Project Depolymerization: Tokenization of Blockchains

Antoine d'Aligny
student
EFREI Paris
Villejuif, France
antoinedaligny@outlook.fr

Emmanuel Benoist
School of Engineering and Computer Science
Bern University of Applied Sciences
Biel, Switzerland

Christian Grothoff
School of Engineering and Computer Science
Bern University of Applied Sciences
Biel, Switzerland

***Abstract*—GNU Taler is an electronic payment system implemented as Free Software. The goal of this project is to enable payments with blockchain-based cryptocurrencies in GNU Taler.**

Blockchain-based cryptocurrencies come with their own special set of challenges, such as lack of finality, unpredictable delays and fees in transactions. Our work analyzes the limitations that arise from using a blockchain as a settlement layer for GNU Taler and describes ways to mitigate their impact. By proving that blockchains can be used as a settlement layer for GNU Taler, we show that it is not only capable of handling bank money, but also widely used cryptocurrencies.

For cryptocurrencies owners, this integration offers a new solution for instant and low-cost payments that can scale beyond blockchains limitations while preserving or enhancing privacy.

I. Introduction

Today, popular cryptocurrencies like Bitcoin [1] and Ethereum [2] are not useful for electronic payments in everyday life (say to buy bread, pay for a beer or a snack in a vending machine). There are three main reasons for this. First, the distributed character and the validation of blockchains do not allow fast transactions: a transaction in Bitcoin or Ethereum has to be entered in a block and then one has to wait for a certain number of blocks for this transaction to be considered valid. To have a serious validation, it may be necessary to wait for one hour [1].

Second, the block size and number of blocks mined are two factors limiting the amount of transactions per second that distributed cryptocurrencies can perform. The number of transactions per second is currently small (3 to 4 for Bitcoin and 20 for Ethereum). [3] This makes it impossible to use these two systems as a means of payment in the daily life of users, since the systems simply cannot handle the transaction rates required by millions of users. In practice, the transactions that are successful are those with the highest payment fees attached. Which brings us to the third reason: the effective payment fees are too high for small purchases, as the fees may even exceed the value of the purchase, especially for small purchases like snacks from a vending machine.

We developed a way to use the GNU Taler electronic payment system as a second-layer solution for Distributed Ledger Technology (DLT) based cryptocurrencies. The GNU Taler system is based on cryptographic tokens distributed by an exchange that can be used for instant payments. Users pay the merchants using digital tokens that were blindly signed by an issuing payment service provider, called an exchange. Merchants receiving GNU Taler payments need to redeem the digital tokens at the exchange. Merchants can either receive fresh tokens, or the exchange can aggregate many off-chain micropayments so that the merchant would receive one bulk transfer for many micropayments on the blockchain.

Our solution allows to use the GNU Taler system to make payments in Bitcoin and Ethereum. An exchange is created, to which the user transfers an amount in cryptocurrency. In return, the user receives (blindly signed) tokens corresponding to this amount and can spend them at will in any store that accepts these tokens. The transaction is then instantaneous: the exchange operator instantly confirms the validity of the tokens by checking its signature and ensuring that tokens are not double-spent. The merchant can then immediately run the business logic, and freely determine when the payment is to be aggregated and converted into an on-chain transaction.

A key issue with any layer-two solution is that the merchants must have some confidence that the operator can be trusted. GNU Taler includes an auditor component which can be used to provide real-time audits of an exchange operator. By setting up one or more auditors that have both access to the exchange's database and see the on-chain transactions, this trust issue can be mitigated.

We give some background on the GNU Taler payment system in Section II. Then in Section III we present the Depolymerization system, which allows to transform Bitcoin and Ethereum assets into GNU Taler tokens and vice versa. We also present in Section IV the different specificities of our system allowing to solve the inherent problems of blockchains.

II. Background: GNU Taler

The GNU Taler system has been designed as an electronic payment system for fiat currencies (Figure 1). [4] Customers who want to use GNU Taler use a Taler wallet. To get tokens into their wallet, customers make a wire transfer to an exchange. In response, the exchange issues tokens to the users who store them in their wallet.

The GNU Taler system is based on four types of entities. The consumers who want to buy goods from merchants. An exchange that signs the tokens into existence, and receives

deposited tokens from merchants. Finally, the exchange is supervised by one or more auditors who check that all transactions are regular and that the exchange has adequate funds in escrow to meet its obligations from tokens in circulation.

When users need tokens, they make a money transfer to the exchange. Then they generate tokens and have them signed by the exchange. The signature is blind, so the exchange does not know the public key of the tokens it has signed [5].

The user spends the tokens at a merchant by signing a digital contract with the private keys of one or more tokens. The merchant must then present the tokens to the exchange, which verifies the signature and checks against double-spending. Here, the exchange cannot determine which consumer is spending the token (due to the blind signature). If the tokens are valid, the merchant is credited with the amount of the received tokens.

III. Depolymerization Architecture

The Depolymerization project consists of a banking interface that connects an exchange to Bitcoin or Ethereum as the underlying settlement layer. The system allows owners of digital currencies to deposit this currency in an exchange, get tokens in exchange, and then to pay with these tokens. The (micro) transactions between customers and merchants are then done within the GNU Taler system and not on the blockchain. Figure 2 shows how Depolymerization allows funds to be transferred to GNU Taler and then transactions to be made off-chain.

The Depolymerization system consists of several components. Figure 3 shows the interactions between the Taler exchange, the Depolymerization *Wire Gateway*, the Depolymerization *DLT Adapter*, and the DLT Full Node. Here, the Taler exchange represents the previously existing Taler payment system, specifically the `taler-exchange-wirewatch` and `taler-exchange-transfer` components that are traditionally interacting with the banking system. The Depolymerization Wire Gateway is simply a REST API that presents the Taler exchange with a view of the blockchain that (largely) matches the expected semantics of a traditional settlement layer. At the center of this architecture is a relational database (PostgreSQL) which collects the incoming (credit) and outgoing (debit) transactions of the system. The DLT Full Node is the existing Bitcoin or Ethereum "full" client (`bitcoind`[1] or `geth`[2]). The Depolymerization DLT Adapter is responsible for DLT-specific adaptations.

When users want to withdraw tokens, they have to credit the exchange's account on the respective DLT. As all users' money is transferred to the same address of the exchange, each user must add information allowing the exchange to associate the incoming funds with the originating user's wallet. To do this, the customer sends a transaction that contains both the money and a public key of the user's wallet in transaction *meta-data*. This public key will be used to validate requests for issuing fresh tokens. While meta-data is easy to add in Ethereum, for Bitcoin we use a multi-output transaction. Here, the main output is our account while the other outputs (whose transaction values are negligible) correspond to an ephemeral public key that identifies the user's wallet.

When customers want to withdraw tokens corresponding to the transfer they made, they sign the requests for new tokens with the private key corresponding to the public key indicated during the transfer. The Taler exchange retrieves the withdrawal request, checks that the public key used during the money transfer matches the signature used for the request, and finally blindly signs the new tokens and sends the signature back to the wallet.

The Taler exchange is also responsible for redeeming tokens that were spent at merchants. If and when a merchant decides to be credited on-chain, the exchange will instruct the Depolymerization Wire Gateway to transfer the funds from its DLT escrow account to the DLT address indicated by the merchant.

IV. Blockchain-specific Problems and Mitigations

In this section we describe how the Depolymerization system addresses Blockchain-specific problems.

[1]https://bitcoincore.org/
[2]https://geth.ethereum.org/

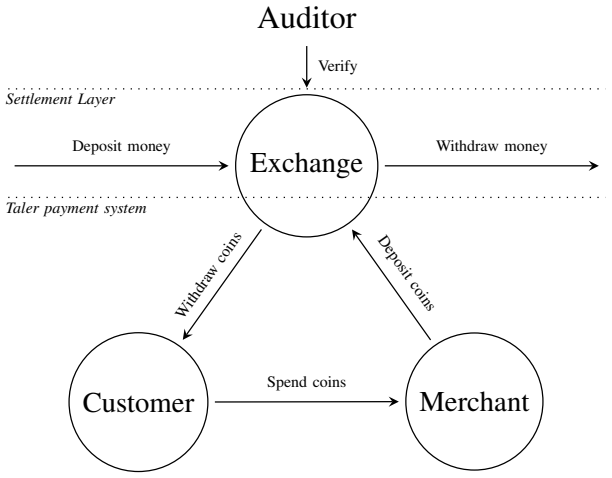

Fig. 1. GNU Taler overview

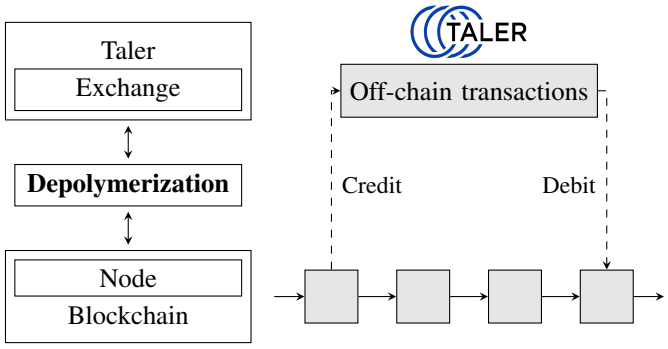

Fig. 2. Blockchain settlement layer with Depolymerization.

A. Forks

A big risk for an exchange operator is to believe that an incoming on-chain transaction was final, allow the wallet to withdraw tokens, and later have the original on-chain transfer reversed.

This can happen with DLT systems in the case of a fork. If a transaction is included in a block (for instance D1 in Figure 4), the exchange might believe that it is durable and final. But if a fork happens that does not contain D1, the transaction may not appear in the new blocks of the ultimately authoritative longest chain. Moreover, we can also have in one of the new blocks (for instance D2 in Figure 4) a conflicting transaction that uses the money at the origin of our transaction for a different transfer. This would prevent the original transaction from ever being committed on the longest chain.

Since the blindly signed tokens cannot easily be identified (because they were signed *blind*), the exchange could lose money. The canonical solution to the problem is to wait a certain number of blocks before validating a transaction. In Depolymerization, the number is set depending on the DLT and the history of forks observed by the system. The resulting delay only impacts the initial issuing of coins, and not the off-chain transactions.

If the Depolymerizer detects that a fork has reverted an incoming transaction, it suspends operations until the reverted transactions appear in the fork *or* until the operator manually intervenes to resolve the situation.

One such possible intervention enabled by GNU Taler is for the exchange to revoke the affected denomination keys (i.e. the keys used for blind signature of one type of coins), and to request all wallets to reveal the blinding factors of tokens in circulation that correspond to those denominations. This would allow the exchange to re-issue the tokens that were from on-chain transfers that were not reversed. However, in theory it might be too late, as the token might also have already been spent. Still, this remains a possible mitigation for a Depolymerizer operator in case the canonical solution was inadequate.

B. Fees are Bids

Due to the limited rate for on-chain transactions, it is possible for cryptocurrency transactions to get stuck for a long time. Especially if the transaction fee was set too low, it is even possible that transactions effectively never make it out of the pending transaction pool onto the main chain.

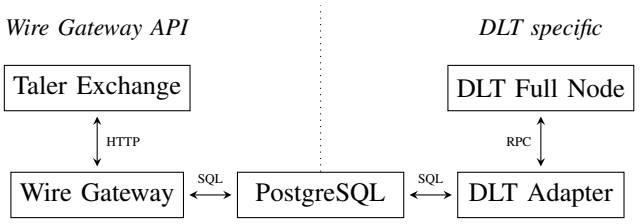

Fig. 3. Depolymerization architecture.

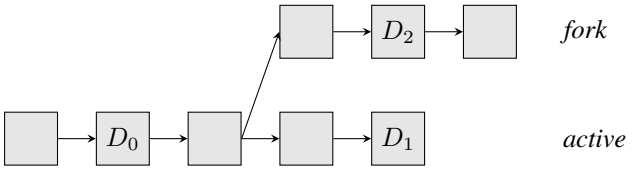

Fig. 4. Blockchain fork

This is problematic when merchants expect to be credited in a timely manner. Depolymerizer keeps track of pending transactions and identifies those that are taking an excessive amount of time to mine. For such stuck transactions, it eventually replaces the transaction [6] with one where the fee was increased to bump its mining priority. Since the process of replacing transactions is expensive, acceptable delays and transaction fees are configurable.

C. Tiny Amounts

The GNU Taler amount format is based on RFC 8905 [7]. It allows up to 2^{53} unit and 8 decimal digits. This format is perfectly suited for Bitcoin where the maximal amount is 21 million bitcoins and the smallest unit being the Satoshi, one Satoshi being worth 10^{-8} Bitcoin. However, the smallest unit of Ether is the Wei, with one Ether being worth 10^{18} Wei. The amount of Ether in circulation continues to grow without a cap, with over 119,000,000 Ether in circulation at the time of writing those lines. Therefore, it is not possible to represent all Ethereum amounts with the current format.

A standard Ethereum transaction requires 21'000 units of gas [3]. The average gas price is currently around 30 GWei. Therefore, a standard transaction costs about $63 \cdot 10^{18}$ Wei in transaction fees. Since the transaction fee is so high, even if we truncate amounts to 10^{-8} Ether (10^{10} Wei), we can still represent any amount that can be practically wired. Thus, in Depolymerizer, all Ether amounts must be multiples of $10^{10} Wei$.

V. Advantages

The Depolymerization system allows users to turn Bitcoin or Ethereum funds temporarily into tokens. The tokens are quickly exchangeable and can be used for daily expenses.

While the number of transactions on blockchains is limited by the size of the blocks, their frequency and thus the size of the blockchain, the GNU Taler payment system has no intrinsic limit. Marco Boss [8] has successfully configured a GNU Taler exchange to process over 23,000 token transactions per second. Since each transaction uses a limited number of tokens (on average, half of the binary logarithm of the number of currency units spent) an exchange can therefore be expected to process at least 2,300 transactions per second for typical amounts. This is comparable to the Visa network, which is said to perform about 1'700 transaction per second globally. [3], [9]

[3]https://ethereum.org/en/developers/docs/gas/#post-london

VI. Related work

Blockchain-based systems lack a central instance to validate a transaction, making instantaneous transactions impossible as an expensive distributed Byzantine fault-tolerant consensus protocol must be executed before transactions are confirmed. One way to work around this problem are layer-2 solutions like Lightning, which is an additional payment layer on top of Bitcoin. Its goal is to settle transactions faster without involving a full transaction on the blockchain every time that money is moved. Lightning works by establishing *payment channels* between two parties, where one or both parties "lock" an initial amount to the channel. Signatures communicated outside the blockchain then change how money is allocated between the two sides of the payment channel. Eventually a payment channel will be closed by submitting a multi-party signature of the latest allocation between the two parties to the Blockchain, releasing the locked money to the two endpoints according to the most recent allocation.

A payment can be *routed* through a network of multiple bidirectional channels. If channels Alice-Bob and Bob-Carol exist and have sufficient capacity, then Alice can send a payment to Carol over the route Alice-Bob-Carol. Routing payments with Lightning is thus contingent upon the existence and discovery of channels with sufficient capacity, forcing participants to lock significant amounts of Bitcoin in a channel, resulting in opportunity costs. The cost of operating a lightning node is prohibitive to an average user. As a result, Lightning basically re-introduces financial intermediaries (aka banks, except here not regulated) with the associated trend towards centralization [10]. Our work is thus a logical continuation and simplification of this trend: instead of a complex federated structure, we simply use a centralized payment system to provide virtually instant transactions, which also eliminates the need for customers to operate a node that needs to be permanently online.

Aside from scalability, Bitcoin and Ethereum also suffer from coins not being fungible, as they are traceable. As a result, freshly mined coins may be considered more valuable as they cannot possibly have been tainted by criminal transactions in the unspent transaction output's (UTXO) transaction history, which may result in coins being rejected by cryptocurrency exchanges or merchants. Mixing services for DLTs attempt to re-introduce privacy and thus fungibility, but only further taint a UTXO's history as it is clear that the coin was mixed. With Depolymerization, all tokens issued via GNU Taler have no transaction history, and are thus perfectly fungible.

VII. Future Work

While the GNU Taler exchange was recently extended to support wallet-to-wallet (peer-to-peer) payments, the GNU Taler wallet currently does not yet support this new feature. This is a major limitation in practice as it requires merchants to receive all payments on-chain eventually. Once GNU Taler wallets support direct wallet-to-wallet payments, it will become practical to do day-to-day transactions with Bitcoin or Ethereum.

Another concern is that in order to operate legally, a Taler exchange operator will typically be required to perform know-your-customer (KYC) checks. GNU Taler's cryptographic design allows in principle the identification of users withdrawing or receiving funds through the system. In a deployment with fiat money, a GNU Taler deployment can simply re-use the existing KYC processes used by the banks connected to the underlying settlement layer. However, with cryptocurrencies, the operation would typically be immediately global, which could create challenges for practical KYC. Furthermore, the non-fungibility of cryptocurrencies is expected to create problems for anti-money laundering, it will require defining a threshold for when UTXOs should be considered tainted before the Depolymerization system allows the wallet to withdraw tokens.

VIII. Conclusion

Contemporary cryptocurrencies are too slow and expensive for daily purchases and fail to meet the fungibility of cash. Thanks to Depolymerization, one can use GNU Taler to pay for services in real time with privacy, allowing merchants to deliver the goods without noticeable delay.

Acknowledgements

We thank Florian Dold and Sebastian Marchano for adding Bitcoin support to the GNU Taler wallet. This work was partially funded by a grant from Taler Systems SA.

References

[1] S. Nakamoto, "Bitcoin whitepaper," *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019)*, 2008.

[2] V. Buterin, "A Next-generation smart contract and decentralized application platform," 2013–2021. [Online]. Available: https://ethereum.org/en/whitepaper/

[3] D. Mechkaroska, V. Dimitrova, and A. Popovska-Mitrovikj, "Analysis of the possibilities for improvement of blockchain technology," 11 2018, pp. 1–4.

[4] F. Dold, "The GNU Taler system: Practical and provably secure electronic payments. phd thesis," Ph.D. dissertation, University of Rennes 1, 2019.

[5] D. Chaum, C. Grothoff, and T. Moser, "How to issue a central bank digital currency," in *SNB Working Papers*. Swiss National Bank, February 2021, no. 2021-3.

[6] D. A. Harding and P. Todd, "Opt-in full replace-by-fee signaling," Bitcoin Improvement Proposals, BIP 125, December 2015.

[7] F. Dold and C. Grothoff, "The 'payto' URI Scheme for Payments," RFC 8905 (Informational), RFC Editor, Fremont, CA, USA, Oct. 2020. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8905.txt

[8] M. Boss, "Gnu taler scalability: Measuring and improving the performance of gnu taler on grid'5000," B.S. thesis, Bern University of Applied Sciences, June 2022.

[9] D. Mechkaroska, V. Dimitrova, and A. Popovska-Mitrovikj, "Analysis of the possibilities for improvement of blockchain technology," , pp. 1–4, 11 2018, available at https://www.researchgate.net/publication/330585021_Analysis_of_the_Possibilities_for_Improvement_of_BlockChain_Technology [16.05.2022].

[10] J.-H. Lin, K. Primicerio, T. Squartini, C. Decker, and C. J. Tessone, "Lightning network: a second path towards centralisation of the bitcoin economy," *New Journal of Physics*, vol. 22, no. 8, p. 083022, aug 2020. [Online]. Available: https://doi.org/10.1088/1367-2630/aba062

Availability

An experimental public Depolymerization exchange is available at https://bitcoin.ice.bfh.ch/. To use the service, one only needs to install a GNU Taler wallet from https://wallet.taler.net/ and instruct it to use this exchange to withdraw coins.