Preparing Simplified Payment Verifications for Cross-Blockchain Token Transfers

Marten Sigwart*, Philipp Frauenthaler*, Christof Spanring†, Stefan Schulte*

* Distributed Systems Group
TU Wien, Vienna, Austria
{m.sigwart, p.frauenthaler,
s.schulte}@dsg.tuwien.ac.at

† Pantos GmbH
Vienna, Austria
contact@pantos.io

***Abstract*—Blockchain relay schemes rely on off-chain clients constantly submitting block information from a source blockchain to the relay running on a destination blockchain. As clients incur costs when submitting block headers, an incentive structure needs to be in place that compensates clients for their efforts.**

In this paper, we develop an incentive structure for blockchain relays that follow a proof on demand approach where block headers are optimistically accepted and only fully validated if identified as illegal by off-chain clients. The preliminary cost analysis shows that such blockchain relays are able to drastically reduce operational costs over relays that validate every single submitted block header.

I. Introduction

The Token Atomic Swap Technology (TAST) research project[1] aims to create a platform for cross-blockchain interoperability. The overarching goal is to investigate possible means of interconnecting various blockchains [2]. As a first step towards more general blockchain interoperability we have developed a prototypical blockchain relay capable of performing on-chain Simplified Payment Verifications (SPVs) [5]. That is, clients are able to query a destination (block)chain *B* whether a certain transaction *tx* has occurred on some source (block)chain *A*. The ability to verify transactions across blockchains in a way that requires no trust in a third party paves the way for cross-blockchain applications such as cross-blockchain token transfers [3].

In our prior work [5], we described the underlying concepts of our proposed blockchain relay and implemented these concepts in a first proof-of-concept prototype for Ethereum-based blockchains.[2] However, the devised prototype still needs to be extended before it can actually be leveraged for applications like cross-blockchain token transfers. In particular, since the prototype relies on third parties to relay block headers from the source chain to the destination chain and to dispute any illegal block headers arriving at the destination chain, an incentive structure needs to be in place to motivate these third parties to participate.

Further, in order for the proposed blockchain relay to be useful for cross-chain verifications, it needs to be continuously kept up-to-date with the newest block headers from the source chain. However, submitting block headers incurs financial cost. Hence, depending on the block interval of the source chain, keeping the prototype up and running can become rather expensive. As such, a cost analysis is necessary to get an idea of the operational cost of the prototype. The results of the analysis can then be used to derive concrete parameter values for the incentive structure.

As such, in the work at hand, we provide a) a detailed description of the prototype's incentive structure and b) a preliminary analysis of the operational cost.

To this end, Section II briefly recaps the concepts of blockchain relays in conjunction with on-chain SPVs, Section III provides detailed information on the incentive structure, and Section IV provides the cost analysis. The next steps of TAST are outlined in Section V. Finally, Section VI concludes the paper.

II. Recap: White Paper VI

In [5], we described the concepts of our proposed blockchain relay. The relay leverages on-chain SPVs to enable a destination chain to reliably answer queries about the state of a source chain, e.g., whether a certain transaction exists on the source chain. This is achieved by closely replicating the source chain within the destination chain. Whenever a new block is appended to the source chain, clients relay this block to the destination chain. The destination chain validates the submitted block according to the validation rules of the source chain and if the validation succeeds, stores the block. However, storing each block completely on the destination chain is very expensive due to the limited overall storage capacity of blockchains. Instead, it is sufficient to only store succinct pieces of data representing full blocks—so-called block headers. These block headers contain enough information to verify the inclusion of a transaction within a block without storing the transaction data itself.

Furthermore, validating relayed block headers according to the protocol rules of the source chain on the destination chain can also be an expensive operation if, for instance, the necessary cryptographic primitives are not natively implemented on the destination chain. Hence, validating each submitted block header can cause high cost. To counteract this, the

White Paper, TU Wien; November 2019, version 1.0.

[1] http://www.dsg.tuwien.ac.at/projects/tast/

[2] https://github.com/pantos-io/go-testimonium

proposed relay uses an optimistic approach for validating block headers on the destination chain. Instead of performing a full validation for each submitted block header, each header is only partially validated where the expensive validation steps are omitted at first. Of course, this potentially opens the door for malicious behavior where clients submit invalid block headers to the destination chain. To prevent such behavior, clients have the opportunity to dispute any block headers they deem invalid. In case of a dispute, the full validation is carried out, subsequently detecting and then removing any illegally submitted blocks. This way, any illegal blocks are seeded out and the true state of the source chain can be re-established on the destination chain. Of course, until an invalid block is disputed, it exists on the destination chain and could potentially be used for illegal transaction verifications. As countermeasure, the destination chain assigns a "lock" period to each newly received block header of the source chain. Within this lock period, no transaction verifications are possible giving clients enough time to submit a dispute transaction.

Finally, to verify on the destination chain that a certain transaction has been included in the source chain, an on-chain SPV is carried out. A client sends a verification request to the destination chain of the form "Is transaction *tx* of block *b* part of the valid source chain?". Along with the verification request, the client sends a Merkle proof of membership [3]. After receiving the request, the destination chain performs two verifications. First, it verifies that the header of block *b* is actually a valid header of the source chain. Second, the Merkle proof certifying the inclusion of transaction *tx* in block *b* is verified. If both of these checks are successful, the destination chain can provide an affirmative answer to the client request without requiring native access to the source chain. Note that while the destination chain is completely decoupled from the source chain, the client triggering the transaction verification needs to have access to the source chain in order to construct the correct Merkle proof of membership. However, the information provided by the client can be completely validated on the destination chain and thus does not have to be trusted.

III. Incentive Structure

The relay scheme that we propose in [5] relies on clients continuously submitting block headers of the source chain to the destination chain as well as on clients disputing any submitted illegal block headers. Clients that submit or dispute block headers incur cost since they need to provide a fee for posting the respective transaction to the destination chain. To keep the system alive, an incentive structure has to be in place that compensates submitting and disputing clients for their efforts. Otherwise, clients have no incentive to participate. Thus, we propose an incentive structure that rewards clients for submitting and disputing block headers.

In order to compensate clients for disputing illegal block headers, clients that submit block headers are required to deposit a stake. As outlined in Section II, newly submitted block headers get locked for a predefined time period. A certain amount of the provided stake gets locked for the same period. While the stake is locked, it cannot be withdrawn and cannot be used for submitting further block headers. Thus, the total amount of stake of a client determines the number of block headers the client can submit simultaneously. After the submitted header has passed the lock period without a dispute, the submitter regains control of the corresponding amount of locked stake. If however a dispute is carried out and the subsequent complete validation of the respective block header fails, the client that triggered the dispute earns the locked stake of the client that submitted the header as well as any stake that was locked for any submitted block headers that succeed the illegal block header.

This kind of penalty discourages clients to submit illegal block headers since they risk losing their stake as long as there is at least one honest client participating in the system. In return, honest clients get motivated to dispute illegal block headers since they can earn a reward for their service. In order to sufficiently compensate disputing clients, the amount of stake locked for each submitted header must be higher than the cost of disputing a header:

$$\textit{required stake per block} > \textit{dispute cost} \tag{1}$$

To encourage clients to continuously submit block headers to the destination chain, we propose a fee model where a submitter receives a "verification fee", i.e., a small financial reward, every time a transaction inclusion verification takes place using one of the block headers that were submitted by the client. The verification fee has to be provided by the client requesting a transaction inclusion verification for a specific block header *b*. After the verification, the submitter of block header *b* is rewarded with the provided fee. Essentially, whether a client gets fully compensated for submitting a block header depends on the size of the verification fee, the number of verifications taking place on the specific block as well as the cost for submitting a block header:

$$\textit{fee} \times \textit{no. of verifications} > \textit{submission cost} \tag{2}$$

The minimum verification fee can thus be calculated as the submission cost of a block header divided by the number of verifications taking place on the submitted block header:

$$\textit{fee} > \frac{\textit{submission cost}}{\textit{no. of verifications}} \tag{3}$$

With an incentive structure in place, clients are encouraged to keep submitting and disputing block headers, thus keeping the system alive and healthy. In the following section, we provide a preliminary analysis of the operational cost of the proposed relay scheme.

IV. Cost Analysis

A. Stake and Verification Fee

In [5], we introduced a proof of concept implementation of the proposed relay scheme for Ethereum-based blockchains. The effort required by transactions in Ethereum are measured

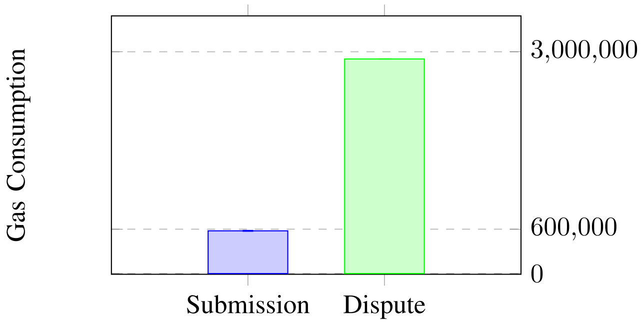

Figure 1: Avg. Gas Cost for Submitting and Disputing Block Headers

in gas. That is, each operation (e.g., accessing storage) in Ethereum costs a certain amount of gas. When posting a transaction, a client can decide how much Ether (ETH) to pay for each unit of gas. The higher the price per unit of gas, the higher the probability of the transaction being included within the next immediate block but the higher the total cost of the transaction. Vice versa, transactions with a lower gas price are less expensive, but run the risk of being bypassed by miners. As such, we can objectively measure the cost of submitting and disputing block headers in the amount of gas required by the transaction. If we want to find out a client's cost in ETH, we also need to take the gas price into consideration.

To get an idea for specific values for the stake and verification fee for the incentive structure described in Section III, we measured the actual gas consumption for submitting and disputing block headers. The measurement was repeated 100 times and was performed on a private Ethereum blockchain[3]. Figure 1 shows the average gas consumption of block header submissions and disputes. The average gas consumption of submission is just below 580,000 gas per block header with a standard deviation of about 5,000. Average gas consumption for disputing a block header is much higher at about 2.9 million gas with a negligible standard deviation of 580. We can now use these values to calculate preliminary parameters for the verification fee and the stake. The recommended gas prices for the Ethereum main chain at the time of writing[4] are 1 GWei (= 1,000,000,000 Wei) for transaction confirmations under 30 minutes, 3 GWei for confirmations under 5 minutes, and 10 GWei for confirmations under 2 minutes. Table 1 shows the cost in ETH. We can conclude that the required stake per block for submitting clients should be higher than 0.0029 (0.0087, 0.029) ETH for a gas price of 1 (3, 10) GWei.

Similarly, we can calculate the verification fee by additionally taking the number of expected transaction inclusion verifications per block header into account. For instance, with a fee higher than 0.0006 ETH, one inclusion verification would be enough for the submitter to be compensated for the cost of submission, provided the submitter used a gas price of 1 GWei. With an exchange rate of 156.99 EUR per ETH for the Ethereum main network at the time of writing, the fee of one transaction inclusion verification would amount to about 0.10 EUR. Figure 2 displays an overview of the minimum verification fee required with the verification request rate as parameter. Naturally, with more verifications per block (per minute, per hour), the required fee decreases proportionally. Ideally, the verification fee can be adjusted according to the actual number of verification requests.

Table 1: Submission and Dispute Cost per Block Header

Gas Price (GWei)	Submission Cost (ETH)	Dispute Cost (ETH)
1	0.0006	0.0029
3	0.0017	0.0087
10	0.0058	0.029

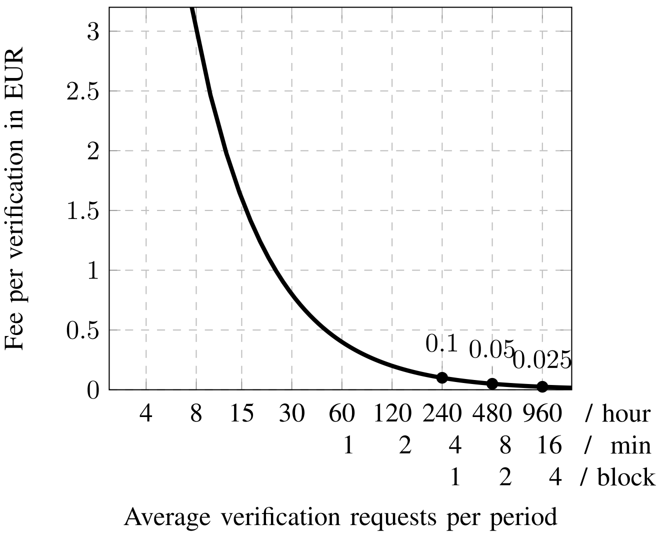

Figure 2: Fee per verification in relation to verifications per period.

B. Operational Cost

As seen in Fig. 1, submitting block headers without full validation cost about 580,000 gas, while the full validation alone costs about 2.9 million gas. Hence, fully validating block headers at submission, as done in traditional blockchain relays, would cost around 3.5 million gas. This gives a clear indication about the benefits of the devised approach as optimistically accepting block headers is about six times cheaper than the traditional approach. However, the cost savings of the optimistic approach become even more evident when considering longer time periods.

To keep the proposed relay scheme up-to-date, all new block headers of the source chain need to be relayed to the destination chain. Hence, clients need to regularly submit these block headers to the destination chain. If we consider an average block time of the source chain of 15 seconds and consider the Ethereum main chain as destination chain with the exchange rate 156.99 EUR, we can approximate the operational cost of the proposed scheme. Table 2 and Table 3 display the approximate operational cost when fully validating each submitted block header and when optimistically validating block headers, respectively. For instance, fully validating each

[3] https://www.trufflesuite.com/ganache

[4] 8 November 2019, https://ethgasstation.info/

Table 2: Operational Cost with Full Block Header Validation

Gas Price (GWei)	Cost/Submission (EUR)	Cost/Hour (EUR)	Cost/Day (EUR)	Cost/Year (EUR)
1	0.55	131.12	3,146.85	1,132,866.33
3	1.64	393.36	9,440.55	3,398,599.00
10	5.46	1311.19	31,468.51	11,328,663.34

Table 3: Operational Costs with Optimistic Block Header Validation

Gas Price (GWei)	Cost/Submission (EUR)	Cost/Hour (EUR)	Cost/Day (EUR)	Cost/Year (EUR)
1	0.09	21.77	522.46	188,086.59
3	0.27	65.31	1,567.39	564,259.76
10	0.91	217.69	5,224.63	1,880,865.87

submitted block header with a gas price of 10 GWei would lead to annual cost of 11.32 Mio. EUR whereas submitting block headers without a full validation would only cost about 1.88 Mio. EUR annually—a cost reduction of 9.44 Mio. EUR. Of course, depending on the average block time of the source chain, the exchange rate of the destination chain and the chosen gas price for submitting block headers, the cost savings would deviate proportionally.

V. Next Steps

With the basic incentive structure established and already implemented in the prototype, the next steps of the TAST research project will be two-fold. First, it is planned to further improve the prototype. Second, the prototype will be used as basis for the development of cross-blockchain tokens.

A. Further Improvements

As mentioned above, a first prototype of the proposed relay scheme has been developed. While this theoretically enables the confirmation of transactions across blockchains in a completely decentralized manner, in order to function correctly, the scheme needs to be continuously updated with block header information from the source chain. As we have seen in Section IV, this can cause significant financial cost. In future work, we will continue to seek ways to reduce these cost. For instance, it might be cheaper to submit block headers of the source chain to the destination chain as batch instead of submitting block headers individually. Further, we will explore ways in which the concepts employed by the prototype can be implemented on other blockchain platforms in order to bring trustless cross-blockchain transaction confirmations to a wide range of different blockchain networks.

B. Cross-Blockchain Token Transfers

The TAST project aims to enable a cross-blockchain token [1]. Ideally, such a token enables users to choose on which blockchains they keep their tokens with the possibility to freely transfer tokens between blockchains. This way, users are not locked-in by particular blockchains and are able to take advantage of new blockchain technologies offering novel capabilities. Furthermore, the distribution of assets across the participating blockchains can give an indication about the significance of a particular blockchain [4].

Cross-blockchain token transfers should only be successful (i.e., the specified amount of tokens is created on the destination chain) if the same amount of tokens has been burned (i.e., destroyed) on the source chain. If this was not the case, tokens could effectively be created out of nothing. The developed prototype enables clients to perform on-chain SPVs, e.g., users can query the destination chain whether or not a particular transaction exists within a particular source chain without requiring any trust in a single entity. As such, the prototype can build the basis for the development of the envisioned cross-blockchain token where the prototype is used to confirm the existence of a particular "burn" transaction on the source chain before (re-)creating the burned amount of tokens on the destination chain. Hence, one of the next immediate steps within TAST will be the development of a prototypical implementation of such a cross-blockchain token.

VI. Conclusion

The ability to perform on-chain SPVs in order to confirm the inclusion of transactions across blockchains is crucial for enabling blockchain interoperability. In the last TAST white paper, we proposed and implemented a relay scheme capable of on-chain SPV. In this paper, the prototype was extended by an incentive structure which is crucial for keeping the prototype alive. Further, we conducted a preliminary analysis on the operational costs of the prototype. With the incentive structure in place, the prototype can now act as basis for the development of cross-blockchain token transfers as envisioned by TAST.

Disclaimer

Information provided in this paper is the result of research, partly based on publicly available resources of varying quality. Popular use of cryptocurrencies includes investment and speculation on price developments of currencies and assets. The goal of this paper is to describe technical aspects relevant for the TAST research project. Economic considerations or future price developments are therefore not discussed. Technologies are described from a purely technical point of view. Therefore, the information in this paper is provided for general information purposes only and is not intended to provide advice, information, predictions, or recommendations for any investment. We do not accept any responsibility and expressly disclaim liability with respect to reliance on information or opinions published in this paper and from actions taken or not taken on the basis of its contents.

Acknowledgment

The work presented in this paper has received funding from Pantos GmbH within the TAST research project.

References

[1] M. Borkowski et al. *Towards Atomic Cross-Chain Token Transfers: State of the Art and Open Questions within TAST*. 2018. URL: http://dsg.tuwien.ac.at/projects/tast/pub/tast-white-paper-1.pdf. White Paper, Technische Universität Wien. Version 1.2. Accessed 2019-11-04.

[2] M. Borkowski et al. *Cross Blockchain Technologies: Review, State of the Art, and Outlook*. 2019. URL: http://dsg.tuwien.ac.at/projects/tast/pub/tast-white-paper-4.pdf. White Paper, Technische Universität Wien. Version 1.0. Accessed 2019-11-04.

[3] P. Frauenthaler et al. *Towards Efficient Cross-Blockchain Token Transfers*. 2019. URL: http://dsg.tuwien.ac.at/projects/tast/pub/tast-white-paper-5.pdf. White Paper, Technische Universität Wien. Version 1.0. Accessed 2019-11-04.

[4] S. Schulte et al. "Towards Blockchain Interoperability". In: *BPM Blockchain and Central and Eastern Europe Forum*. Vol. 361. Springer. 2019, pp. 1–8.

[5] M. Sigwart et al. *Towards Cross-Blockchain Transaction Verifications*. 2019. URL: http://dsg.tuwien.ac.at/projects/tast/pub/tast-white-paper-6.pdf. White Paper, Technische Universität Wien. Version 1.0. Accessed 2019-11-04.