GRAVITY: A Peer-to-Peer Exchange Protocol Using Proof-of-Work

Abstract. A purely peer-to-peer protocol for cross-blockchain trade would allow payments and trades to be sent directly from one party to another without going through an intermediary exchange or marketplace. Bitcoin transactions form part of the solution, but the main benefits are lost if a trusted third party is still required to mediate trades across different blockchains. We propose a solution to the cross-blockchain exchange problem by describing a protocol that allows trades between peers with Bitcoin [1] on one side, and a second sufficiently capable blockchain on the other, such as Radiant [2]. As long as Bitcoin has the majority of hash power, then the second blockchain can validate the Bitcoin originated transaction using Simplified Payment Verification (SPV) and then release the coins on the second blockchain by accepting and validating a sufficient number of headers. Any two willing parties can create and complete the transactions with nothing more than the respective blockchain nodes, without the need for a third party.

1. Introduction

Trades across blockchains relies almost exclusively on exchanges serving as trusted third parties to process electronic trades. While the system works well enough for most trades, it still suffers from the inherent weaknesses of the trust based model. Completely peer-to-peer trades are not really commonplace, centralized exchanges are predominant in mediating the vast majority of cross blockchain trade volume. The overhead of the exchanges increases the costs and limits casual peer-to-peer trades, and there is a broader cost in prerequisite steps to verify that an exchange website or application is legitimate. With the need for exchanges, the need for trust spreads. Exchanges must be wary of their customers, hassling them for more information than they would otherwise need. Even decentralized exchanges must remain vigilant to ensure they comply with various regulations, privacy laws and constantly monitoring threats.

What is needed is an electronic cross-blockchain trade system that is peer-to-peer and based on proof-of-work instead of exchanges, allowing any two willing parties to trade directly with each other without the need for a third party. Trades that are completely peer-to-peer, involving only the peers and their respective blockchain nodes, would protect users from exchange vulnerabilities, and buyers and sellers would be protected since they never lose custody of their coins. In this paper, we propose a solution to the problem of trading across proof-of-work blockchains without the use of an intermediary using a peer-to-peer protocol, leveraging the ability to validate the expended proof of work on the Bitcoin network, and the sufficiently capable programming instruction set on Radiant blockchain. The system is secure as long as the respective blockchains are secure, users can build and broadcast their transactions directly to blockchain nodes without the need of an intermediary or third party.

2. Proof-of-Work

We can leverage the self-evident nature of proof-of-work signals to implement the cross *Bitcoin-to-other-blockchain* protocol. Recall that the Bitcoin blockchain uses a proof-of-work consensus mechanism wherein Bitcoin miners scan for a value that when hashed, such as with SHA-256, begins with an expected number of zero bits. The average work required is exponential in the number of zero bits required and can be verified via executing a double SHA-256 hash. Once the hashing effort has been spent to make it satisfy the proof-of-work target, the block cannot be changed without redoing the work. As later blocks depend upon the previous blocks chained before it, the work to change any given block would require redoing all the blocks after it.

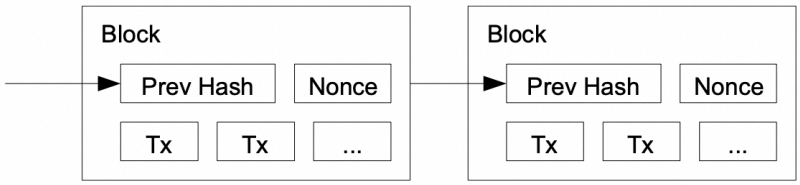

Diagram 1: Proof of work is a self-evident consensus mechanism and can therefore be leveraged in other blockchains to verify the total energy expenditure of a chain of block headers

Proof-of-work is the only possible self-evident consensus mechanism. Clients can efficiently, in constant time O(1), assess what happened on the Bitcoin network with a high degree of confidence that increases exponentially with each additional block in the chain of blocks. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. Leveraging the self-evident nature of Bitcoin's proof-of-work is what makes it possible to do a cross-blockchain trade between Bitcoin and a secondary blockchain, such as Radiant.

It is important to note that the Radiant blockchain uses SHA512/256 as the proof-of-work algorithm which increases the security of the system in that Bitcoin miners cannot redirect their SHA256 hash power to Radiant in an attempt to forge Radiant headers when performing cross-blockchain swaps with *third party blockchains*. The full implications of the different proof-of-work algorithms and security bounds are left for a future paper.

3. Simplified Payment Verification

Recall that it is possible to verify payments without running a full Bitcoin network node. The key to accepting cross blockchain payments is to use merkle-tree inclusion proofs, what Bitcoin calls "Simplified Payment Verification (SPV)", and thus verifying a sufficiently long chain of blocks was computed, with a high enough target difficulty. From the Bitcoin white paper:

"*A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped. He can't check the transaction for*

himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it." - Section 7, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008

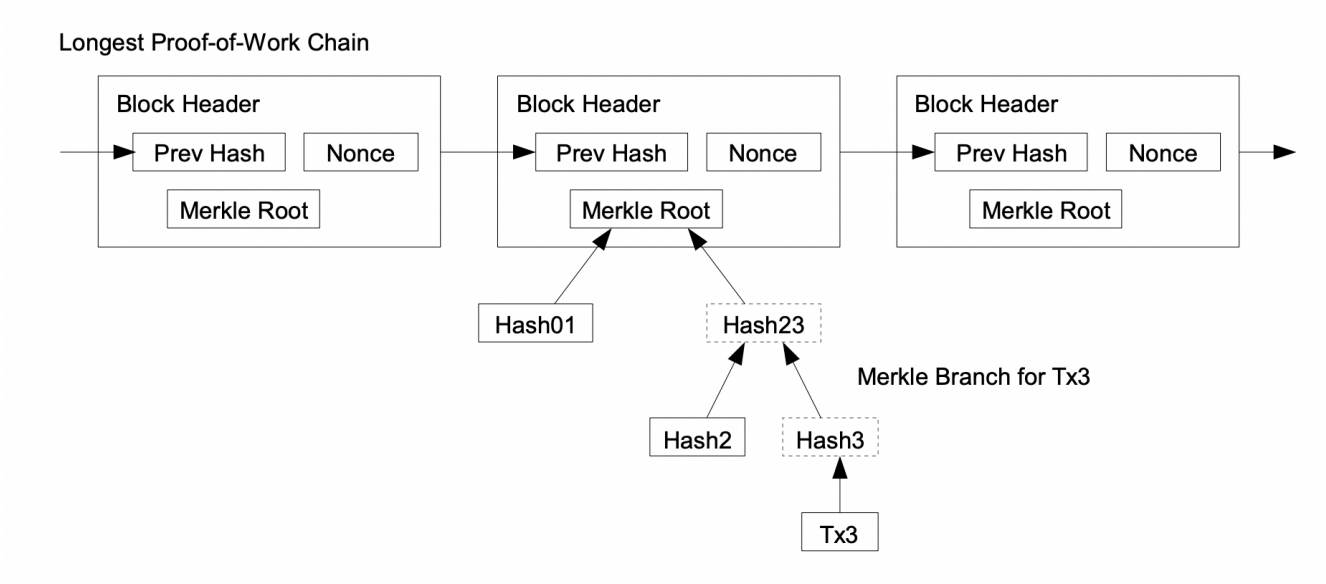

Diagram 2: Simplified Payment Verification: validate transaction was included in a block and compare against all known block headers

For this peer-to-peer exchange protocol, we implement a smart contract on Radiant blockchain to lock an unspent transaction output (UTXO), that can only be unlocked, or spent, by providing a list of block headers from the Bitcoin network, along with a Merkle proof of the transaction made by the counterparty in the trade. Radiant has a sufficiently capable programming instruction to accept, decode, and validate Bitcoin block headers and the associated Merkle proof of the relevant transaction. The Bitcoin white paper continues:

"*As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network.*" - Section 7, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008

As long as the total value of the payments made on Bitcoi ,are less than some fraction of the total energy needed to forge an alternative chain of Bitcoin block headers, then the trade can be considered secure. In the next sections we describe how the peer-to-peer protocol works by leveraging this fact about the security guarantees that Simplified Payment Verification offers.

4. Standard Operation

The standard operation steps of the protocol are as follows:

1. Maker broadcasts a transaction to Radiant, with properties:
    1. Amount of Bitcoin Satoshis to receive for the trade.
    2. Amount of Radiant Photons offered in exchange for the Bitcoin Satoshis.
    3. Receive address of where Taker will send Bitcoins to Maker
    4. Number of block headers that will be required by the SPV proof.
    5. A covenant that only unlocks Radiant Photons if a valid Bitcoin SPV proof is provided.
2. Taker spends the the initiating user transaction to temporarily claim the trade:
    1. Adds a small amount of Radiant Photons to new UTXO as good faith collateral that they intend to complete the trade.
    2. A time limit exists to complete the trade or the collateral is forfeit.
3. Taker broadcasts the transaction to the receive address specified by the Maker in Step 1.
4. Taker uses the SPV proof once their transaction is confirmed to claim the Radiant Photons.

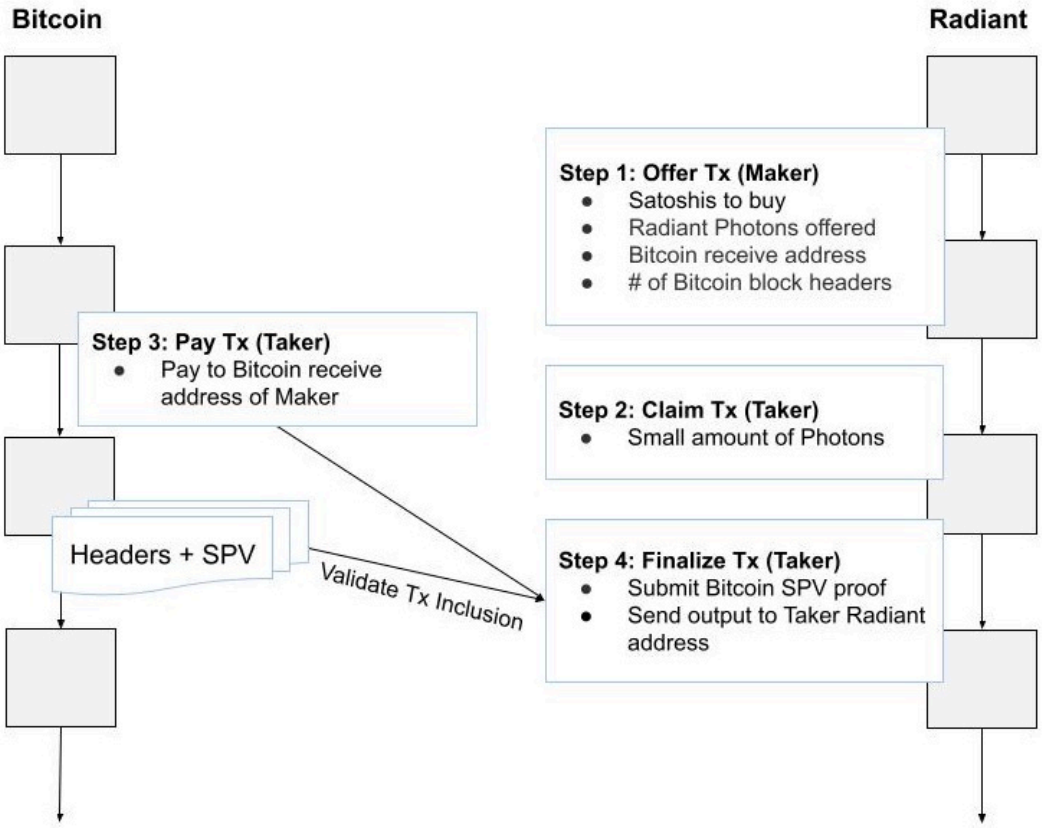

Diagram 3: Standard Operation Overview: Trade between Bitcoin and Radiant.

The Maker posts a transaction on Radiant with a special covenant that can only be spent in three ways.

The first way allows it to be spent by anyone so long as they add the predetermined amount of Photons the initiating user expects. This acts as a form of bond or collateral to prevent malicious actors from intentionally disrupting a user from executing their trade intent. The collateral is refunded

when the trade is successfully completed, or it is forfeit if the elapsed time has passed. For example, it may be sufficient to give the buyer up to several blocks and perhaps much longer such as 200 Bitcoin blocks to mitigate sudden Bitcoin network congestion which results in a transaction confirming many hours later.

The second way the transaction may be spent is by anyone posting a valid SPV proof of the transaction paying the required amount to the address posted by the Maker along with the required number of block headers. The Taker has the most incentive to do this to complete their transaction, however any participant in the system can automate this process on their behalf. A small extra fee could be added for a relayer service to monitor for these transactions continuously.

The third way the transaction may be spent is that the Maker user cancels the trade, spending it to themselves to prevent anyone else from taking the trade. The Maker can cancel the trade anytime and no time limit is needed.

5. Multiway Blockchain Operation

The protocol can be extended to leverage Radiant, acting as a secondary bonding blockchain, to connect any two proof-of-work based blockchains together such as Bitcoin, Litecoin, Dogecoin, Kaspa, Ethereum Classic, etc. The key enabling technique is the use of Radiant Photons as a collateral to cover the cost of a default on either side of the trade.

The multiway blockchain operation steps of the protocol are as follows:

1. Maker broadcasts a transaction to Radiant, with properties:
    1. The first and second proof of work algorithms types.
    2. Amount of first blockchain (ex: Bitcoin) units to receive for the trade.
    3. Amount of second blockchain (ex: Dogecoin) units *offered* for the trade.
    4. Receive address of where Taker will send first blockchain units to Maker
    5. Number of block headers that will be required by the SPV proof. Example: 10 block headers.
    6. Extra collateral of Radiant Photons to cover the expected value of the trade.
    7. Contains a covenant that only unlocks the collateral Radiant Photons if a valid SPV proof is provided.
2. Taker spends the the initiating user transaction to temporarily claim the trade:
    1. Taker attaches where they want to receive their second blockchain tokens
    2. Taker attaches their extra collateral of Radiant Photons in the same amount as Maker.
3. Taker broadcasts the transaction to the receive address specified by the Maker in Step 1.
4. Maker broadcasts their payment to the second blockchain to the receive address specified by the Taker in Step 2.
5. Either party or service may broadcast the respective SPV proofs and required block headers of both blockchains and simultaneously release the collateral to both parties.

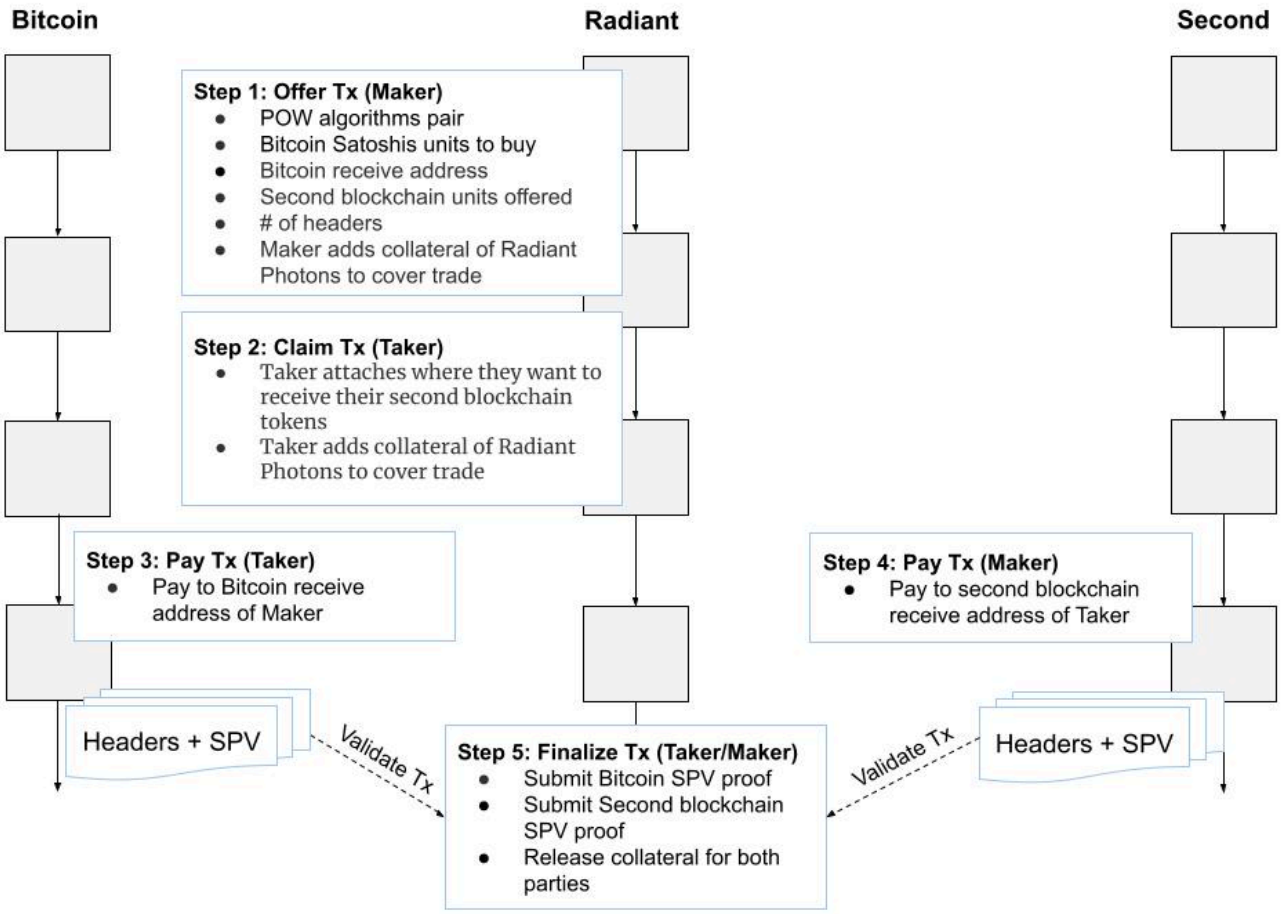

Diagram 4: Multiway Blockchain Operation Overview: Trade between Bitcoin and a Second blockchain using Radiant as facilitator.

The multiway blockchain operation requires both parties to use Radiant units as the collateral and effectively turns Radiant into a trustless bond service. The solution works between any two blockchains as long as they are based on proof-of-work: their SPV proof and header hash algorithms can be verified with the Radiant programming instruction set codes.

6. Security

The cost of attacking this protocol is at least equal to the total energy cost of producing the requisite number of forged block headers, and therefore the system is secure enough as long as the total aggregate value of cross blockchain trades is less than that amount. Since Simplified Payment Verification provides a probabilistic security measure, it is important to choose parameters carefully to ensure that the cost to attack is an order of magnitude greater than the value of the potential gain from any attempt to execute the attack and steal the locked outputs.

We consider the scenario of an attacker who generates a forged chain to supply the requisite number of blocks to be input in the unlocking script of the locked outputs, here we provide a calculation to show the total energy cost.

Calculations

- The difficulty to mine a Bitcoin (BTC) block as of April 12, 2024 is 86,388,558,925,171.
- The lowest value of 1 BTC as of April 12, 2024 was traded at $68,540.00.
- The block reward is 6.25 BTC. We ignore the incremental reward increase due to fees to simplify calculations.

We can therefore assume that the opportunity cost an attacker would forgo would be equal to 6.25 x $68,540.00 or about $428,375.00.

With the proof-of-work exchange protocol described in this paper we can see that trades can be considered security as long as the total value of trades in a given block is less than 6.25 BTC ($428,375.00). If the peer chooses a larger number of blocks such as 10 blocks then the total cost of an attack would be 62.5 BTC ($4,283,750.00). In other words, peer-to-peer trades can be considered reasonably secure if the total value of trades is less than 1/2 of the total opportunity cost of the blocks required for settlement, or about 31.25 BTC ($2,141,875.00). The total throughput of trade volume per month would be 135,000 BTC ($9,252,900,000.00). In practice it will likely be 1/10th that for extra security and cautiously chosen parameters.

Even if an attack is accomplished, it does not affect the protocol as a whole, such as forever destroying the mechanism or creating any lasting damage to other users. An attacker can only try to steal coins from the other blockchain during the execution of the attack. Users can adapt by changing their preferences through various parameters fully in their control such as: making smaller trades, increasing the required number of blocks to redeem, limiting a time window that the trade can take place, and also adjusting the difficulty target. The users have full control over their security parameters prior to posting or accepting a trade.

7. Conclusion

We have proposed a peer-to-peer protocol for cross-blockchain trades without relying on an intermediary. We started with the basic building blocks of proof-of-work and merkle-tree inclusion proofs, which together provides an efficiently computable and self-evident account of a transaction history on the Bitcoin network. We proposed a peer-to-peer protocol between Bitcoin and Radiant to be able to execute trades without the need for any third party and with users maintaining full custody of their digital assets at all times. As long as the total aggregate value of the trades in any given time window is less than the total energy cost required to forge a chain of block headers, the protocol is secure. Users can create transactions for buy or sell offers and publish and accept trades directly using the respective blockchain nodes. Users can post their offers to any website, social network or forum. Additionally, we have proposed an extension to the protocol which allows the

interoperability between a *third* proof-of-work based blockchain with Radiant acting as the *trustless* intermediary using the Radiant token as a type of collateral to enable bi-directional peer-to-peer trades between Bitcoin, Radiant and any other proof-of-work based blockchain such as Litecoin, Dogecoin, Kaspa, Ethereum Classic and others.

8. References

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf, 2009.

[2] "Radiant: A Peer-to-Peer Digital Asset System", https://radiantblockchain.org/radiant.pdf 2022.