# Clocktower V1

An on-chain payment and subscription service

Hugo Marx and George 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 functionality (helcim.com, n.d.) 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 platorms in favor of their own platforms (Goggin 2018). 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 (Nakamoto 2008). 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 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.

## Timing System

The Ethereum blockchain is like a giant decentralized clock, currently creating a block every twelve seconds. For each node, seconds matter, as they go through the task of creating blocks and gossiping them to the network. Its therefore ironic that even with this elaborate timing mechanism smart contracts are unable to know what time it is unless asked, like a person with an expensive watch who can't look down at it unless told to do so.

There are many ways to measure time in a scheduling system, the most common being Unix Epoch time which has been incrementing seconds since Thursday January 1st 1970 0:00. However, polling the contract every second would be too expensive and inefficent in the context of subscriptions and payments.

Another option would be using Ethereum blocks themselves as our time increment. Blocks are sometimes used to represent moments in time on Ethereum based systems. The problem with this approach is that there is no guarantee that a block will be set at twelve seconds in the future and one of the critical goals of Clocktower is to eventually be able to schedule transactions years into the future.

The situation is further complicated when considering that timed transactions need to be set at standard increments. But these increments, or time triggers as we call them, have differing scopes. For instance, a weekly subscription needs to be scheduled for a day of the week while a monthly subscription needs a day of the month. And not every month has the same number of days.

With this in mind we have chosen the following standard time trigger ranges that can represent the most common schedules:

- Future Transactions – Unixtime / 3600 (Unix Hours)
- Weekly Subscriptions – 1 - 7 (Weekdays)

- Monthly Subscriptions – 1 - 28 (Day of Month)
- Quarterly Subscriptions – 1 - 90 (Day of Quarter)
- Yearly Subscription – 1 - 365 (Day of Year (not indcluding leap days))

## References

Goggin, Benjamin. 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." 2018. https://www.businessinsider.com/sam-harris-deletes-patreon-account-after-platform-boots-conservatives-2018-12.

helcim.com. n.d. "Visa Interchange Rates Usa." https://www.helcim.com/visa-usa-interchange-rates/.

Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." 2008. https://bitcoin.org/bitcoin.pdf.