

Clocktower V1

An on-chain payment and subscription service

V. Hugo Marx and George P. Atkinson

June 2023

Abstract

Clocktower is a decentralized protocol for subscriptions and payments. Providers and subscribers collaborate off-chain for the initial set-up and third-party agents are financially incentivized to call the protocol contract regularly. This system allows for regular payments to be processed into the future with this V1 allowing up to daily granularity. This whitepaper will explore the economic mechanisms and code behind the protocol.

Introduction

As web-based services proliferate, subscription payment systems have become an important source of recurring revenue for digital content providers. Centralized payment services have reduced the friction of payments on the web, and have made traditional forms of payment (credit/debit/bank transfer) common and simple. However, this convenience comes at a price—online content and providers frequently pay more than 3% for this functionality¹ and these costs are passed to the consumer. Furthermore, payment platforms have become a critical beachhead for censorship of people and ideas on the web, inspiring some to leave popular crowdfunding platforms in favor of their own platforms.² While the major payment networks have generally remained neutral politically, they remain a potential choke-point for free speech and an open internet.

At the same time, we have witnessed a new type of currency layer evolve over the past decades: the cryptocurrency.³ These systems exist outside of national borders and live on distributed networks called blockchains. While many groups have experimented with payment systems on these networks, the problem of recurrent future payments and subscriptions has not yet been adequately addressed.

The problem is actually two-fold. The first part relates to the network fee, which on the Ethereum network is referred to as ‘gas’ and is paid in the native token. The gas price is always in flux, increasing and decreasing with the demand for blockspace on the network. Thus the most immediate issue is how to account for an unknown future gas price on a future transaction. The closely-related second issue is that a decentralized smart contract cannot act on its own—it must be triggered to take action. In a sense, it is unaware of time. This limitation makes it impossible to schedule actions in the future, as with a cron job in normal computing. Without the ability to schedule transactions in the future, common financial services like payroll, subscriptions, regular payments, and many others are impossible in these decentralized systems.

The Clocktower protocol solves these issues by creating EVM-compliant smart contracts that are polled at regularly timed intervals by other economically incentivized actors. Users will be able to schedule transactions at a future time of their choosing. By incorporating such features as subscriptions, future payments, batch transactions, reversible transactions and ERC20 compatibility, we hope to unlock the

potential of fintech and defi projects seeking recurrent payments while staying true to the principle of decentralization.

Goals

To further elaborate on the purposes and constraints of the protocol, we have developed the following goals:

Decentralization

While centralized payment facilitators are the norm, they bring with them a myriad of problems from high fees to censorship. But with a decentralized blockchain contract there is no point of failure, no censorship and no arbitrary gatekeeping.

Immutability

A system that cannot be changed is a system that cannot be censored.

Easy of Use

In the past setting up your own subscription service has been too difficult for normal users. But with Clocktower, if you can use a decentralized app, you can create or join a subscription.

Inexpensive

Traditional payment networks have had the advantage of being able to charge high fees due to extreme costs of setting up your own network. But by building on the existing backbone of EVM compliant blockchains we believe we can eventually undercut the existing networks.

No Oracles

An oracle is a third party data source. Unfortunately, oracles have been manipulated to steal funds⁴⁵. This protocol will not use these data sources as they subject users to unnecessary risk.

Minimum tokens in contract

Hackers hack where the money is kept. Traditional contracts have become targets largely because they rely on the “vault” model where all value is stored within the contract. We seek to turn this model on its head by seeking to hold as little value as possible in the contract. This makes the contract less of a target and allows users to keep secure their own funds in their own wallets.

No protocol token

We believe a protocol should never need its own token to work. A token needed for functionality creates friction for the user when they have to convert it and can lead to inflationary tokenomics. If Clocktower ever issues its own token, it will be used solely for governance purposes.

Centered Header	Default Aligned	Right Aligned	Left Aligned
First	row	12.0	Example of a row that spans multiple lines.
Second	row	5.0	Here's another one. Note the blank line between rows.

Timing System

The Three Participants

1. The Subscriber
2. The Provider
3. The Caller
- 5.

References

1. Helcim.com Visa interchange rates usa. <https://www.helcim.com/visa-usa-interchange-rates/>.
2. Goggin, B. (2018). A top patreon creator deleted his account, accusing the crowdfunding membership platform of 'political bias' after it purged conservative accounts it said were associated with hate groups. <https://www.businessinsider.com/sam-harris-deletes-patreon-account-after-platform-boots-conservatives-2018-12>.
3. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>.
4. Chainalysis (2023). Oracle manipulation attacks are rising, creating a unique concern for defi. <https://blog.chainalysis.com/reports/oracle-manipulation-attacks-rising/>.
5. Afser, Z. (2021). <https://hackernoon.com/how-dollar100m-got-stolen-from-defi-in-2021-price-oracle-manipulation-and-flash-loan-attacks-explained-3n6q33r1>.