PayFlow

Next Generation Crypto Payments

Jan Ole Ernst, Orlando Fraser, Kyle Duffy, Jessica Pointing

July 2023

1 Introduction

Self-Custodial payments are the 'OG' crypto use case however they have not reached the level of widespread adoption that members of the crypto community would have expected and hoped for. We believe the core reason for this is the fact that many recipients of payments do not want to receive crypto and are therefore dissuaded from offering it as payment option.

Additionally, despite the large and growing number of tokens that exist on blockchains, payment apps are very limited in the ones that they support. This cuts out the 100s of millions of dollars of value stored in smaller tokens from interacting directly with payment applications. Holders of these tokens can of course manually swap to a supported token before making a payment, however this is a cumbersome process for most people.

The ideal crypto payments app would allow the recipients to receive fiat to their bank accounts while the sender still can maintain a seemless web3 experience. The regulatory breakthrough that occurred recently to make this possible was the release of Monerium's EURe, which is the first fully regulated E-money released on blockchains. EURe can be burnt triggering an IBAN transfer to a specified bank account. EURe is more than one-to-one backed in high-quality liquid assets and is redeemable on demand. Unlike a bank, an Electronic Money Institution can only safeguard customer funds but not make loans. This sets EURe a level above Stablecoins when it comes to the associated risk. For more information on the differences between EURe and other stablecoins, refer to article here: https://monerium.com/blog/2023/what-is-emoney/.

We are excited by the recent release of Gnosis Pay that leverages Monerium, providing an integration of the E-money with a VISA debit card. However Visa fees may range between 1-3% of the total transaction cost which is an overhead we would rather do without. Using an IBAN payment directly allows this fee to be removed.

We built PayFlow as an attempt address the shortfalls existing in current infrastructure. We hope that this will lead to growth of the crypto payment ecosystem.

2 Implementation

Payflow allows senders to use any token in their wallets to settle an invoice payment. This provides maximum flexibility to the wide range of tokens and their associated communities. However in all cases, the recipient will receive an IBAN transfer to their account.

The payment flow begins with the recipient generating an invoice QR code via the dedicated web service. This QR code can either be visibly shown to the sender for them to scan with a camera connected to a mobile wallet, or alternatively it can be sent to a remote sender.

The sender scans the QR code invoice which will redirect them to their wallet. QuickNode's Token API is then queried to retreive the senders token balances and display them in the UI. The sender can then select which token they would like to use for the payment.

Although we do support all the chains that Monerium supports (Gnosis Chain, Polygon, and Ethereum) we recommend using Gnosis Chain due to the deepest liquidity present for the EURe token on there.

Once the payment token is chosen, the swap to EURe occurs through the 1 Inch Fusion API. The Engine revolutionizes the execution of swaps on decentralized exchanges, offering a new type of decentralized order matching approach that uses the Dutch auction model, while being based on market rates and taking price impact into account. This leads to more optimal pricing for tokens than conventional approaches. This is particularly important for less liquid tokens as slippage can become a greater issue.

Finally, the Monerium API is invoked via the Sender's account. This burns the EURe tokens and triggers the IBAN transfer to the recipient. Desipte there being some latency in the IBAN transfer, the On-Chain burn transaction occurs instantly and therefore its status can be used to check the finality of a payment. This is because there is no way for the sender to revert the process once the burn has occured.

Additionally, we provide an option for recipients to attest to a copy of their payment invoice On-Chain. This provides an immutable proof of the invoice's existence and can be used for claims against Monerium if settlement issues do arise. It is particularly valuable for slow bank settlements. We utilise the Ethereum Attestation Service for this procedure.

3 Outlook

In conclusion, we hope our novel offering can help address some of the current shortcomings of crypto payments, which may be the key to on-boarding the next billion users. Further directions that excite us the encorporation of an encrypted wallet to wallet messaging provider such as XMTP for the secure sharing of invoices.

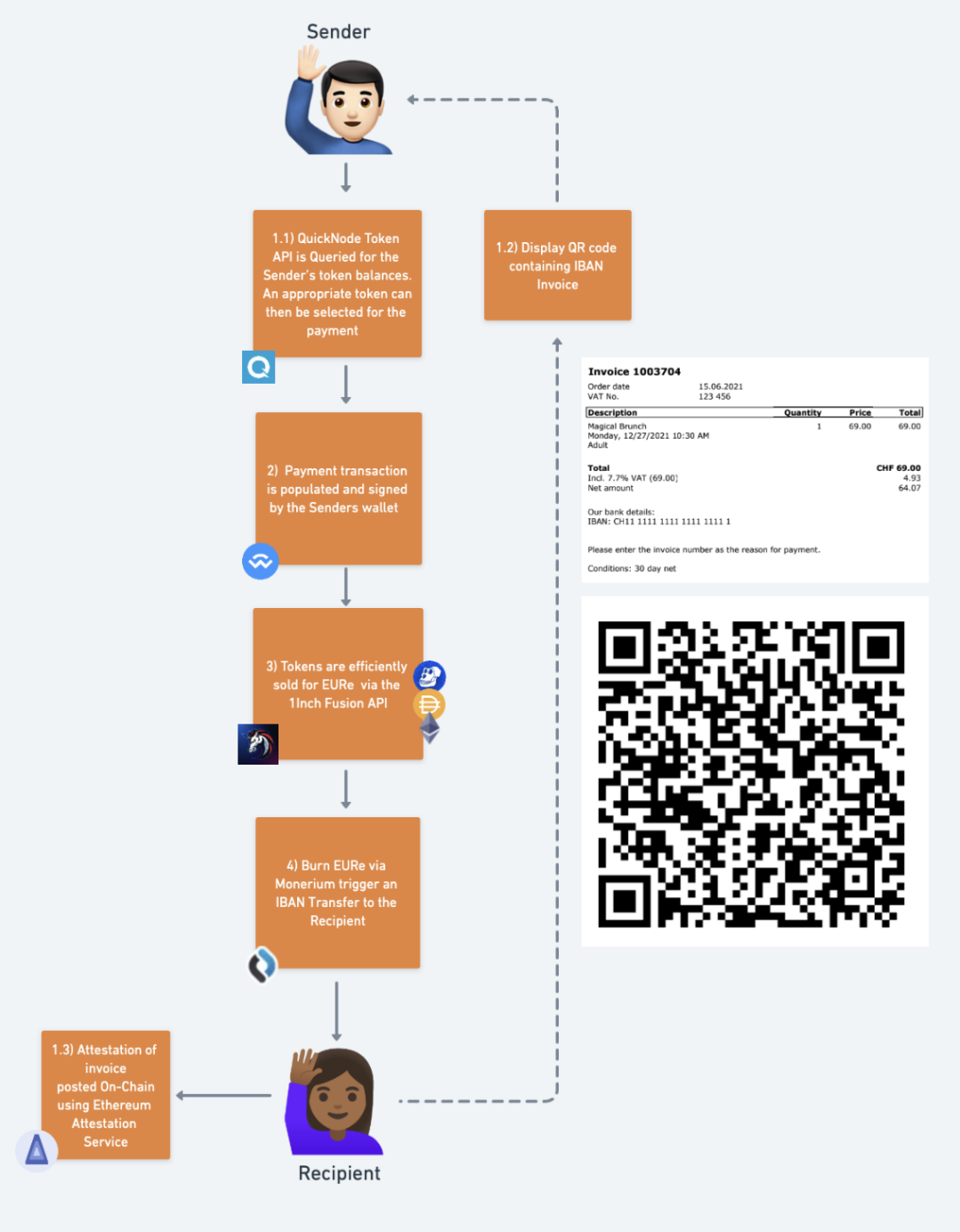

Figure 1: Payflow Usage flow chart. The Multi-stage process has been abstracted away from the senders and recipients, each only needing to perform a single action to carry out the payment. If the Invoice is known beforehand, such as in the case of a merchant payment, then no action is required from the recipient.