Application of drivechain to monero

Twiddle

1. Introduction

Monero leads the way in privacy standards for crypto currency yet falls behind in adoption as a result, one solution to broaden the applications of monero is drivechain. Drivechain is a proposed soft fork to bitcoin which would allow for the creation of “trust-less” side chains pegged 1:1 to bitcoin. It is “trust-less” because miners can steal funds from users, however assuming a sidechain is successful it is more profitable to take tx fees at least in a non tail emission blockchain like btc. The two mechanisms to deliver these features are blind-merge-mining and hashrate escrow. It would be unwise and overall damaging for monero as a whole to implement a 1-1 drivechain hard fork. However by exploring the technical aspects of how this could be performed this paper aims to aid in the development of monero based trust-less side chains pegged to monero.

2. Abstract

Monero’s private by default design and lack of major exchange centralization makes it an attractive central currency to develop drivechains on. Through a minimal scripting system other applications of cryptocurrency can be implemented on sidechains of monero while mainchain currency remains unaffected. Additionally monero’s tx keys may allow for better truly trust-less implementations of drivechains by having a built in secret to attest to an action made. While drivechain is by far not a perfect protocol the benefits it would add to the monero ecosystem, such as increased adoption through expansion of use cases and ease of fiat by having legal entity compliant sidechains, makes preliminary research into implementing it on monero worthwhile despite the fact that drivechains as they are should not be implemented on monero. This paper sets out to be heavily criticized so developers experienced at improving monero can adjust the outline below into something that can expand monero without damaging the security of funds and stability of monero’s fiat currency valuation.

Disclaimer: I am being sponsored to perform research into drivechain implementation on monero. The bounty and my communication with the bounty giver can be found at https://bounties.monero.social/posts/103/2-204m-research-implementation-of-drivechain-on-monero. I do not in any way support the idea of implementing drivechain in monero or adding additional scripting features unless they have zero privacy implications.

3. BTC vs XMR Challenges

There are inherent security issues that the drivechain protocol brings to any project that implements it. The logic behind them being acceptable risks are based around the assumption that any miner will be motivated by maximizing long term profits. Paul Sztorc, drivechain's founder, explains that "the security model [of drivechain] is economic. Miners 'farm' sidechains for their tx fees. The idea is that greedy miners will not kill the goose that lays the golden eggs" (*Frequently Asked Questions*, 2023). Monero as a privacy coin inherently has a higher threat model, it is likely that side chains would be attacked to prevent growth of a XMR based privacy coin ecosystem. Even if miners of these side chains would make more money in the long-term then stealing funds. This is an inherent flaw with implementation of drivechain to monero as it's entire philosophy is based around miners supporting projects which will generate the most revenue for themselves.

Additionally a large argument for drivechain adoption is that eventually bitcoin miner's only reward for mining will be tx fees; so to say tx fees won't be enough to incentivize mining is to refute one of the core elements of bitcoin. This is not the case with monero as tail emission means miners will never have to solely rely on tx fees, which are usually more than 50 times cheaper than btc tx fees (*XMR Vs BTC Tx Fee Historical Data*, n.d.). This will likely make it more profitable to steal from a bundle instead of collecting fees. Additionally, in the math that supports drivechain, a large security mechanism is the effect that attacking a sidechain will have on the main chain price (Sztorc, 2015). As XMR is viewed by the community as a currency, not a speculative financial asset, the impact of a side chain failing may be lower than in btc.

The worst scenario, however, would be a sidechain rewrite. In the original drivechain white paper the issue of what happens when a sidechain is overwritten is not evaluated for long. The issue is glossed over as a rewrite occurs "if the slot is in use: during the next 26,300 blocks, it accumulates 13,150 fails. (Ie, 50% threshold)" (*Bips/bip-0300*, n.d.) since the counter of activation votes reset once a sidechain is activated, for a sidechain to stay active it constantly needs to receive sidechain ACKs or it will be removed. This is a strange design as it costs tx fees to ACK a sidechain with no financial incentive. This makes rewriting a sidechain a consistent risk. Unless a sidechain's user base constantly ACKs to defend their sidechain every 26,300 blocks all of their mainchain currency will be stolen by the nature of anyone can spend deposits relying on the data stored in the D1 cache to reject them as illegitimate withdrawals. Luckily, this issue is lessened by the fact that in this outline regular monero transactions can still have scripting elements attached, though the miner of the block could choose to reject these transactions, attempting to cause this disaster scenario to occur.

Monero does not have anywhere near the scripting capabilities of bitcoin as the design philosophy is entirely about making the most useful cash like privacy preserving cryptocurrency. Luckily, drivechain relies entirely on bitcoin's scripting. It does not utilize any of the more complex features that would be very difficult to port across protocols. The solution this paper proposes is to add consensus significance to a limited set of tx_extra tags which will allow for the necessary scripting features without touching any of the important aspects of monero that allow it to preserve privacy. Despite the fact that there are privacy implications that come with the use of the tx_extra field (*[Discussion] Consider Removing the Tx_extra Field · Issue #6668 · Monero-Project/monero*, 2020) it has multiple presidents of use in other features of monero such as multisig. Additionally, to be able to mark a script transaction invalid the script must be unencrypted making tx_extra the perfect field to use.

4. 1-1 feature implementation XMR drivechain

Disclaimer: the following is meant to be a 1-1 application of drivechain onto the monero network as a hard fork. "Fixing" the drivechain protocol to fit the standards of privacy and security we expect as monero users is out of the scope of this paper or will be mentioned in the further research section. The only exceptions to this are the replacement of human readable aspects M1 of bip300 with a single 10 byte ticker field and the addition of the BMM_WITHDRAWAL message.

Any implementation of drivechain will require adding scripting features to monero through the use of the tx_extra field or similar. This could have impacts on privacy by making transactions less uniform. The implementation described below is meant to be as stripped back as possible. It is also important to note that tx_extra is currently used to store other data needed to enable some features. This has been considered and has influenced the design of the drivechain messages to fit the standards used by other features of monero that utilize this field. Additionally the coming serphais/jamtis upgrades should only affect the necessary number of bytes needed for the sidechain subaddress field in the DEPOSIT message, as its changes to addresses make subaddresses obsolete and addresses in general longer.

Caches

The same caches as outlined in the original drivechain whitepaper are outlined in the two following tables. There have been slight modifications where necessary to make drivechains function better on monero and to remove some extraneous fields that were originally specified in the drivechain whitepaper.

D1 - the sidechain list

Field No.	Label	Type	Description
1	Sidechain Number	uint8_t	ID number of sidechain used to uniquely identify each sidechain.
2	Sidechain Ticker	char[8]	String Ticker to be used to refer to sidechain (Ex: XMR2) max length of 8 and must be unique.
3	Active	bool	Is this Sidechain active?
4	Activation Status	int , int	The age of the proposal (in blocks); and the number of "fails" (a block that does NOT ack the sidechain). This is reset after the sidechain activates.
5	Private Key	uint256	Used to implement “Anyone can spend” outputs which rely on trust in miners to confirm validity.
6	Wallet Balance	uint256	Current amount of XMR stored inside the side chain’s wallet.

D2 - the withdraw list

Field No.	Label	Type	Description
1	Sidechain Number	uint8_t	ID number of sidechain that funds are being withdrawn from.
2	Bundle Hash	uint256	Keccak-256 transaction hash of bundle withdrawal transaction.

3	Work Score (ACKs)	uint16_t	How many miner upvotes a withdrawal has. Starts at 0. Fastest possible rate of increase is 1 per block.
4	Blocks Remaining	uint16_t	How long this bundle has left to live (measured in blocks). Starts at 26,300 and counts down.

Axioms

- 1 byte **DC_MSG** - Similar to the tag system implemented for adding public keys in tx_extra (*Tx_extra Field Description*, 2020) with the additional parity tag added at the end of the checksum. This tag indicates the type of drivechain message, allows transaction to be marked invalid if it doesn't fit msg format while also creating temporarily unspendable outputs depending on the type.
- 1 byte **SC_NUM** - Indicates the sidechain code, there can only be one active sidechain for each code at one time.
- 32 bytes **TX_KEY** - The tx_key of the transaction, some functions of drivechain require checking the output amounts of transactions this is randomly chosen by the sender so it should not have privacy impact on other transactions made by a wallet to publish this for certain transactions.
- 33 bytes **SCRIPT_CHECKSUM** - Keccak-256 hash output of the script with the **DC_MSG** byte appended to the hash to prevent non drivechain transactions using the tx_extra field to be interpreted as drivechain transactions. While also making it easy for code to tell if a transaction is a drivechain transaction.
- 8 byte **TICKER** - Ticker of the proposed sidechain.

Message Types

The following breaks down the tx_extra field for each message type. The message part of the tx_extra field cannot be encrypted to be considered a drivechain message. All messages but the BUNDLE_1BYTE_ACK & BUNDLE_2BYTE_ACK have a constant length. All transactions that have aspects of a drivechain message but are not valid (checksum fails, too short, etc …) are treated as normal transactions with arbitrary data in their tx_extra field. Any below mentions of conditions where a transaction is invalidated assumes the message is properly formatted with a valid checksum but fails a consensus rule of the message. The tag of each message is the DC_MSG field, the actual value corresponding to each tag is arbitrary so they have been excluded from this paper. All message types are invalid if there is already a message of that type for the same SC_NUM in the block besides DEPOSIT.

- BUNDLE_1BYTE_ACK - Max Length: 290 bytes
  1-byte DC_MSG (BUNDLE_1BYTE_ACK)
  n-byte 1BYTE_UPVOTE_VECTOR
  33- byte SCRIPT_CHECKSUM

Upvotes specified bundles based on the supplied vector. Same as defined in the drivechain whitepaper. Ex: Upvoting 3rd bundle of sidechain 1 and 4th bundle of sidechain 3 assuming sidechain 2 has no bundles proposed the vector would be { 0x02, 0x03 } but if sidechain 2 has a bundle proposed the ACKer would have to ACK a sidechain 2 bundle as well.

- BUNDLE_2BYTE_ACK - Max Length: 546 bytes
  1-byte DC_MSG (BUNDLE_2BYTE_ACK)
  n-byte 2BYTE_UPVOTE_VECTOR
  33-byte SCRIPT_CHECKSUM

Upvotes specified bundles based on the supplied two byte vector. Allowing bundles of indexes above 256 to be ACKd. Each index should be little endian encoded. Ex: Upvoting the 356 bundle of sidechain 1 { 0x6D01 }. It is important to note that the tx_extra size limit may be hit while using this message type with a transaction with a lot of outputs. Luckily the conditions that require this are very unlikely and would additionally only be able to occur if the miner of the block does not want to ACK bundles and a user attempts to include a tx to be included in the block with their 2 byte bundle ack.

- BUNDLE_AUTO_ACK - Length: 34 bytes
  1-byte DC_MSG (BUNDLE_AUTO_ACK)
  33-byte SCRIPT_CHECKSUM

Upvotes all bundles that are leading their rivals by at least 50 upvotes.

- BUNDLE_PREV_ACK
  1-byte DC_MSG (BUNDLE_PREV_ACK)
  33-byte SCRIPT_CHECKSUM

Upvotes all bundles that were upvoted in the last block.

- PROPOSE_BUNDLE

  1-byte DC_MSG (PROPOSE_BUNDLE)
  1-byte SC_NUM
  32-byte BUNDLE_HASH
  33-byte SCRIPT_CHECKSUM

Proposes a withdrawal bundle to be voted on. Drivechain pushes the responsibility of adding most of the needed behind the scenes work onto any sidechain created (*Drivechains: A Detailed Analysis*, 2023). Because of moneros low tx fees it may be preferable for the proposed bundle to include all of the bundled transactions in a separate tx_extra tag to make it easy to prune after the bundle is accepted or rejected. Though this would only be an improvement if a solution to the requirement of miners needing to run sidechain nodes is solved as it still makes the main chain only users need to trust the corresponding sidechain withdrawal transactions have been made. As sidechain users need to run a main chain node, adding an alarm mechanism and punishment for trying to steal could help encourage good behavior. Invalid if BUNDLE_HASH already exists in a D2 entry, the sidechain number is ignored during validation to minimize possible fraud.

- PROPOSE_SIDECHAIN

  1-byte DC_MSG (PROPOSE_SIDECHAIN)
  1-byte SC_NUM
  8-byte TICKER
  32-byte SIDECHAIN_KEY
  33-byte SCRIPT_CHECKSUM

Proposes a new drivechain. Invalid if a sidechain is currently active in the specified SC_NUM. Invalid if the DRIVECHAIN_KEY is used by another D1 entry. Invalid if SIDECHAIN_KEY is any byte repeated 32 times as this would break controls on withdrawals or prevent accepting blind merge mine requests based on specifics of code implementation. Also invalid if SIDECHAIN_KEY is not unique amongst all sidechains.

- ACK_SIDECHAIN

  1-byte DC_MSG (ACK_SIDECHAIN)
  1-byte SC_NUM
  32-byte SIDECHAIN_KEY
  33-byte DRIVECHAIN_CHECKSUM

ACKs a proposed sidechain. Multiple can be included in a single block but only the first is counted. Is invalid if there is no proposed sidechain for the D1 entry associated with the SC_NUM that has the specified SIDECHAIN_KEY.

- DEPOSIT

  1-byte DC_MSG (DEPOSIT)
  1-byte SC_NUM
  32-byte TX_KEY
  32-byte SIDECHAIN_SUB_ADDRESS
  33-byte SCRIPT_CHECKSUM

All spends from the sidechain wallet are invalid unless they are a WITHDRAW DC_MSG type and their tx hash matches an "approved" bundle hash. A DEPOSIT is invalid if the sidechain's wallet address and private view key cannot decode the deposit transaction. The transaction is also invalid if TX_KEY, the sidechain's address, and tx_hash fail to decrypt transaction amount as it is likely the depositing user is being deceived in some way or sending to a subaddress, which will cause the funds to be lost.

- WITHDRAW

  1-byte DC_MSG (WITHDRAW)
  1-byte SC_NUM
  32-byte TX_KEY
  9-byte TX_FEE
  33-byte SCRIPT_CHECKSUM

The bundled withdrawal has been approved by 13,150 ACKs. Invalid if transaction hash does not match an approved bundle hash for that sidechain. This is the main reason that drivechain should be a hard fork. If not enough users update their code an approved withdrawal and unapproved withdrawal appear like a regular transaction without inspecting the script in the tx_extra field.

- BMM_ACCEPT

  1-byte DC_MSG (BMM_ACCEPT)
  1-byte SC_NUM
  32-byte ONE_TIME_PUB_KEY
  32-byte SC_BLOCK_ID
  33-byte SCRIPT_CHECKSUM

A blind merge mine accept makes the request output spendable after 10 confirmations. This is done by making a special one time public key to sign the BMM withdrawal transaction with to attest that the BMM withdrawal requestor also made the BMM ACCEPT transaction. Invalid if multiple ACCEPTS for one sidechain are included in a block. Invalid if the message uses the same one time public key as the ACCEPT message.

- BMM_WITHDRAWAL

  1-byte DC_MSG (BMM_WITHDRAWAL)
  1-byte SC_NUM
  32-byte TX_KEY
  33-byte BMM_ACCEPT_SCRIPT_CHECKSUM
  33-byte SCRIPT_CHECKSUM
  32-byte WITHDRAWAL_SIGNATURE

A BMM_WITHDRAWAL is a slight improvement on the original bip 301 specification. By adding a third transaction to actually be able to redeem the BMM_REQUEST payout risks associated with the BMM requestor needing to risk a majority of an entire block's tx fees can be mitigated. Invalid if sidechain has been reorged to invalidate the accepted block and has been signed with the ACCEPT public key or if it hasn't been ten blocks since the ACCEPT and

REQUEST pair block. Invalid if sidechain hasn't been reorged to invalidate the accepted block and has been signed with the REQUEST public key.

- BMM_REQUEST

  1-byte DC_MSG (BMM_REQUEST)
  1-byte SC_NUM
  32-byte ONE_TIME_REFUND_PUB_KEY
  46-byte SC_BLOCK_HEADER
  32-byte SC_BLOCK_ID
  4-byte PREV_MAINHEADER_BYTES
  32-byte TX_KEY
  33-byte SCRIPT_CHECKSUM

Sends mainchain XMR to the wallet address that is created when a private key is the SC_NUM byte repeated 32 times. This is to create a different type of "anyone can spend" transaction that has different consensus rules. Invalid if it does not have a matching BMM_ACCEPT in the block for that SC_NUM. Invalid if there is more than a single BMM_REQUEST & BMM_ACCEPT for each SC_NUM in a block.

5. Further Research

Economic influence - Any major change to the capabilities of a crypto currency especially when it could enable new features, change mining incentive structure, or impact the privacy and security of the main chain will undoubtedly have effects on the cryptocurrency's economics. Hopefully as layer 2 labs continues to develop the drivechain concept they will be able to gather in depth real world data on how drivechain or similar protocols affect the economics of a crypto currency. Which can then be used to better predict what effects drivechain would have on monero's economics.

Theft-less Tx_Key escrow - When a user initially deposits to a sidechain they may not need to leak their tx_key or sidechain sub address. Instead drivechain could be reformatted to use Tx_Keys to prove an address on a different chain is owned by the same entity. This would in theory improve privacy of deposits and enable instant withdrawals. By saving the Tx_key of the deposit transaction Alice makes. She would then be able to attest that she is owed the same amount of sidechain XMR minus transaction fees by signing a special sidechain transaction or tx_extra script with that key. Consensus would be able to be made easily on the sidechain as all sidechain users run full nodes and the sidechain deposit wallet private keys are public. If Alice wishes to make a withdrawal back to mainchain currency she can make a special sidechain transaction to make the sidechain currency unspendable. Creating a message that has a bundle proposal script signed with this key on the main chain then waiting at least till the next block to publish the bundle withdrawal including the sidechain tx_key from the previous transaction. This would allow for attestation that Alice was the first to know the secret and thus must be the one to have "burned" the sidechain currency. As well as allow for validation by sidechain users of the amount burned. The main issues with this method of escrow would be finding a way to implement it without requiring mainchain users to also run sidechain nodes. Though it at least keeps the normal level of security associated with cryptocurrency by not allowing miners to permanently steal funds just by sheer hashrate.

Blind merge mining - Blind merge mining has been heavily criticized for its effects on mining centralization as either miners lose potential profit by accepting bind merge mined requests or miners will need to run sidechain nodes to be able to make their own accept messages (*Drivechains Introduce New Incentive Dynamics to Bitcoin*, 2023). Additionally instant withdrawals realistically need to be implemented for blind merge mining to ever be used, since a blind merge mine requestor has to have large sums of main chain currency to be able to cover probably somewhere near the tx fees of the entire block. They then get paid in sidechain currency which takes months to withdraw back onto the mainchain. As a sidechain reorganization also has no effect on the mainchain the sidechain blind merge miner would lose their mainchain currency with no reward. Though the BMM_WITHDRAWAL message helps with the later the concerns of further incentivizing centralization need to be addressed and fixed before drivechain should be implemented on any chain.

6. Community Sentiment

BTC DRIVECHAIN SENTIMENT

In general the three common opinions on the Drivechain proposal are, drivechains are a bad idea and the specification for how they are proposed to be implemented is insecure, drivechains are a good idea but how they are proposed to be implemented is insecure, and the drivechain proposal is good all around. Based on community research the majority of btc users aware of the drivechain proposal fall into the first two categories. This is easily demonstrated by the fact that in a sponsored BIP-300 pull request written by luke-jr there isn't a single response that directly supports drivechain besides responses made by drivechain's creator Paul Sztorc (luke-jr (Sponsored by layer 2 labs), n.d.). This negative sentiment exists despite the fact that drivechain offers a rich field for blockchain developers to make new technologies. The problems simply are too glaring for them to feel confident supporting its development. Two very thorough critiques of drivechain have also been made by Peter Todd, a blockchain analyst who was sponsored by layer 2 labs to write a detailed analysis of the drivechain protocol, and Shinobi of bitcoin magazine respectively. Though there are some supporters of drivechain as it stands the main problems people have with drivechain, specifically with incentive changes and mining centralization impacts, have not been properly addressed by drivechain's faq page or Sztorc tweets making the value of the supporters sentiment dubious. Specifically he dismisses the concerns of centralization by saying "All BIP300 does, is supercharge [Merge Mining]" by increasing the profits that come from mining which he claims is good for bitcoin. Aljosha Judmayer, a senior researcher at the Austrian information security research center SBA research, in his paper "Merged Mining: Curse or Cure?" explains the observed trend of mining pools having a larger share of merge mined block discovery then on a non merge mined cryptocurrency stems from the fact that "additional costs regarding bandwidth, storage and validation of the merge-mined blockchain's blocks/transactions are incurred regardless of the relative size or hash rate of the miner" (Judmayer et al., 2017, 329). If anything drivechain will lead to increased centralization as the profit from drivechain merge mining is less than a merge mined coin by lack of block reward and though theoretically miners could use the blind merge mining features it seems unlikely as they would be leaving profit on the table as it is unlikely Sztorc predicted 99% of sidechain fees going to mainchain miners will occur as sidechain miners take all of the risk.

XMR SENTIMENT ON GENERAL CHANGES

The monero community is generally against any addition that either harms privacy and/or adds features that doesn't bring monero closer to being a completely private cash like cryptocurrency. The cryptonote v2 whitepaper even states "privacy and anonymity are the most important aspects of electronic cash" (Saberhagen, 2013) prioritizing plainly privacy over the utility of a cryptocurrency. However there have been disagreements in the community especially on removing features from monero for privacy reasons. In general developers will push for the highest level of privacy with some prioritizing the utility of a feature. The fact that tx extra has not been removed demonstrates this trend. Though its arbitrary data impacts fungibility, its ability to be used to add new features brings enough value to warrant its existence with just a limit on size (*Monero Research Lab Meeting - Wed 15 March 2023, 17:00 UTC*, n.d.). As such sometimes utility is prioritized over absolute privacy of users. The utility of a "fixed" drivechain is quite high well it exists in the constraints of the accepted risk inherent to usage of tx extra.

Removing or limiting features is hard for the community to form a consensus on; however the constant improvements to privacy and security also show how far the community is willing to go to keep monero the best private digital cash. This is clearly demonstrated by the serpahis/jamtis upgrade which is a massive effort that will more than double the length of addresses. No matter what it takes, the majority of the community will support major changes if they increase privacy and security of funds evidenced by the "several tens of thousands of USD [donated] through the CCS to support implementation work" (Brunner, 2023). Showing a loose consensus that these upgrades are worth implementing. As such the main thing that would prevent drivechain adoption are the security issues it brings. The protocol needs to be fixed before it is mentioned seriously in any way to the community. Though the privacy implications of proper usage of the drivechain specification above are minimal, the security and economic issues undermine monero's goal of being the best private digital cash. Though these changes can be implemented as a soft fork a hard fork makes more sense as it will help to increase the security of funds secured in sidechains. A "fixed" drivechain with properly reviewed code and economic research supporting it would be a pretty attractive feature to add since a failed sidechain just means people will withdraw their mainchain currency from side chains. Making a "fixed" drivechain something reasonable for the community to support its development.

7. Conclusion

Increasing monero adoption and use cases by creating a pegged sidechain system makes a "fixed" drivechain protocol worth implementing. Through a minimal tx_extra scripting interface drivechains as proposed on btc can be implemented on monero. Through a handful of upgrades and practical testing drivechains can be the protocol that allows monero to function as the best private digital cash and the reserve currency that backs other applications of crypto currency. This in turn will insulate monero from entities that seek to prevent its adoption and will benefit the monero user base overall.

8. References

Beikverdi, A., & Song, J. (n.d.). Trend of centralization in Bitcoin's distributed network. *2015 IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, 1-6. 10.1109/SNPD.2015.7176229

bips/bip-0118. (n.d.). GitHub. Retrieved January 28, 2024, from https://github.com/bitcoin/bips/blob/master/bip-0118.mediawiki

bips/bip-0300. (n.d.). GitHub. Retrieved January 26, 2024, from https://github.com/bitcoin/bips/blob/master/bip-0300.mediawiki#user-content-The_Six_New_Bip300_Messages

bips/bip-0301. (2019, July 23). GitHub. Retrieved January 26, 2024, from https://github.com/bitcoin/bips/blob/master/bip-0301.mediawiki

BTC Scripting. (2024, January 17). Bitcoin Wiki. Retrieved January 25, 2024, from https://en.bitcoin.it/wiki/Script

[Discussion] Consider removing the tx_extra field · Issue #6668 · monero-project/monero. (2020, June 20). GitHub. Retrieved January 26, 2024, from https://github.com/monero-project/monero/issues/6668#issuecomment-670978771

Drivechains: A Detailed Analysis. (2023, October 13). Peter Todd. Retrieved January 23, 2024, from https://petertodd.org/2023/drivechains

Drivechains Introduce New Incentive Dynamics to Bitcoin. (2023, September 5). Bitcoin Magazine. Retrieved February 8, 2024, from https://bitcoinmagazine.com/technical/drivechains-introduce-new-incentive-dynamics-to-bitcoin

Frequently Asked Questions. (2023, March 22). Drivechain. Retrieved January 23, 2024, from https://www.drivechain.info/faq/index.html

Judmayer, A., Zamyatin, A., Stifter, N., Voyiatzis, A. G., & Weippl, E. (2017, September 13). Merged Mining: Curse or Cure? *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, *Lecture Notes in Computer Science (LNCS, volume 10436)*, 316–333. https://link.springer.com/. https://doi.org/10.1007/978-3-319-67816-0_18

luke-jr (Sponsored by layer 2 labs). (n.d.). *[WIP] BIP-300 implementation*. github. Retrieved January 23, 2024, from https://github.com/bitcoin/bitcoin/pull/28311

Paul Sztorc Research Director, Tierion May 15th, 2019. (2019, May 15). Drivechain. Retrieved January 23, 2024, from https://www.drivechain.info/media/slides/construct-2019.pdf

Sztorc, P. (2015, November 24). *Drivechain - The Simple Two Way Peg*. Truthcoin. Retrieved January 27, 2024, from https://www.truthcoin.info/blog/drivechain/

tx_extra field description. (2020, January 5). Monero Stack Exchange. Retrieved February 6, 2024, from https://monero.stackexchange.com/questions/11888/complete-extra-field-structure-standard-interpretation

XMR vs BTC tx fee historical data. (n.d.). Monero vs Bitcoin fees. Retrieved January 27, 2024, from https://monero-bitcoin-fees.vercel.app/