

# Litepaper

Interlock Team

2021-8-4

## Contents

<b>1</b>	<b>Introduction: Trust, Security, and Privacy</b>	<b>1</b>
<b>2</b>	<b>Security</b>	<b>2</b>
<b>3</b>	<b>Improving Privacy and Security with Decentralization</b>	<b>2</b>
<b>4</b>	<b>Decentralizing Security with Ethereum, Solana, Airlock</b>	<b>2</b>
<b>5</b>	<b>User Incentive Structure</b>	<b>3</b>
<b>6</b>	<b>Emission Schedule</b>	<b>3</b>

## Introduction: Trust, Security, and Privacy

Trust is the cornerstone of prosperity and innovation — it facilitates interaction and exchange between people. Most waves of progress arose from discovering social and technological means to *scale up* trust. Everything from religion to education to banking to law to trade-unions and so on, has helped scale mutual trust between people. All of these mechanisms for promoting trust depend on centralized institutions — instead of trusting every individual, people could trust intermediaries like their bank or government. The explosive growth of the internet has also caused people to, once again, outsource their trust to central institutions. These institutions, however, exhibit many of the same flaws as their predecessors — namely, they become increasingly corrupt and increasingly exploitative, as their revenue-growth inevitably declines.

The Interlock Network leverages — among other things — the latest Blockchain Technology to achieve decentralized and resilient trust on the Web. While the early Web was the most democratic that the Web has ever been, it was quite small. Growth exploded, however, when Web2.0 came around, effectively democratizing and globalizing *participation* on the Web. The darkside of Web2.0 is that it sustains itself by data-mining and selling their users' personal information, in addition to optimizing their feeds and search-results to keep users engaged and clicking on advertisements. This state of affairs is a clear *perversion* of the original vision, ideal, and promise of the Internet and Web. The next evolution of the Web — the blockchain-powered **web3** — can correct the course and re-democratize the web without sacrificing its accessibility.

## Security

The mass onlineing of people during the web2 era has created a target-rich environment for cyber-criminals, scammers, and high-tech-grifters. While people have to deal with exploitative online service providers and social networks — that seek to exploit their attention — they also have to deal with rapacious, anonymous online criminals — that seek to exploit their bank-accounts and credit-cards. A huge part of the problem is that the wealthiest technology companies cannot justify the costs of securing their own users, as securing them necessarily causes disruptions to their advertising-revenue stream and disruptions to their personal-data-marketplaces — which are often frequented by criminals, and nation-state-actors.

The insecurity of the internet-user — whether browsing from home, from work, or on-the-go — has reached pandemic proportions.

- **75 percent** of orgs experience phishing attack every year
- **74 percent** of the attacks are successful
- **34 percent** of fraud involved collusions between company employees and scammer
- **24 percent** involves employees as the source
- **3.86 million** dollars is cost of a single breach
- **50 percent** of recipients open phishing emails and click on the link
- **28 percent** of phishing attacks are targeted

Todo maybe make these stats graphical.

## Improving Privacy and Security with Decentralization

There is an unintentional, but mutually-supporting, dynamic between the corporate online platforms that violate our privacy and the criminal online grifters that violate our security. Interlock believes that both privacy and security can be improved by moving *trust* away from the center of the network (i.e. Facebook, Google, etc) to the *edges* of the network (i.e. directly into people's browsers and onto the blockchain).

## Decentralizing Security with Ethereum, Solana, Airlock

Security is a very difficult problem, and while much of the blame can be directed at the incentives of large tech corporations, some of it can also be directed at users feeling inconvenienced by security, for no observable benefit. Just as nobody wants to brush their teeth three times a day, nobody wants to jump through multiple security-hoops and fight with their security tools to enjoy the internet. Good and unintrusive security tools also face the *leaky-roof-problem* — just as people usually do not notice the roof on their home until it starts leaking, people do not notice security tools until they fail to prevent a breach.

Interlock takes a two-pronged approach to solving the problem — we attack the problem in the browser and on the blockchain.

We secure users' browsers from phishing, and other kinds of attacks, with a — uBlock-based — browser extnesion called Airlock. In addition to block ads, the extension uses advanced

heuristics to detect phishing pages and scam-websites and prevents users from entering any sensitive information like passwords or usernames. While only mildly intrusive, we seek to motivate users to install and use extension by linking it to a crypto-currency, called INTER. Users earn INTER for installing the extension and browsing the web with it.

We use blockchain — a hybrid of Ethereum and Solana — to allow users to interact and transact with each-other. No more walled gardens. Users can create one or more INTER accounts and link them to their various web2 accounts. Users can interact with each-other by upvoting, downvoting, and sharing. The twist is that all of their interactions are publicly visible and users can customize their feeds and queries in ways that traditional platforms like twitter, tiktok, and google could never allow without destroying their own profitability. We essentially use blockchain to put the user back in control of their own attention.

Please see the FAQ and technical whitepaper for more details and information.

## User Incentive Structure

The Interlock Network has structured the user-incentives to encourage *thoughtful* voting. To this end — and unlike every other social network — votes are a finite resource. Users can upvote (or downvote) accounts by spending special *vote tokens*. Upon doing so, the target account gets a significant portion of those vote tokens deposited into their account, and the voter get a *vote receipt*. Vote receipts can be exchanged for INTER tokens at various times and at various exchange rates. In other words, users stand to make money — potentially — by *actively* voting — hoarding votes will yield no rewards. Users can get vote tokens by either being popular/trustworthy (and therefor upvoted) or by waiting for the vote-tokens to get airdropped into their account.

Todo add mermaid sequence diagram to help clarify the how users votes and receipts interact with the INTER token.

## Emission Schedule

In short, we plan to emit **1 billion** tokens, in **5 phases**, each subsequent phase doubling the total supply of tokens. Dates and times for the phases are chosen at the discretion of the Interlock Team based on strategic and economic circumstances — we are not committing to any fixed emission schedule. This means that the token is short-term inflationary but long-term deflationary.

Todo add token emission schedule chart from slide-deck or imitation.