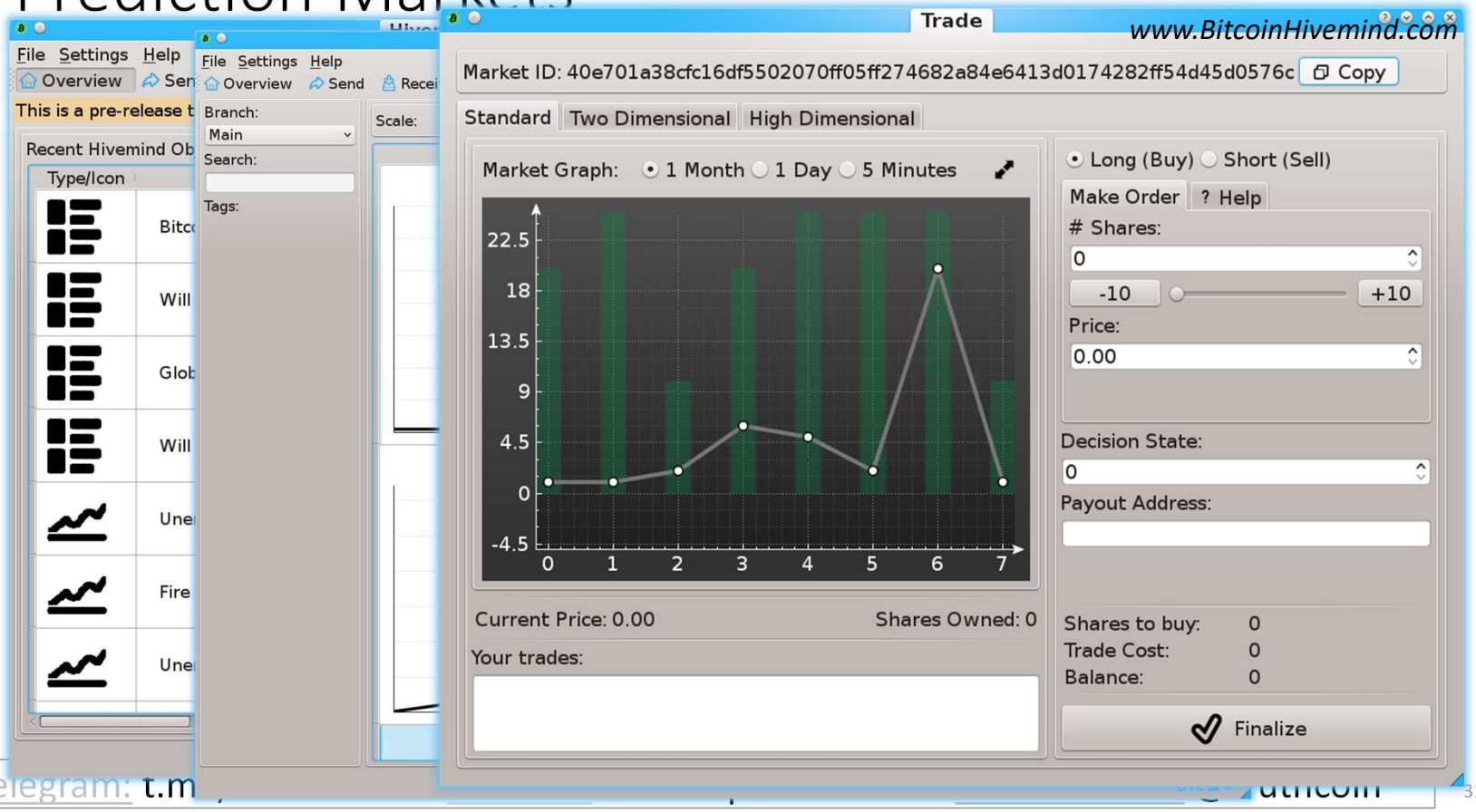


Telegram: t.m ruthcoin

...

Prediction Markets

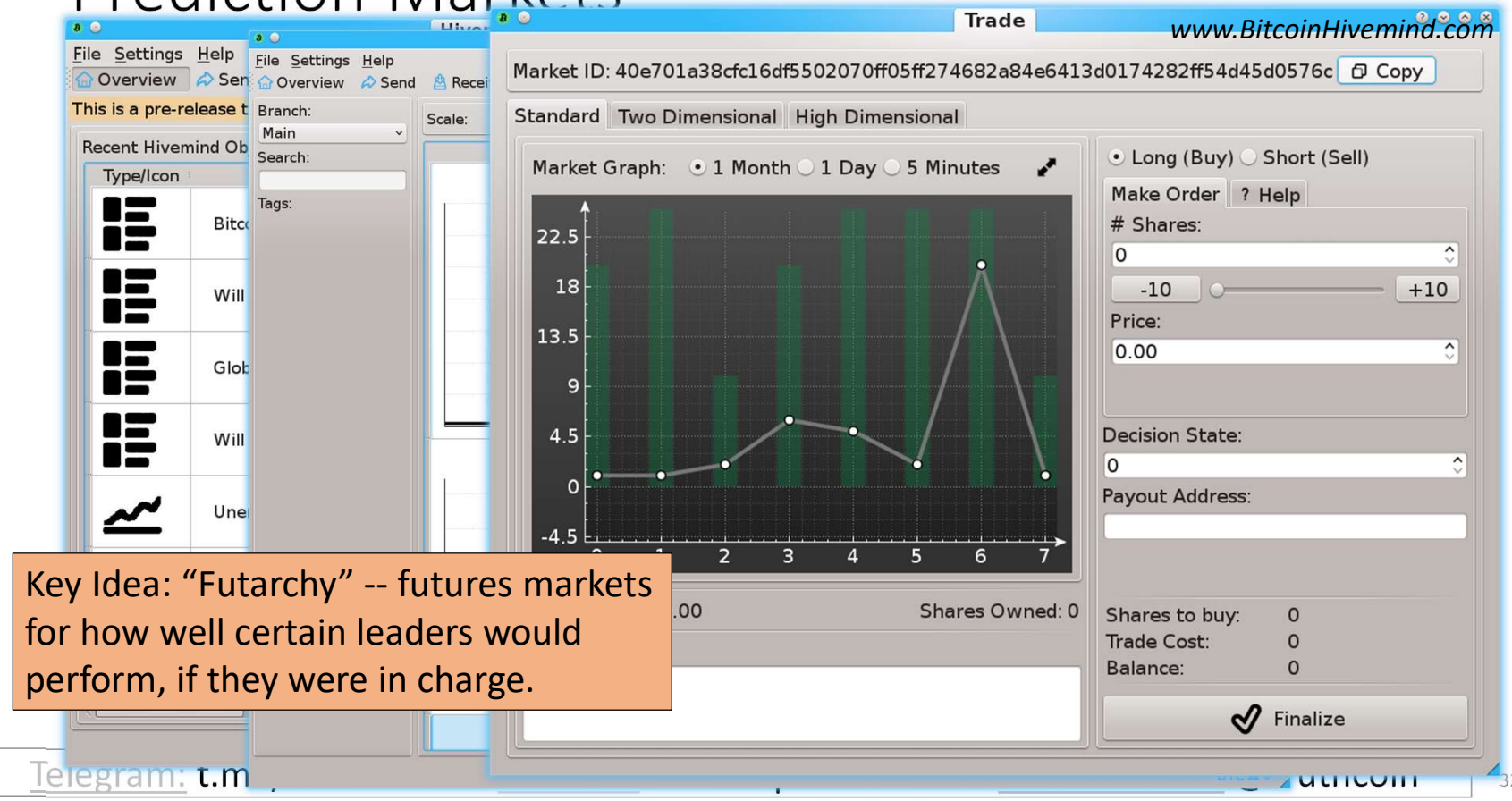
- Screenshots from my own BTC sidechain project



… This software can do a lot of things…

Prediction Markets

- Screenshots from my own BTC sidechain project

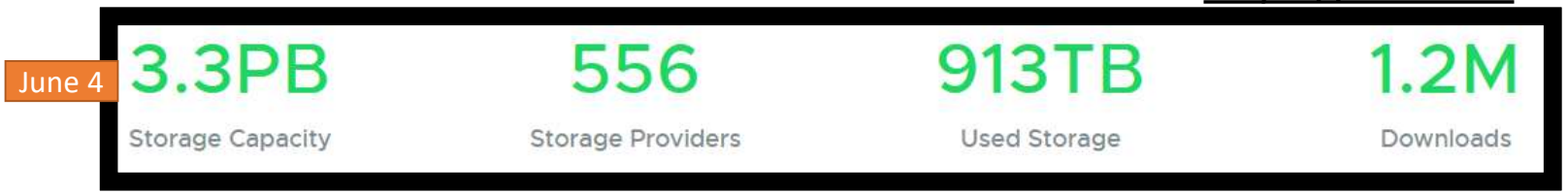


…but the crowd favorite is ‘Futarchy’ – where there are futures markets for how well certain leaders would perform, if they were in charge. ... This idea is very distressing to bad leaders, [laugh] , because *WE* can learn about exactly how bad *they* are going to be, *before* we cast a vote for anyone. I think that this is one of the most important ideas in the whole world.

Altcoins we should copy (?): Sia

- P2P Cloud Storage – Managed via Blockchain
- Running for 5 years
- No files ever lost?
- $1-2 per TB/month (vs $23 on Amazon S3)

https://sia.tech



Telegram: t.me/DcInsiders Website: www.drivechain.info Paul's Twitter: @truthcoin

33

This is Sia, which is David Vorick's project (who some of you may know). (Decentralized P2P cloud storage, managed and enforced by the blockchain). So, you have a hard drive at home, a lot of that space you aren't using. And you also have a bandwith connection at home, most of that bandwith you also aren't using. With this you rent it out. Sia has been running for 5 years, it's very decentralized – it would keep running if the dev team quit. He's got the costs down an order of magnitude below Amazon.

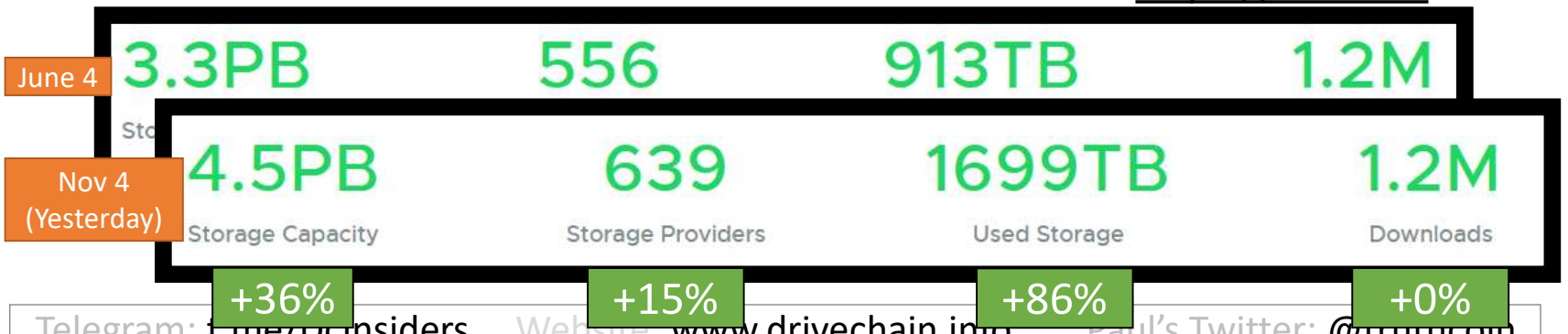
Using his Altcoin software – you can walk across a border, buy a new a blank computer, type in your 12 word seed phrase, and it will automatically download your entire filesystem (to that computer). It's really kind of cool.

Again, I gave this talk in June, 5 months ago. But I looked up the new numbers, yesterday…

Altcoins we should copy (?): Sia

- P2P Cloud Storage – Managed via Blockchain
- Running for 5 years
- No files ever lost?
- $1-2 per TB/month (vs $23 on Amazon S3)

https://sia.tech



Telegram: t.me/DCinsiders Website: www.drivechain.info Paul's Twitter: @truthcoin

34

...and here they are. They're up a lot.

Unfortunately, you don't often hear about projects like this, because *99+%* of Altcoins are scams, and it drowns out the useful projects. Which is sad. Yet another thing solved by Bip300, since no scammer would make a Bip300 sidechain.

Finally: How Bip300 Improves Layer1

1. Never Change Layer 1 Again
   – "Protocol Ossification"
   - No "drama".
   - No "mob rule".
2. Shrink Layer1 Blocksize.
   - Improves Decentralization.
   - Protects your node.

"Frozen Bitcoin" - Marco Verch , Creative Commons License

Telegram: t.me/DcInsiders Website: www.drivechain.info Paul's Twitter: @truthcoin

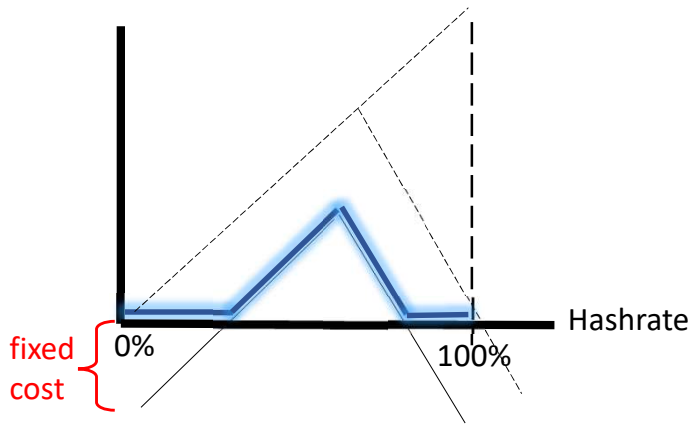
35

I will mention that, as an added bonus, if miners upgraded to activate Bips 300+301, then ---theoretically--- that might be the very last time anyone ever needs to upgrade their Bitcoin software again, ever. Which is more convenient, but also more secure as well. (If you're worrying about protecting Layer 1.)

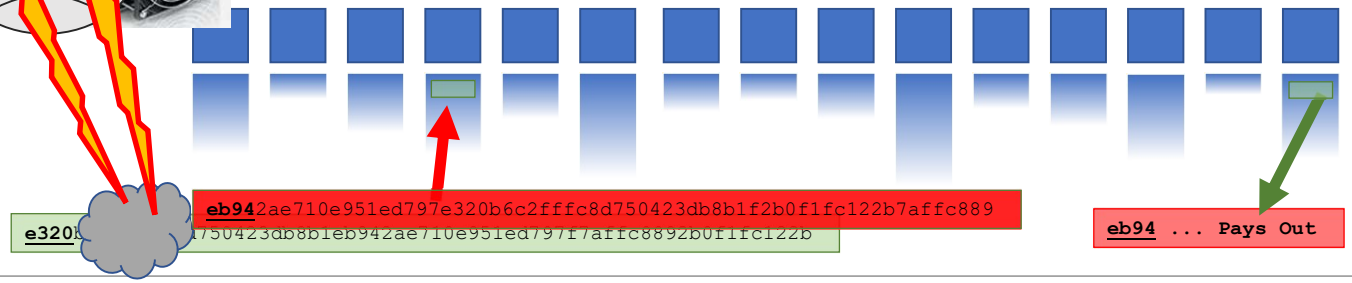
Furthermore, in my opinion, Bip300 is the only practical way of eventually forking the Layer1 Blocksize *down* to 350k, which I know at least some of claim to want. Because this would improve decentralization (as recommended by some experts, including Luke Dashjr). …

Two Supposed Drawbacks

(#1) **Miners-Can-Steal** from Bip300 Scripts
(and this is bad)



(#2) **Merged-Mining is a Side-Hustle**
(and those are bad)



Telegram: t.me/DcInsiders Website: www.drivechain.info Paul's Twitter: @truthcoin

36

… Ok now for those *drawbacks*.

Here they are. The first supposed drawback of Bip300, is that miners can ---with a little bit of setup and technical knowledge and effort on their part, and certainly patience--- miners can remove all the coins from a Bip300 sidechain, and pay those coins, to themselves. Hence it is called the "miners- can-steal" problem. Here you see an evil miner, replacing that one hash I mentioned before with a different hash, and then it eventually pays out (to the miner).

The second, supposed drawback of Bip300, *sigh* is: if some miners ever have a profitable side- hustle, then maybe some other miners might not be able to have that side hustle. And then they might go out of business; and wouldn't be able to buy as many Xmas presents for their children.

(#1) **Miners-Can-Steal** from Bip300 Scripts (and this is bad)	(#2) **Merged-Mining is a Side-Hustle** (and those are always bad)
The free market allows entrepreneurs to go bankrupt – this is **an essential part of creativity**. True: not every SC will succeed. But those few that do, will pay fees to miners and boost BTC's appeal (since BTC can now easily do everything). The failures will serve as a warning to lazy or incompetent developers.	The fixed cost in question… …is **zero** under BMM. …was already **microscopic**, vs other miner fixed costs. …**must always be small** enough for non-mining nodes to exist (since their revenue is the smallest of all, $0.)
Bip300 has multiple safeguards in place to make "stealing" difficult. Stealing requires **3-6 months** of openly dishonest mining activity. Humans can audit theft, by checking just 32 bytes.	Mining is a complex task involving many "sub-tasks" (getting cheap power / sourcing good ASICs / etc). Each has its own incentives, innovation, and fixed costs. **No stopping those.**
Miners "can" **steal from Lightning Network** (by broadcasting old state + censoring Justice Txns), but this criterion is never held against LN.	Bizarre implications: if BitFury sold t-shirts on the side, for profit, then **t-shirts = bad for BTC**. If Saylor altruistically paid miners $0.10 per year, then MS = bad for Bitcoin.
The user is **sovereign**. Users are **allowed** to sell their BTC for USD; or use BTC to buy "bad" products (ie "drugs"). Or invest in Alts / scams. Bip300 allows users to spend BTC to a script.	MM is the opposite of bad – it is good and necessary. MM alone can **boost BTC's fee revenues by 10,000x** or more. Without MM, long run hashrate may be too low.
This supposed "flaw" is actually a pro, as it gives miners motive and opportunity to **destroy "parasite sidechains"** (SC which antagonize other SCs). I am not aware of any other way of efficiently accomplishing this. And I believe it is prerequisite for high-quality smart contracts.	What is probably happening is that people are **confusing node costs** with **mining costs**. Node costs *must* be low, for decentralization. But mining costs have no such requirement. In fact, if we wanted mining costs to be low we could remove the upward difficulty adjustments.
The **whole point** of SCs is that Layer1 nodes ignore them. With federations, you trust a fixed committee of law-abiding people. With BIp300 you trust a decentralized P2P process.	MM is **already unblockable**. Satoshi invented MM in 2010, and envisioned many independent MM chains. We have been MM since 2011, with no end in sight.

Both of these are so, false, that its hard to know where to begin.

(#1) **Miners-Can-Steal** from Bip300 Scripts (and this is bad)	(#2) **Merged-Mining is a Side-Hustle** (and those are always bad)
The free market allows entrepreneurs to go bankrupt – this is **an essential part of creativity**. True: not every SC will succeed. But those few that do, will pay fees to miners and boost BTC's appeal (since BTC can now easily do everything). The failures will serve as a warning to lazy or incompetent developers.	The fixed cost in question… …is **zero** under BMM. …was already **microscopic**, vs other miner fixed costs. …**must always be small** enough for non-mining nodes to exist (since their revenue is the smallest of all, $0.)
Bip300 has multiple safeguards in place to make "stealing" difficult. Stealing requires **3-6 months** of openly dishonest mining activity. Humans can audit theft, by checking just 32 bytes.	Mining is a complex task involving many "sub-tasks" (getting cheap power / sourcing good ASICs / etc). Each has its own incentives, innovation, and fixed costs. **No stopping those.**
Miners "can" **steal from Lightning Network** (by broadcasting old state + censoring Justice Txns), but this criterion is never held against LN.	Bizarre implications: if BitFury sold t-shirts on the side, for profit, then **t-shirts = bad for BTC**. If Saylor altruistically paid miners $0.10 per year, then MS = bad for Bitcoin.
The user is **sovereign**. Users are **allowed** to sell their BTC for USD; or use BTC to buy "bad" products (ie "drugs"). Or invest in Alts / scams. Bip300 allows users to spend BTC to a script.	MM is the opposite of bad – it is good and necessary. MM alone can **boost BTC's fee revenues by 10,000x** or more. Without MM, long run hashrate may be too low.
This supposed "flaw" is actually a pro, as it gives miners motive and opportunity to **destroy "parasite sidechains"** (SC which antagonize other SCs). I am not aware of any other way of efficiently accomplishing this. And I believe it is prerequisite for high-quality smart contracts.	What is probably happening is that people are **confusing node costs** with **mining costs**. Node costs *must* be low, for decentralization. But mining costs have no such requirement. In fact, if we wanted mining costs to be low we could remove the upward difficulty adjustments.
The **whole point** of SCs is that Layer1 nodes ignore them. With federations, you trust a fixed committee of law-abiding people. With BIp300 you trust a decentralized P2P process.	MM is **already unblockable**. Satoshi invented MM in 2010, and envisioned many independent MM chains. We have been MM since 2011, with no end in sight.

So, Bip300 is designed, to prevent miners from stealing from sidechains. But, it is nonetheless possible. Similarly, – miners "can" (can in quotes **) steal from the LN. In fact its much easier for miners to steal from the LN, since Bip300 has this 6 month timeout period. So, were you worried about miners stealing from the lightning network a moment ago? If so, just cross off this entire left half of the page. I have to stress: this comparison isn't to knock the LN, I'm saying that the criterion is stupid. 51% hashrate can do a lot of horrible things, but that doesn't stop us from *allowing users* to opt-in to certain tradeoffs. After all, its Bitcoin not Prison.

(#1) **Miners-Can-Steal** from Bip300 Scripts (and this is bad)	(#2) **Merged-Mining is a Side-Hustle** (and those are always bad)
The free market allows entrepreneurs to go bankrupt – this is **an essential part of creativity**. True: not every SC will succeed. But those few that do, will pay fees to miners and boost BTC's appeal (since BTC can now easily do everything). The failures will serve as a warning to lazy or incompetent developers.	The fixed cost in question… …is **zero** under BMM. …was already **microscopic**, vs other miner fixed costs. …**must always be small** enough for non-mining nodes to exist (since their revenue is the smallest of all, $0.)
Bip300 has multiple safeguards in place to make "stealing" difficult. Stealing requires **3-6 months** of openly dishonest mining activity. Humans can audit theft, by checking just 32 bytes.	Mining is a complex task involving many "sub-tasks" (getting cheap power / sourcing good ASICs / etc). Each has its own incentives, innovation, and fixed costs. **No stopping those.**
Miners "can" **steal from Lightning Network** (by broadcasting old state + censoring Justice Txns), but this criterion is never held against LN.	Bizarre implications: if BitFury sold t-shirts on the side, for profit, then **t-shirts = bad for BTC**. If Saylor altruistically paid miners $0.10 per year, then MS = bad for Bitcoin.
The user is **sovereign**. Users are **allowed** to sell their BTC for USD; or use BTC to buy "bad" products (ie "drugs"). Or invest in Alts / scams. Bip300 allows users to spend BTC to a script.	MM is the opposite of bad – it is good and necessary. MM alone can **boost BTC's fee revenues by 10,000x** or more. Without MM, long run hashrate may be too low.
This supposed "flaw" is actually a pro, as it gives miners motive and opportunity to **destroy "parasite sidechains"** (SC which antagonize other SCs). I am not aware of any other way of efficiently accomplishing this. And I believe it is prerequisite for high-quality smart contracts.	What is probably happening is that people are **confusing node costs** with **mining costs**. Node costs *must* be low, for decentralization. But mining costs have no such requirement. In fact, if we wanted mining costs to be low we could remove the upward difficulty adjustments.
The **whole point** of SCs is that Layer1 nodes ignore them. With federations, you trust a fixed committee of law-abiding people. With BIp300 you trust a decentralized P2P process.	MM is **already unblockable**. Satoshi invented MM in 2010, and envisioned many independent MM chains. We have been MM since 2011, with no end in sight.

The second one is even sillier. I think what I would like to highlight is that the implications are ridiculous. So, if BitFury sold t-shirts on the side, for profit, then *t-shirts = bad for BTC*. They would be as bad for Bitcoin as Bip300 is, anyway. If Michal Saylor altruistically paid miners $0.10 per year, then MS = bad for 9 Bitcoin. Blah blah blah... I think what's really happening here, is that people are confusing nodes with miners. Miners run nodes, but not the other way around. We want nodes to be as cheap as possible. That is absolutely important; but we don't want mining to be as cheap as possible. If we wanted that, we could just get rid of all of the upward difficulty adjustments.

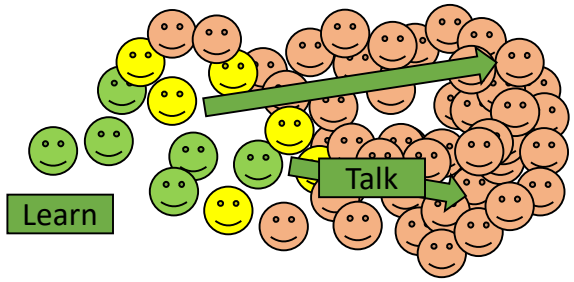
So I have total contempt for these two supposed drawbacks. In fact both of them are not drawbacks at all…

(#1) **Miners-Can-Steal** from Bip300 Scripts (and this is bad)	(#2) **Merged-Mining is a Side-Hustle** (and those are always bad)
The free market allows entrepreneurs to go bankrupt – this is **an essential part of creativity**. True: not every SC will succeed. But those few that do, will pay fees to miners and boost BTC's appeal (since BTC can now easily do everything). The failures will serve as a warning to lazy or incompetent developers.	The fixed cost in question… …is **zero** under BMM. …was already **microscopic**, vs other miner fixed costs. …**must always be small** enough for non-mining nodes to exist (since their revenue is the smallest of all, $0.)
Bip300 has multiple safeguards in place to make "stealing" difficult. Stealing requires **3-6 months** of openly dishonest mining activity. Humans can audit theft, by checking just 32 bytes.	Mining is a complex task involving many "sub-tasks" (getting cheap power / sourcing good ASICs / etc). Each has its own incentives, innovation, and fixed costs. **No stopping those.**
Miners "can" **steal from Lightning Network** (by broadcasting old state + censoring Justice Txns), but this criterion is never held against LN.	Bizarre implications: if BitFury sold t-shirts on the side, for profit, then **t-shirts = bad for BTC**. If Saylor altruistically paid miners $0.10 per year, then MS = bad for Bitcoin.
The user is **sovereign**. Users are **allowed** to sell their BTC for USD; or use BTC to buy "bad" products (ie "drugs"). Or invest in Alts / scams. Bip300 allows users to spend BTC to a script.	MM is the opposite of bad – it is good and necessary. MM alone can **boost BTC's fee revenues by 10,000x** or more. Without MM, long run hashrate may be too low.
This supposed "flaw" is actually a pro, as it gives miners motive and opportunity to **destroy "parasite sidechains"** (SC which antagonize other SCs). I am not aware of any other way of efficiently accomplishing this. And I believe it is prerequisite for high-quality smart contracts.	What is probably happening is that people are **confusing node costs** with **mining costs**. Node costs *must* be low, for decentralization. But mining costs have no such requirement. In fact, if we wanted mining costs to be low we could remove the upward difficulty adjustments.
The **whole point** of SCs is that Layer1 nodes ignore them. With federations, you trust a fixed committee of law-abiding people. With BIp300 you trust a decentralized P2P process.	MM is **already unblockable**. Satoshi invented MM in 2010, and envisioned many independent MM chains. We have been MM since 2011, with no end in sight.

… the left one allows for super-reliable oracle and high-quality smart contracts, and the right one is the only thing that is going to keep hashrate security up, in the future. So, they're not drawbacks at all, in fact they're both pretty cool; features.

Future of Bip300 – Depends on You!

1. Learn !
   - Download the software
   - Read drivechain.info
2. Talk
   - Soft forks need consensus
   - Invite on podcasts/whatever
3. View Altcoins Differently



drivechain.info/releases/
Drivechain = Bip 300+301

Releases

Download Latest Version (v40)

Software	Linux	Windows	Mac	Source
Mainchain v40.01	tar.gz	.exe	dmg, tar.gz	Github
Testchain v14	tar.gz	.exe	n/a	Github
Trainchain v77	tar.gz	.exe	n/a	Github
Thunder v5	tar.gz	.exe	n/a	Github
zSide v5	tar.gz	n/a	n/a	GitLab

Click here for CHECKSUMs

Telegram: t.me/DcInsiders Website: www.drivechain.info Paul's Twitter: @truthcoin

41

Ok, what should you do? Here is what I suggest: The most important thing is, to learn. The best way to learn, is to actually download the software and use it. Don't listen to what people say on Twitter. Run the testnet software yourself ... otherwise you know ... *nothing*.

Second: the Bitcoin community prides itself on consensus – we don't make a change, until lots of people agree that they want it. So: help spread the word. So, talk to your friends or whatever.

Finally, maybe (?) this might help – Change the way you view Altcoins. They aren't rivals, that are inherently evil; they're a place where technology is previewed, before it is copied into BTC.

Thank You

for Your Attention!

(Find me and talk to me!)

Telegram: t.me/DcInsiders Website: www.drivechain.info Paul's Twitter: @truthcoin

42

Ok that's the talk, thank you! :)

Frequently Asked Questions | Drivechain: Peer-to-Peer Bitcoin Sidechains

Updated March 2023

See also Drivechain Q&A by fiatjaf (creator of Nostr).

1. Security

How are drivechains secured?

Miners “farm” sidechains for their txn fees (and exchange-rate value-add). Why kill the “goose that lays the golden eggs”?

Well, it depends on:

How many eggs they lay

How much the dead goose is worth, and

How much effort it takes to actually kill the goose.

So, no two drivechains will have the same level of security.

Some will lay many “eggs”. These will have high fee-revenues, and/or will enhance the underlying coin-utility.

Similarly, some drivechains are more valuable to “kill” than others. The more coins on a drivechain, the higher the incentive to “kill” it (and take all those coins).

Finally, how to “kill” such a drivechain?

Because of the “slow return” feature of BIP300, it isn’t easy. Miners must 51% attack in a very transparent and obvious way, in full view of everyone, for a continuous 3-6 months, *before* the coins can be stolen.

The formal security model is here.

In general, Drivechain security is higher when:

The drivechain in question is popular with users.

There are many popular drivechains.

What if a sidechain isn’t popular?? Can miners “steal” from a sidechain?

An unpopular sidechain is one which:

Has low total txn fees, AND/OR

If the sidechain went away, the market price of Bitcoin would NOT fall significantly.

In such a case, Miners lose very little, economically, by taking the sidechain's coins. Especially if mining turnover is low (among pools/devices), and hashrate is stable.

Isn't that bad?

Not really.

We currently have ZERO sidechains. So even a 99.99% unpopularity rate (and a 100% failure rate of unpopular sidechains) would be an improvement over the status quo. At least we'd improve from 0% to 00.01%.

The risk-reward decision is one each user should make. Not you! If you don't like a particular sidechain, or sidechains in general, then don't use them! It's like that slogan: "If you don't Like Gay Marriage, don't get one!".

Users today sell their BTC for goods/services; for fiat; and for Alts. Why deny them the option to move their coins to a sidechain? They are the owner. Not you! Mind your own business!!

What negative impact could sidechains have on the mainchain (ie, Bitcoin Core)?

There are none, actually.

I looked into it in detail, in 2016.

Really?! What about miner incentives?

Sidechain merged-mining is a new revenue stream for miners, yes.

But Altcoin merged-mining has existed for years. It was invented by Satoshi in 2010. And has been in widespread use ever since.

All BIP300 does, is supercharge MM. With sidechains, miners would (hopefully) get huge revenues (and profits) from MM... instead of the pittance they get from MM today.

Are you sure that isn't bad?

Yes, I'm sure.

Profits are good for miners. And good for us. They increase Bitcoin's security budget. They increase the network Difficulty. They deter 51% attacks (by making them more expensive).

Mining has seen many “changes” that have increased profits:

Using ASICs, instead of CPUs

Using a pool whose software maximizes txn-fees (vs one that leaves this “free” money on the table)

Collecting natgas tax credits, while taking advantage of stranded energy

Negotiating lower-than-normal energy prices via a “demand response” contract

Merged mining is no different than those changes.

But this is a change that affects the protocol!

BIP300 affects the L1 Bitcoin protocol; the sidechains *themselves* do not.

The L1 protocol *never* behaves differently, based on something a sidechain does, ever. It only behaves differently based on what the BIP300 messages do. **All** BIP300 messages are included in the L1 blockchain – your node has to look at them anyway. Enforcing BIP300, does NOT mean downloading sidechain software, nor seeing sidechain blocks nor sidechain transactions.

Whether the *miners* download sidechain software, and collect coins over there... that’s *their* business, not yours. They already face this decision with merged-mined Altcoins. And they make it without any input from you! Mind your own business!

Are you absolutely sure about that? It sounds heretical.

Unfortunately, Blockstream’s paper mistakenly defined “mining centralization” as: “when any miner increases their profits”. (Read Section 4.3 and see for yourself.)

This mistake is the worst thing to happen to Bitcoin in its history. It led to years of irrational prejudice against merged mining. Years of “miner centralization bad” = “any increase in miner profits bad” = “miners collecting more txn fees sometimes, is bad”. Which is unfortunate because the opposite is true. Of course.

BIP300 forces miners to care about something new: maximizing sidechain utility, and sidechain txn fees. This is *good* for us – one more task that our mining servants perform, for us. And if they don’t perform –if they don’t work as hard as they possibly can, as hard as all their rivals at least– then they are fired.

Miners have to care about new stuff all the time (such as natural gas credits example, two answers ago). This is heathy and normal.

What is the correct definition of “mining centralization”, then?

If you ask me, the correct definition of "mining centralization" is: the cost of starting up a new, viable **mining pool**. Thus, we can increase decentralization by making it easy to pool hop, and making high-quality open source pool software widely availiable for free.

The centralization you should focus on, is CONOP centralization – the cost of starting up a new full node. CONOP centralization is the "real" form of centralization, and it is unaffected by the arrival of a new BIP300 sidechain. (There is a microscopic, fixed increase in CONOP, due to enforcement of the BIP300 rules, but by the time BIP300 activates, this increase will have been offset 1000x by everyday advances in computer power/cost.)

Your node only enforces the BIP300 rules on L1 messages; your node does not look at any L2 messages.

How are sidechains secure, if my L1 node isn't looking at them?

For block-finding, it is the same as merged mined Namecoin which has existed for years.

For the withdrawals – well, why wouldn't miners steal from them?

It would end the flow of sidechain txn fees.

It might negatively affect the price of Bitcoin.

The slow, rare nature of the BIP300 withdrawal makes it very easy for everyone to audit a theft. Even laypeople will know, with certainty, who is stealing from who. It's like shoplifting, but you are on national live television, and can only move in ultra-slow motion. The theft will be noticed, understood, communicated worldwide, and universally condemmed, several months before it can actually "go through".

More details are in the original 2015 post.

If withdrawals are so slow, won't users hate that?

No. Only specialists will use the BIP300 withdrawal. It can only pay out to 20,000 L1 destination UTXOs, anyway. So it is capped at 20,000 outputs per 3-6 months.

Everyone else will transact *with* those specialists. The specialists will be exchanges like Coinbase/Kraken/Sideshift, or they will be private users trustlessly swapping coins with HTLCs.

The specialist charges a fee, but users get to move their coins from L2 back to L1 immediately. The layperson customer never has to wait.

What if a sidechain becomes so successful, that it becomes the dominant chain?

Drivechain is asymmetric. The child sidechain is subordinate to the parent mainchain, always. If the

mainchain ceases to exist, then all child sidechains cease to exist as well.

Does Drivechain rely on a UASF to prevent sidechain theft?

No.

I will unpack this answer, in three sections.

(i) The UASF Can Do Anything (It Can Prevent Miner-Theft)

A UASF can block a sidechain-theft... but a different UASF can *force* a sc-theft to go through!

The UASF is flexible. Here are some possible UASFs:

Every coinbase after block #800,000 must contain the word “Hello”.

Block #888,888 must only contain TxIDs that start with an 8.

Block #1,000,000 must contain an OP RETURN gif of Napoleon Bonaparte dancing.

Starting block #925,000, every TxID that starts with 7, is banned.

Starting block #975,000, every TxID must start with 4, is banned.

The following Bip300 withdrawal TxID, is banned forever: “4h2f...”

The following Bip300 withdrawal TxID, MUST be included in block #950,000: “4h2f...”

You can even do all those, together. (In which case, the Napoleon gif will need to be one whose TxID starts with 4.)

Anyway, you can see that we can force any sc-theft to succeed via UASF, or fail.

Thus, it is **wrong** to imbue the UASF with an “anti-theft” feature. Inherently, it is neither pro-theft nor anti-theft. It allows users to clarify, VERY loudly, what they want to buy, when they hand over $186,000 USD (at 3/22/2023 prices) to miners in exchange for the newest 6.75 BTC (assuming +0.5 BTC of tx fees). UASFs have no inherent allegance to a consensus rule; nor any inherent hostility.

But, yes, a UASF can block a sc-theft.

(ii) UASF Drama?

But what is the effect on 3rd parties? Is there drama.

To explain this, we must explain the UASF in more detail.

First: what is this UASF?

Sidechain-theft can be blocked, with a UASF of the following form: prevent the upcoming theft-txn from entering the blockchain, ever. If it works, then their sidechain-coins are saved! If it doesn't work, then the UASFers lose nothing – they're in the same position they're in now. That is what the victims will try.

Second, this "withdrawal dispute" UASF has unusual properties:

No code changes are needed. No code needs to be written, nor reviewed nor bike-shedded. No software needs to be downloaded, etc. Miners have already chosen the TxID they will steal with, and everyone knows what it is – thus, the UASFers need only select it, and ban it. It is a simple point-and-click.

While the UASFers are *immediately* alerted to the problem, their UASF cannot take place *until later* – until *after* the theft-txn has accumulated its required 13,150 ACKs. Thus, the actual USAF is planned "today", but it cannot actually happen until "3-6 months from now".

There is no need for the UASFers to choose an exact time of their fork. Nor do they need to specify activation, nor signal to each other. The fork event is tied to "the inclusion of the theft-txn" in a L1 block. So, no coordination is needed among UASFers. They can successfully pull the whole thing off, even if they never speak to each other.

Third, let's imagine that a theft is attempted, users counter with a UASF, and the miners don't back down. On the day of the theft, the coin splits into two. What happens now?

Well, one coin will have a higher market price than the other.

The miner-thieves hope that their coin is the higher-priced. If so, they will happily mine the more-valuable chain. 100% of the hashrate will mine the more profitable coin, even miners who were personally against the theft *or miners who prefer to own the UASF coin*. This is a crucial point, see "if a miner would rather hold B2X, they could earn it four times faster by mining B1X and trading it for B2X", for the explanation in the context of SegWit2x. Thus, the UASFers will be on a stalled chain, with 0% hashrate. They may see a few altrustically mined blocks, but it will not be enough. The UASFers have lost, and they stay on a stalled chain, individually, until each admits defeat. They must "unblock" the TxID of the theft txn, and allow it.

In this case, all neutral people will be on the longest-hashrate chain, the whole time – they will not even notice that anything has happened. So they are unaffected by the failed UASF.

But what if the UASF succeeds? If the UASF-coin has the higher price, miners will be forced to mine it (by the exact same logic as before.) The network will remain one blockchain (or re-fuse into one blockchain). It will be a chain where the theft-txn *did* get all 13,150+ ACKs, and it *could* be included in a block, but it never is (eventually the 26,000 BIP300 window expires, and the theft-txn with it). The

UASFers win; the miners fail to steal.

But what of the neutral parties? If the price differential is large, then the network will never actually split (this happened with SegWit2x – "fork futures" warned us in advance which chain would die, and it was never born). If the price-differential is tiny (ie, market is mostly indifferent – this is pretty unlikely), then both chains may live for a short time. The networks have identical protocol rules, so every txn broadcast during this time will be included in both chains. (In other words, there would be full transaction replay; unlike in the BCH case where there was the exact opposte: mandatory full replay protection.) Any malicious double-spenders, can be defeated by via recipient asking for txn confirmation on *both* chains, before considering a payment finalized (it is not possible for a layperson user to "accidentally" double-spend, in this case). Ultimately, one chain wins and the other dies – it is as if they own a DropBox folder that splits into two identical dropbox folders and then collapses back into one.

In the very worst case (and unlikely) scenario, there is a reorg that affects some transactions. This requires the market to be somehow "undecided" up until (and during) the fork, and then to decide to be anti-UASF for a little while, and then change its mind. It is a pretty far-fetched scenario. More likely, fork futures will warn us in advance, which coin will be worth more.

(iii) In Context

Any group of people, can decide to UASF, at any time, for any reason. (Such as the dancing Napoleon gif reason.) Drivechain *might* create "theft events", which attract UASF attention, but probably not. And what of all the UASFs that DC prevents? For example, DC (if popular) removes the need for all future soft and hard forks. On net, drama on L1 would plummet due to Drivechain.

Also, reorganizations –while unfortunate– are already an inherent risk of using Bitcoin. Each user can voluntarily mitigate this risk, in the usual way (waiting for more confirmations). Drivechain should only be blamed for any new risks it might introduce – not risks that already exist!

What does DC "Rely" On, if not UASFs?

If you go here, you see that DC relies on:

The m parameter (sidechain-able BTC being worth more, than mono-chain BTC)

The b parameter (the fee-revenues from the sidechains).

Why does drivechain allow miners to deny the creation of a given sidechain? Are you against permissionless innovation? Are you a BitMain shill??

Miners will add a sidechain if it makes money to do so.

Also, Miners will remove a sidechain, if it makes money to do so.

Miners earn more, by removing a sidechain?! How could that happen??

If one sidechain prevents a 2nd from reaching its full potential, then the 1st sidechain is a troublemaker. It should be gotten rid of, the same way that security guards keep out thieves.

See my "Smart Contract Ecology" presentation (or answer below for more details.

This is actually why a sidechain-system is superior to one single general purpose blockchain (as in Ethereum).

In the security model you mention "sounding the alarm", where users and miners warn other users and miners. Isn't this centralization / collusion?

One reddit user writes: "Drivechains have 1008-block cycles ostensibly to protect against theft, so that someone can 'raise the alarm' and tell miners to downvote a particular theft withdrawal, but that sounds too much like centralized collusion to me."

While this is collaboration, it is not centralization. Drivechain is designed so that everyone can **independently** respond to the alarm by doing the right thing. They do not need to coordinate with a leader, or a large miner or other users, or anything else. They simply know what to do, because, by design, it is very easy for them to learn what to do. In this case the design is much better than, the March 2013 consensus failure emergency. A drivechain theft would be exactly like that event (in which everything worked out just fine), except that it would be much *better*, because **everyone** would: [1] have plenty of warning, and time to respond (two months or so), and [2] would already know what to do (either downvote everything, or manually upvote the winner, both will work).

Why can there be only 256 sidechains? Won't we run out?? There are 600,000 Altcoins on coinmarketcap!

256 is the right number. The people who disagree, fail to grasp the following facts:

We can have sidechains *of sidechains*, so the true number is unlimited.

By limiting the number to 256, we can id a sidechain using just one byte. Any more would require two bytes, and allow us to count to 65,000+ which is overkill.

The "600,000 Altcoins on coinmarketcap" represent only ~40 novel ideas. The other 599,960 coins are just a carbon-copy of one of the 40, with a different name. The name is the only new thing.

Many of those ideas are novel consensus mechanisms.

They replace proof-of-work with something else. (This is near-certain to fail.)

They try to solve a problem that has already been solved by Merged-mining. So they add no value to a merged-mined Bitcoin sidechain.

If necessary, we could just add a second BIP300, "BIP300b", that adds 256 more slots.

2. Comparisons

How does this proposal compare to the proposal in the Oct 2014 paper "Enabling Blockchain Innovations with Pegged Sidechains"**?**

Only in Appendix B is there a concrete suggestion. It was never implemented in the real world, and in the paper it is immediately qualified with the sentence "A detailed analysis of this problem and its possible solutions is out of scope for this document".

Nonetheless we can compare.

In Drivechain it is impossible to conduct a surprise attack, impossible to harass the community writ large with many withdrawal attempts (ie a "mosquito strategy"), and very easy for users to understand that the attack is happening, long before it actually happens. Also, each attempt is very simple, one question of 'Endorse'/'Reject' – quite comparable to the the March 2013 anti-consensus event.

A slow transparent process means that it is impossible for miners to attack the chain and claim that they didn't know that they were doing so – with transparency, everyone knows, observers as well as the miners themselves. So it is a clearer demonstration of malice.

Blockstream's skiplist proof is "in the tens of kilobytes range". DC requires first an M3 message, and next many M4 messages. Roughly 1 marginal byte per sidechain per block. Over 13,150 blocks, this is 13.150 KB per sidechain of course. So Drivechain's size is slightly smaller.

What is the difference between drivechain and extension blocks?

Both approaches attempt to solve the problem of extensibility – "extending" the capabilities of Bitcoin beyond those which currently exist.

This extensibility problem is a difficult one to solve, because of Bitcoin's unique emphasis on "consensus" – that all users agree on the state of the blockchain. Since all users must agree, and agreement isn't free, there is also an implicit agreement on a "minimum required effort" or "minimum tolerable workload". Bitcoin plays by certain rules, and if those rules are to be meaningful they must be enforced as-written.

So we have a situation where [1] the rules (including "required effort" rules) must be enforced, but

simultaneously one where [2] users might like to experiment with new rules. In short, we want the benefits of a "hard fork" (and of permissionless innovation) without paying the costs (which are a loss of consensus, or non-enforcement of important rules).

The trick is to try and solve both problems at once. A 'hard fork' solves only problem [2], and 'doing nothing' solves only problem [1]. Extension blocks make some progress toward solving problem [2], at the expense of tremendous sacrifice on [1]. This is because users of the non-extended original chain, are subject to a potential barrage of messages. These messages can be sent at any time, by anyone (including an attacker), and could take on any properties (large in size, difficult to process, slow to validate)...most important of all, invalid messages can be sent for free. In this scenario, the cost of maintaining consensus over "Original" is in great danger (according to some) of rising to "Original" + "Extension", anyway. This means that the extension block is effectively a hard fork, and we have failed to solve challenge [1].

Instead, Drivechain condenses the from-extension-to-original messages into infrequent, easy to validate, unambiguous, chain-scale messages. It essentially flips the consensus threat on its head by arguing that the sidechain should do all of the consensus labor, and it should then present a tiny, minimal easy-to-verify proof of that labor to the mainchain at infrequent intervals. (In the sense of being "difficult to generate but easy to verify", it resembles proof-of-work itself.) This allows us to solve problem [2] without compromising on [1].

This is why Adam Back in particular emphasizes the "slow return" feature of Drivechain, whenever possible (recall that Dr. Back was a major innovator and promoter of extension blocks in early 2014).

What about Zmn..'s Sidechain-Headers-on-Mainchain (SHoM) **?**

Again, to repeat the answer for extension blocks (above), **the distinction between hard and soft forks isn't the point**.

The point is, instead, **the** burden **placed on existing users**. While an extension block does allow 'oldtype nodes' to ignore the extension data, it does this at a cost of no longer being able to fully-validate the block. It is a 'backdoor hardfork', of a kind, because users need to upgrade.

Imagine five different scenarios:

Hard Fork to a 2.2 MB

Evil fork to a 2.2 MB

Extension Block adding +1.2 MB

Segwit ExtBlock adding +1.2 MB

Drivechain adding +1.2 MB

Keep in mind that, in order to use Bitcoin as money, every user must check every txn for double-spending. Therefore, if we narrowly assess each of these scenarios in terms of "the burden they place on existing users", we get the following:

A hard fork is bad, because old users must upgrade, and track 1.2 more data.

An evil fork is bad, because old users must upgrade, and track 1.2 more data.

An extension blocks soft fork is bad, because while old users don't need to upgrade yet, they might need to have done so at any time.

A SegWit extension block soft fork was bad, for the exact same reasons (immediately above).

A drivechain is good, because it does not force you to upgrade; and if you need to upgrade you will be given plenty of warning, and ultimately even if none of the upgraded / non-upgraded people agree there are no consensus failures on the mainchain.

In my view, SHoM is too similar to an extension block. And it therefore lacks drivechain's most important features.

What about NiPoPoW by A. Kiayias and D. Zindros ?

I tweeted my thoughts on this article. I am happy that the authors worked on this, but I do not think that I can use it for anything.

What about ZK Validity Rollups?

Rollups pack a list of txns into a smaller amount of L1 space. Thus, they are a perfectly legitimate L2.

They have several drawbacks when compared to drivechain.

First: the benefits of rollups are much lower.

Rollup's increase in onboarding capacity is capped. See an example of capped-ness here:

```
The onchain transactions needed to open and settle (and
occasionally rebalance) self-custodial Lightning channels
take up a measureable amount of limited bitcoin block space.
This block space footprint results in a hard upper limit
on the number of self-custodial users who can be onboarded
to Lightning in a given period of time. The additional
transaction capacity enabled by validity rollups could
be used to support more Lightning transactions ...
For 2-P2WPKH-input-1-P2WSH-output-2-P2WPKH-output
```

```
dual-funded channels, rollups can create room for up to
3.8x more Lightning channel open transactions.
```

In contrast, in Drivechain the onboarding growth factor is not limited to 3.8 – instead it is unlimited.

If rollups use an account model (vs utxo), their growth factor may be 10x or 100x more (ie, it may be 38x or 380x). But I have yet to see anyone describe, design, or code this.

Furthermore, rollups do not have as much flexibility as sidechains. (Sidechains have unlimited flexibility – everything in a rollup must in principle be *writeable* to L1, whereas sidechains are the reverse: everything experienced on the sidechain must be in principle *ignorable* on L1.)

Second, rollups require a big change to L1: L1 must validate zk-snarks. Bip300 is just an integer that counts from 1 to 13,150, which is something that anyone can understand and audit. Zk-stuff is rightly called "spooky moon math" and most experts are (or were) confounded by it (see here and here). The average person has zero chance of ever grasping the difference between a zk-proof system that is *pretending to work* (vs one that is working genuinely). You might say: so much the worse, for the average person! Rightly so, but "most L1 node runners" also have zero chance of understanding or auditing these systems. Nor does the economic center of gravity of the Bitcoin system. In contrast, things like hash functions and signatures are simple operations that a user can perform for themselves, many times – thus they can learn the basics and "audit" their computer.

Third, rollups do nothing to solve the "data availability problem". Drivechain does not solve it either... but Drivechain is at least designed with this DA failure mode in mind. To marginally address DA, Drivechain rewards L1 miners with txn fees (via merged mining); and rewards L2 users (via useful services). Rollups are often presented as though they are impervious to failure. But really: DA is where the rubber meets the road, and rollups do nothing about this big problem.

Fourth, despite the above limitations, the main "advantage" that rollups have over DC, is very very small. The advantage is: the supposed benefit that "51% miners cannot steal from" rollups. Firstly, this comparison is weak, because in DC an actual theft requires 6 months of open, easily-demonstrated misbehavior. So DC theft is enormously impractical – like robbing Fort Knox in slow motion. Secondly, in the rollup case, if evil miners are determined to steal (from rollups), then they can also spend six months doing something comparable: refuse to allow the L1 zk-snark message into the L1 blockchain. This holds the rollup funds hostage – miners can refuse to allow rollup-withdrawals, unless desperate users sell their coins to the miners for pennies on the dollar. If miners start this on Jan 1, likely that many users will have given up by July 1. So the main advantage rollups have over DC is not significant.

Fifth, the "advantage" in point four is (yet again) just a misunderstanding of the DC "miners can steal" problem. "Miners can steal" is not a bug, it is a feature (for DC). See the long presentation on

"Sidechain Privatization", if you want to be one of the very few people who understand why. Not that it matters much in this case, since rollups are also not flexible or general purpose enough to cause too much inter-chain damage.

3. Usefulness

How can we ensure that Great Altcoins are transformed into Sidechains?

If Altcoins are useful, they should have fee-paying users. Therefore, miners should want to claim these fees.

Why would anyone make a sidechain, when instead they could make a great ICO Scam and/or Altcoin?

It doesn't matter.

If they make an Altcoin, and the Altcoin is useful, then we will copy that Altcoin into a sidechain (as we have already done for zCash and Ethereum). This is easy to do.

If they don't make the Altcoin; or they do make it and it isn't useful, then we won't copy it.

People buy Altcoins to make money! Not for their features, Paul! How could you make such a silly mistake?

Darknet markets have switch from BTC only, to XMR only. Since no one holds the coin (the buyer, the seller, nor the DNM), this cannot be related to the coin's exchange rate. It can only be related to the XMR superior privacy feature.

But sure, if people only want to buy/flip/pump crypto-assets, then they can continue to do that, on the BitAssets sidechain.

Two sociopaths can't pump-and-dump each other. It requires at least one guillible victim. In Alt-land the guillible victim is always told **a story** that involves the coin's distinctive features. With sidechains, we can copy these features. We get the utility, AND we disable the "story". So, sidechains help in either case.

With respect to a "LargeBlock sidechain" specifically ...

...why should I need to xfer my UTXOs from main-to-side at all? That's inconvenient – with a hard fork, they just show up there.

Sidechains are "opt in". So if you want to use the new feature, you must "opt in" to it.

...will the "SmallBlock mainchain" even have enough tx-bandwidth for all of our [LargeBlocker] coins to escape?

A wealthy Bitcoiner could deposit *many coins* into the sidechain in a single transaction.

He can then onboard new users over there, without consuming any marginal L1 bytes.

So sidechains can grow in all the ways that Altcoins can grow.

4. Abilities and Limitations

Can we have a sidechain that uses Proof of Stake?

Yes, we could. The concept of the 1st sidechain BIP, hashrate escrows is flexible enough to copy *any* blockchain – public or private, proof-of-stake, proof-of-space, proof-of-steak, etc. Even weirdo stuff like Corda.

However, Drivechain ships with a specialized, customized feature called 'blind merged mining' (BMM), which makes consensus on the sidechain *free*. As in, free in both the economic and engineering sense (see below). If a chain uses BMM, it freely inherits all of Bitcoin's proof of work security. In fact, the sidechain gets all of Bitcoin's security, even if its transaction fees [or its other miner-revenue-sources] fall to zero.

For those reasons, BMM is the recommended consensus algorithm for Bitcoin drivechains.

(...perhaps we should invent some sexy-sounding "proof-of-X" name for BMM, like "Proof of Merge"? And bundle it with ridiculous-sounding (but technically true) claims like "even more efficient than PoS".)

How is Blind Merged Mining doing achieving consensus for free (above)?

The original specification is here, and the BIP text is here. I would first look at the table in the beginning of the BIP text.

BMM only allows one side:block to be found per main:block. This side:block hash must be inserted into "critical real estate" in the L1 coinbase. L1 miners "auction off" this real estate, to the highest bidder.

Here is a more detailed explanation.

Can Bitcoin L1 switch to Blind Merged Mining?

No. The BMM trick requires a "regular" PoW blockchain to exist. It can't work all by itself.

All the money earned by all sidechains will ultimately go to mainchain Bitcoin miners, so, economically, it really is as if miners were actually mining several chains at once. Except, in this case they only need to run a Bitcoin node.

If Simon keeps a cut, then who would ever use BMM? Why allow Simon to keep a cut, when Mary can run a full node and collect 100%

The full node might be expensive to run.

For example, a node costs $20 to run (amortized over 10 minute periods) and fees are $100 (also amortized over 10 minutes), then Simon can BMM and pay $81 to choose the next sidechain block. Mary won't run her own node.

So, Simon's cut actually helps Mary make *even more money* than she would have made otherwise. It isn't a disadvantage at all.

The equilibrium value of the cut is near zero. *Every* sidechain user is already running a side:node. So it is a sunk cost. Paying $81 to earn $100, is always profitable. It doesn't matter that the node cost $20. Paying $82 to win $100, is more profitable than losing the bid (where you pay nothing to earn nothing). So the equilibrium "cut" will always be near-zero.

If the fullnode costs are too *low* to justify BMM...well that simply indicates that there's no problem and no one needs to care.

Obviously, in an asymmetric system, a mainchain can have two or more sidechains. But can you do the reverse, and have a sidechain of two different mainchains at once?

Yes. But this is a convoluted and terrible idea.

For example, you could have a sidechain of Bitcoin that was also a sidechain of Ethereum. The user would need to run all three full nodes, in order to validate the sidechain. The sidechain might need to be blind merged-mined on only one chain, or perhaps it could alternate chains or have an extremely strange chain-integration rule. The security/stability of the sidechain would probably be equal to that of the most insecure/unstable mainchain.

Is there anything that drivechains can't copy?

The underlying consensus of L1 (PoW vs PoS), and the community.

For example, Monero has a larger anonymity set, as of this writing. And Ethereum has more txn fees and users.

Is the 13,150 ACK parameter hardcoded? Why not let each sidechain specify it?

Yes.

To prevent a “race to the bottom”.

To promote solidarity among all sidechains, in the event of a theft.

5. Other

What kind of sidechain projects can we expect?

Please navigate to the sidechain projects section.

For more info, watch “Drivechain - Overview and Misconceptions”.