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.

1. 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.

2. 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 arbitraty 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 funds (Chainalysis 2023) (Afser 2021). 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 soley for governance purposes.

3. Timing System

Clocktower

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. Unfortunately, polling a smart contract every second on a public blockchain would be too expensive and inefficent in the context of subscriptions and payments. Furthermore, the EVM currently creates blocks ever 12 seconds, so measuring times less than block size are not really possible.

What about using Ethereum blocks themselves as our time increment? In addition to only being slightly more efficient than the one second interval, there is no guarantee that a block will be set at twelve seconds in the future. One of the goals of Clocktower is to allow transactions to be scheduled years into the future, and a change in the block production interval could cause significant problems around future transaction timing. In order to keep the system as resilient as possible

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

Afser, Zaryab. 2021. 2021. https://hackernoon.com/how-dollar100m-got-stolen-from-defi-in-2021-price-oracle-manipulation-and-flash-loan-attacks-explained-3n6q33r1.

Chainalysis. 2023. "Oracle Manipulation Attacks Are Rising, Creating a Unique Concern for Defi." 2023. https://blog.chainalysis.com/reports/oracle-manipulation-attacks-rising/.

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.