Conflux Network:

Engineering An Economic Design

Andreas Park[1,2] and Andreas Veneris[1,3,4]

[1]Conflux Foundation Advisor
[2]The Rotman School of Management, University of Toronto
[3]Dept. of Electrical and Computer Engineering, University of Toronto
[4]Dept. of Computer Science, University of Toronto
andreas.park@rotman.utoronto.ca, veneris@eecg.toronto.edu

Abstract

Distributed ledgers or blockchains, in particular those based on Proof-of-Work (PoW) protocols, rely as much on economic mechanisms as on technology. In this paper, we describe how we approach the design of the economic mechanisms that underline Conflux, a high throughput/performance PoW blockchain, by providing a detailed analysis of its economic viability. Conflux offers several innovations relative to well-understood blockchain networks such as Bitcoin and Ethereum, both in terms of technology design but also in terms of the economics that underpin the technology. Most notably, a major difference in Conflux when compared to the status-quo is that processing of blocks occurs in parallel rather than serially, and users who commit code or information to the blockchain face ongoing costs and/or benefits for the duration they occupy chain space. Hence, the ecosystem design requires to assess carefully those parameters including how new block processing affects the fundamental limits of blockchain performance, and how storage costs affect user incentives in this new decentralized ecosystem.

NOTICE

NOTHING IN THIS WHITEPAPER CONSTITUTES LEGAL, FINANCIAL, BUSINESS, OR TAX ADVICE AND YOU SHOULD CONSULT YOUR OWN LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISER BEFORE ENGAGING IN ANY ACTIVITY IN CONNECTION HEREWITH. NEITHER CONFLUX FOUNDATION LTD. (THE CONFLUX), ANY OF THE PROJECT TEAM MEMBERS WHO HAVE WORKED ON THE CONFLUX PLATFORM OR PROJECT IN ANY WAY WHATSOEVER (THE CONFLUX TEAM) NOR ANY THIRD PARTY SERVICE PROVIDER SHALL BE LIABLE FOR ANY KIND OF DIRECT OR INDIRECT DAMAGE OR LOSS WHATSOEVER WHICH YOU MAY SUFFER IN CONNECTION WITH ACCESSING THIS WHITEPAPER, MATERIALS PRODUCED BY THE CONFLUX, OR ACCESSING THE WEBSITE AT [HTTPS://WWW.CONFLUX-CHAIN.ORG/] OR ANY OTHER MATERIALS PUBLISHED BY THE CONFLUX. The Conflux and the Conflux team do not and do not purport to make, and hereby disclaims, all representations, warranties or undertaking to any entity or person. All statements contained in this Whitepaper, statements made in press releases or in any place accessible by the public and oral statements that may be made by the Conflux and/or the Conflux team may constitute forward looking statements (including statements regarding intent, belief or current expectations with respect to market conditions, business strategy and plans, financial condition, specific provisions and risk management practices). You are cautioned not to place undue reliance on these forward-looking statements given that these statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results to be materially different from that described by such forward looking statements. These forward-looking statements are applicable only as of the date of this Whitepaper and the Conflux and the Conflux team expressly disclaims any responsibility (whether express or implied) to release any revisions to these forward-looking statements to reflect events after such date. You understand that the Project and the creation and distribution of the Tokens involve significant risks, including but not limited to, the risk that (i) the technology associated with the Conflux Project may not function as intended; (ii) the Conflux Project may fail to attract interest or adoption, either from key stakeholders or the broader community; (iii) no guarantees that the price per Token determined by the market will be equal to or higher.

I. Introduction

When NASA prepared to travel to space they spent millions to develop a ballpen so that astronauts can write in zero gravity. Faced with the same problem, the Soviet Union used pencils. This anecdote is Conflux's philosophy in a nutshell: its main goal is to take the best parts of existing permissionless blockchains and push those bounds significantly.

What is Conflux? In brief, it is a Proof-of-Work (PoW) blockchain network that allows the parallel processing of blocks and transactions, while eventually forming a final serial chain. This feature contrasts other well-known networks, such as Bitcoin and Ethereum, which process blocks strictly one-by-one.[1] The parallel processing creates economic incentives for miners that are notably different from serial chains and in this paper we discuss how the differences improve the security and economic viability against double-spending attacks.

Conflux also seeks to overcome the problem of the unpaid smart-contract space occupation. In Ethereum, when introducing a new contract, a user merely pays at the time of the inclusion of the code in the chain whereas the community as a whole faces the burden of keeping the contract in storage. Conflux introduces ongoing costs of contract maintenance which give users an economic incentive to avoid wasting resources.

To provide intrinsic value, Conflux seeks to attract users that actively use the network for value-added services. Conflux believes it is critical that there are no barriers-to-entry for those who make meaningful contributions. This is why Conflux is a permissionless network with economic-driven governance mechanisms that incentivize community

[1] Ethereum does allow a limited number of so-called "uncle" blocks to allow for faster processing, but the setup of Ethereum is intrinsically not parallel.

contributions to ensure a secure, stable, and predictable environment for commercial activities.

This document discusses several aspects of the Conflux network that involve economic mechanisms. These mechanisms affect the users' and miners' costs and rewards and thus their behavior, therefore it is crucial to plan ahead so as to avoid creating unintended consequence. This paper is a companion paper to the technical Conflux manuscript. It complements the engineering aspects by focusing on the underlying system's micro- and macro-economic mechanisms.

At its core, blockchain technology is an infrastructure solution that allows the secure *(i)* transfer of economic value and *(ii)* execution of programming state/storage, without a trusted third party. To succeed in this scope, it needs to balance several core factors.

First, economic value transfers and payments for the cost of such usage rely on a native token. This token needs to be designed so as to serve as a medium of exchange but also as a unit of account for blockchain-based data. It is also desirable that the token can be used as a store of value so it can sustain long-run incentives for the different parties to use the chain. Finally, as is common with PoW networks, the native token plays a role in the compensation of the network's miners who are central to the operation and security of the network. There are by now a number of papers that highlight how native tokens can spur the adoption and usage of a network,[2] and we build on this body of literature in our analysis.

In this document we describe the distribution of tokens as well as the usage rules and the economic impact of the various rules. Namely, tokens are issued at genesis, as interest payments on subsets of tokens that satisfy certain rules, and as rewards to

[2]See, for instance, Bakos and Halaburda (2018), Cong, Li, and Wang (2018), Fisch (2019), Canidio (2018), or Li and Mann (2018)).

miners who include new blocks. We then provide a calibrated model that simulates the miners' expected income. Tokens interact with the outside world in the sense that there is a exchange rate to fiat currencies (as well as to other crypto-currencies), and we therefore also discuss carefully how the issuance of tokens affects the exchange rates.

In the final part of the paper we provide two formal analyses to provide a better understanding of the economics of Conflux. First, there are some well-known constraints on double-spending proofness for PoW blockchains[3] and we highlight how the Conflux Network expands the set of economically viable states relative to known networks. Second, we provide a formal equilibrium model of user and miner interaction to study how changes in policy variables affect equilibrium outcomes.

II. Cornerstones of the Existing Blockchain World

Before presenting the proposed economic system, we review key concepts from the main existing blockchain models.

Bitcoin is the first working cryptocurrency that solved the double-spending problem. At its core, the Bitcoin blockchain is a one-trick pony that is designed for the transfer of its native token, Bitcoins. It is conceptually set up to be slow as blocks of fixed size are produced serially at a approximately constant rate of one block, which can contain only around $3,500$ transactions, per 10 minutes. Although for a good level of certainty that the value transfer has indeed happened, it is not sufficient that a transaction has been included in a block. The reason is that the block may not be a part of the longest chain but of a fork. This can happen, for instance, when two blocks are created at around the same time — only one of them will eventually become part of the longest

[3]See Chiu and Koeppl (2017) and Budish (2018).

chain. One therefore needs to wait for a few block confirmations before the transaction can be considered as final. The setup, with block formation time of 10 minutes and a even longer confirmation time, is clearly unsuitable for day to day payments. Bitcoin has also other limitations: once all Bitcoins have been mined through block rewards, miners receive only user-determined transactions fees for securing the network. If we take the current income of miners as a benchmark, these fees need to be rather large: At the current block rewards of 6.25 BTC per block and a BTC price of approximately $10,000 (as of the day of this publication) *each* of the 3,500 transactions that fit into a block needs pay a fee of around $18. All these features make Bitcoin unsuitable for remittance payments and likely too expensive to be a substitute payment network for the majority of business transactions (Auer 2019).

The main participants in the Bitcoin network, however, are the miners, short-term speculators, and long-term holders. Very few network participants use Bitcoin for its original purpose, as "peer-to-peer electronic cash." In the future, the long-term holders need to rely on short-term speculators to create sufficient transactions so that the miners are willing to continue to provide the security for the network. This will likely become a challenge in the future. In other words, as it stands, the Bitcoin network today does not incentivize users of the token for meaningful and value-generating economic activity. In addition, the technology infrastructure of Bitcoin has limitations and allows little beyond transfers of Bitcoin. Without Turing-complete scripts, decentralized application (dApp) developers have at most peripheral use for it through introduction of "side-chains" such as the Lightning Network, etc. Governance is also a challenge. Changes to the Bitcoin protocol require that miners agree. This can be difficult when those changes may have

a negative impact on the miners' income — even if the change itself serves the broader ecosystem well.

The *Ethereum Network* is a much improved system relative to Bitcoin and features Turing-complete smart contract functionality, which enables developers to code dApps that run on the network. Ethereum's smart contract language allows the creation of tokens that can be used as non-native payment coins or even as securities. Ethereum's native token Ether has no hard cap on its token supply and can therefore grow organically as usage of the network expands and demand for tokens increases. Ethereum's governance follows a similar mechanism as Bitcoin, with some improvements: miners receive not only block rewards for each block that they create, they also collect transaction fees for the execution of code. Therefore, more complex transactions or operations are rewarded with higher fees.

However, as in Bitcoin, Ethereum also suffers from a low transaction throughput rate: the network can currently process only a maximum around 40 transactions per second. This is nowhere near the rate of need for modern commercial financial infrastructure. For instance, Payments Canada processes around 28 million transactions on an average business day, while Canadian economy is ranked only the 10^{th} by Nominal GDP (Times 2019). Assuming that most activities occur over 12 hours daily, a blockchain payments network to handle this level of transactions would need an approximately minimal throughput of 650 transactions per second (tps). Furthermore, it is equally infeasible to use the Ethereum blockchain as a substitute infrastructure for securities trading: traditional centralized securities exchanges and over-the-counter securities markets worldwide process billions of orders and transactions per day. As a matter of fact, although there are many decentralized exchanges on the Ethereum network, at the

current throughput rates they are fundamentally unable to accommodate a meaningful fraction of today's financial market activities.

A second function issue for Ethereum is that users pay for a contract only at the time of the inclusion of the contract code. Additionally, only the miner that includes this code on the chain gets this one-time reward. Yet every new contract submitted to the Ethereum chain not only requires the network to execute the code, the contract also occupies "chain-space" (*i.e.,* memory in the global state of the Ethereum chain) even if it remains inactive after its submission. In summary, all full nodes of the network need to subsequently store the information resulting in a situation where users can store data on the chain with a one-time inclusion fee, while the storing of such data can be indefinitely long with no maintenance payment required. As such today, the vast majority of the state-tree space of Ethereum is occupied by inactive smart contracts. This unused data waste space in the state-tree of the blockchain, slow down the system, and create undesirable network latency/overhead.

One of the goals for the Conflux project is to build on and vastly improve on the features of existing blockchain systems: guaranteed execution of software code via a Turing-complete virtual machine on a permissionless consensus mechanism with a higher performance while not sacrificing safety and decentralization.

III. An Overview of the Conflux Network

Conflux is a new PoW network with a Turing-complete smart contract language similar to this of Ethereum.[4] The Conflux network provides significant performance improvements with its processing of parallel blocks in a Directed Acyclic Graph (DAG)

[4]See Li, Li, Zhou, Xu, Long, and Yao (2018) and .

structure, which lowers confirmation times and increases transaction throughput substantially.

To address the space congestion challenge, Conflux requires users to bond native tokens into storage to occupy space, which implicitly creates a disincentive to occupy space unnecessarily. The disincentive stems from the payment of interest on existing tokens in the system. The interest on the bonded storage is payed to miners instead of the users to create a long term income to the miners. To address the fairness attack challenge, Conflux assigns the block reward in a way that eliminates the winner-take-all characteristic of mining. Instead of competing for the longest chain, miners in Conflux receive block rewards for all the blocks that they generate, albeit with some penalty mechanisms that encourage following the consensus protocol. Competing blocks are jointly penalized so that selfish mining is not profitable and different miners are incentivized to cooperate along the protocol to keep the network stable and secure.

Similarly to Ethereum, Conflux operates with an account-based model that every normal account associates with a balance and each smart contract account contains the corresponding byte codes as well as an internal state. Conflux supports a modified version of Solidity (the main contract language in Ethereum) and Ethereum Virtual Machine (EVM) for its smart contracts, so that smart contracts from Ethereum can migrate to Conflux easily.

A transaction in Conflux refers to a message that initiates a payment transaction, or deploys/executes smart contract code. Each block consists of a list of transactions that are verified by the proposing miner. Each node maintains a pool of verified, received transactions that have not yet been included in a block. Miners compete with one another by solving PoW puzzles to include transactions into blocks. Similar to Bitcoin and

Ethereum, Conflux adjusts the PoW difficulty so as to maintain a stable block generation rate. Each node also maintains a local state constructed from the received blocks.

The Conflux consensus algorithm operates with a special Directed Acyclic Graph (DAG) structure called TreeGraph. Unlike Ethereum which only accepts transactions on a single chain into its ledger, the Conflux consensus algorithm safely incorporates and processes transactions in all concurrent blocks. There are two kinds of edges between blocks, *parent* edges and *reference* edges. Each block (except the genesis) in the TreeGraph has exactly one parent edge to its chosen parent block. Each block can also have multiple reference edges to refer previous blocks. All parent edges form a tree embedded inside a Directed Acyclic Graph (DAG) of all edges.

At a high level, Conflux uses the novel Greedy Heaviest Adaptive SubTree (GHAST) algorithm (Li and Yang (2020)), which assigns a weight to each block according to the topologies in the TreeGraph. Under this weight assignment, there is a deterministically heaviest chain within the graph called *pivot chain*, which corresponds to the relatively most stable chain from the genesis to the tip of the parental tree.

Parent edges, reference edges, and the pivot chain together enable Conflux to split all blocks in a DAG into *epochs*. As shown in Figure 1, every block in the pivot chain corresponds to one epoch. Each epoch contains all blocks that are reachable from the corresponding block in the pivot chain via the combination of parent edges and reference edges and that are not included in previous epochs. Details about the consensus algorithm can be find in (Li and Yang (2020)).

Experimental results have shown that Conflux is capable of processing $4,000$ transactions per second for simple payment transactions, at least two orders of magnitude higher throughput than Ethereum and Bitcoin. The improvement in throughput is a

result of the TreeGraph structure and the consensus algorithm, so that the network can operate with a much faster block generation rate, no forks are discarded, and with a higher utilization of block space. According to the technical specification, the main net of Conflux will run under a fixed block generation rate at two blocks per second. The daily block generation rate is therefore $60 \cdot 60 \cdot 24 \times 2 = 172,800$ blocks per day.

IV. Token Rules

There is a unique native token on the Conflux network, hereafter referred to as *CFX*. Each CFX contains 10^{18} *Drip*. Transactions on Conflux are handled similarly to those on the Ethereum network and CFX, therefore, plays a similar role as Ether. Namely, users submit transcation with a gas limit and a gas price; the latter is denominated in CFX.

The *Conflux Foundation* is a non-profit entity established by Conflux to make adjustments when the allocation of resources deviates from an equilibrium, to provide incentives to overcome the cold start problem, and to promote participation/development in the network in the early stage.

A. Genesis Tokens

The initial number of tokens is 5,000,000,000 (5 billion). All of these tokens are locked at the launch of the main-net and will then be released gradually, in monthly intervals. These initial tokens will be divided between the following parties:

1. **Core Team**

- *Private Equity Investors*: Up to 600 Million CFXs will be allocated to our private investors. In the last investment round, CFX tokens are sold at 0.1 USD per CFX. See Section IV.B. for the unlock timeline of these tokens. At the time of the writing of this paper, more than 520 Million CFXs in this category are already sold to investors. Unsold tokens in this category at the launch of Conflux will be allocated as Foundation Holdings.
- *Foundation Holdings*: 200 Million CFXs plus any unsold CFXs in the previous category will be allocated to support the long term financial need of Conflux Foundation. These tokens will be unlocked monthly over 2 years.
- *Genesis Team*: 1,800 Million CFXs will be awarded to the founding team including the IIIS team (of Tsinghua University) and Alt-Chain Technologies shareholders (where Conflux spins off from), Conflux Foundation employees, and advisors. The Genesis team's tokens will be unlocked over 4 years.

2. **Community and Ecosystem Building**

- *Community Fund*: 400 Million CFXs will be used for marketing and community building. These tokens will be unlocked over 4 years.
- *Ecosystem Fund*: 2,000 Million of CFXs in the Genesis Issue will become an ecosystem fund to solve cold start problems and to invest promising dApp projects that run on the Conflux network. These tokens will be unlocked over 4 years.

B. Investor Token Unlock Rules

The allocated private investor CFX tokens will be unlocked monthly over two years following the launch of Conflux. Based on the market spot CFX price, the investor tokens may be unlocked in-advance to provide liquidity to the CFX market in facing price volatility. The in-advance unlock rules are as follows.

1. If the last five-day average market spot price of CFX exceeds 0.6 USD, upon the approval of Conflux Foundation, all private investors can receive the CFX tokens that should be unlocked in the first *two* months following the launch of Conflux.

2. If the last five-day average market spot price of CFX exceeds 0.8 USD, upon the approval of Conflux Foundation, all private investors can receive the CFX tokens that should be unlocked in the first *four* months following the launch (i.e., two additional months in-advance on top of the previous rule).

3. If the last five-day average market spot price of CFX exceeds 1.0 USD, upon the approval of Conflux Foundation, all private investors can receive the CFX tokens that should be unlocked in the first *six* months following the launch.

4. If the last five-day average market spot price of CFX exceeds 1.2 USD, upon the apporval of Conflux Foundation, all private investors can receive the CFX tokens that should be unlocked in the first *eight* months following the launch.

5. If the last five-day average market spot price of CFX exceeds 1.5 USD, upon the apporval of Conflux Foundation, all private investors can receive the CFX tokens that should be unlocked in the first *ten* months following the launch.

C. *Token Forms*

The issued tokens exist in two forms: liquid and illiquid. In the liquid form, they can be immediately transferred/used on the Conflux network. There are also three ways in which tokens can be locked up, which makes them illiquid. Illiquid tokens cannot be transferred. Locking can take three different forms.

1. Tokens can be staked so as to earn the user interest.

2. They can be placed into bonded storage to purchase space on the network (e.g., for running dApps).

3. They can be locked up for a pre-determined amount of time to purchase votes in the network governance.

D. *Interest/Seignorage Payments*

The network will distribute interest on all illiquid tokens at a fixed rate. Token holders obtain this interest only if they stake their tokens (i.e., move them to the illiquid state). The interest will be added to the user's holdings at the time when the user un-stakes the token and converts it to the liquid state.

Based on performance-tests from the test-net, Conflux creates two blocks every second so that there are approximately 63,072,000 blocks per year. We use r_c for the system base interest rate, expressed in annual terms, and interest is compounded per block. Therefore, a user that stakes for b blocks receives interest payment:

$$\left(1 + \frac{r_c}{63,072,000}\right)^b - 1$$

per staked token. For instance, if the annual interest is $r_c = 4\%$, a user that stakes for 15,768,000 blocks (around a fiscal quarter) will receive interest 1% per staked token. In those calculations we round the interest payment in tokens *down* to the nearest (1) drip.

By setting a nominal rate of r_c, the resulting annual rate is given by:

$$\text{effective annual rate} = \left(1 + \frac{r_c}{63,072,000}\right)^{63,072,000} - 1.$$

For instance, for $r_c = 4\%$ we have an effective annual rate $\approx 4.08\%$.[5]

The economic mechanism is straightforward: suppose, for simplicity, that all tokens have been issued, that all tokens have been staked, and that no token has changed hands. Then paying interest does not create new value — all that has changed is that there is an increase in the number of tokens (the "monetary base") that represent the network. Owners of tokens neither gain nor lose anything in real terms.[6] When users do not stake their tokens, their interest goes to the public fund. Therefore, the interest payments implicitly shift value from those who do not stake to those who stake.

E. Storage Resources

A key component of the incentive system is the *bonded storage*. Anyone who wants to deploy a smart contract on Conflux network needs to submit a number of tokens to create a bonded storage. The interest payments to tokens in bonded storage are continually disseminated to the miners, instead of those who have locked those tokens.

[5] Since we have large number of payment intervals, we can approximate $\lim_{n\to\infty}(1 + x/n)^n - 1 = e^x$.

[6] Another analogy is that of stock splits: when a firm splits its stocks, say, 1:2, then owners receive for each one "old" stock two "new" stocks. This process does not change the value of the firm, however, and therefor stockholders are no richer or poorer after the stock split.

Therefore, those interest payments create an implicit *reward stream* from the chain space occupiers to the maintainers of the network.

The required deposit for storage resources is measured in the native token: 0.5 CFX for 1 kB. The process is as follows: a user (such as a dApp developer) locks up a number of tokens. The user then occupies space on the network (*e.g.*, deploying a dApp or storing data due to the execution of dApps), tokens are withdrawn from the locked tokens and put into bonded storage. The interest payments for tokens in bonded storage go to the miners. To release tokens from bonded storage, users must free up the space they occupy.

F. Voting Rights

The medium term goal is that the public fund transforms to a DAO, and that Conflux stakeholders vote on its operations using their voting rights. Users obtain voting rights through the locking of tokens: to cast a vote, users must agree to lock up their tokens and the lock-up time determines the number of votes. The lock up duration starts at the time (aka block) of casting of a vote. The voting rights will be awarded

$$\text{number of quarters} \times \text{number of tokens} \times 0.25.$$

For instance,

- *Locking maturity less than a quarter*: No voting rights
- *Locking maturity more than a quarter*: One CFX has 0.25 votes
- *Locking maturity more than half a year*: One CFX has 0.5 votes
- *Locking maturity more than a year*: One CFX has 1 votes

We measure "time" in blocks based on the assumed number of 63,072,000 per year. While tokens are locked to obtain votes, users retain the right to staking interest. The longest locking duration for voting is 4 years. While tokens are locked to gain a voting right, users cannot withdraw the tokens or decrease the locking duration.

G. Network Bootstrap

We next discuss how to economically bootstrap the Conflux network and how the Community Fund and the Ecosystem Fund will be managed in the long term.

Community Bootstrap: To bootstrap the Conflux community, Conflux Foundation offered bounties and grants in the form of FC (Fan's Coin) tokens to those community members who made contributions to Conflux prior its launch. Conflux Foundation will convert the issued FC tokens into CFXs from the Community Fund once the Conflux network goes live. Note that the scale of Conflux bounty and grant programs is moderate. The total amount of issued FC tokens at the time of Conflux launch will be less than 20 millions. After the launch, we will continue the bounty and grant programs with CFXs in the Community Fund at a similar scale.

Ecosystem Bootstrap: One challenge of bootstrapping the Conflux ecosystem is to attract developers to develop and deploy dApps on Conflux. Sending massive CFX airdrops to developers is not an ideal solution because one can game the system and can sell the airdropped CFXs at the secondary market instead of using them for development. To address this challenge, Conflux has a unique sponsor mechanism in which one can become a sponsor for a deployed smart contract to cover its transaction fees and storage costs. Conflux Foundation will use the Ecosystem Fund to sponsor deployed smart contracts on Conflux during the bootstrapping period. Unlike normal airdrops, the

sponsor mechanism in Conflux guarantees that these sponsoring CFXs will not go into circulation unless they are paid first to the miners as transaction fees.

DAO Governance: Conflux Foundation plans to gradually transfer the governance of the Community Fund and the Ecosystem Fund to the DAO of the Conflux stakeholders. The current road map is to complete the transition within two years after the launch of Conflux.

Ecosystem Fund Investment: In the long term, we can use the Ecosystem Fund to establish investment funds to invest on significant dApp projects that are beneficial for the Conflux ecosystem. Conflux Foundation will invite prior Conflux private investors to co-manage such investment funds. We believe the establishment of such investment funds should be under the supervision of the Conflux stakeholder DAO.

H. Mining Rewards

System Maintainers of the Conflux network will receive income from three sources: transaction user fees, block rewards, and interest income that arises from users "renting" space on the blockchain.

User Fees: Users will need to compensate miners when submitting transactions and changing the state on the blockchain. The transaction user fee is distributed proportionally to the binary base factors of blocks as defined in Li and Yang (2020).

Block Rewards: As a common practice in PoW networks, the mining of a block involves a coin-based reward that increases the monetary base and leads to inflation. We denote this block-reward driven inflation rate by r_b. Ignoring any market-driven price changes, economically coin-based rewards are a transfer of wealth from existing holders of CFX collectively to the winning miner.

The initial base block reward per block is 7 CFX, corresponding to $r_b = 8.83\%$. The base block reward remains constant for the first four years. It then decreases at a quarterly rate of 0.958, effectively halving every four years, until the base reward reaches 1.75 CFX per block.

There are some technological subtleties that go beyond the scope of this paper, but that we want to mention here. Namely, although block rewards are determined deterministically in the decentralized network, there is no a pre-defined number of coins that a miner who successfully mines a block receives. Instead, blocks are organized in "epochs" and block rewards are determined/distributed for each epoch. For each block, the protocol assigns a "weight" based on so-called directed acrylic graph features, which is effectively a measure of importance in the parallelly-arranged chain and the reward is based on the block's weight. For details, we refer the reader to the technical white paper.

Storage interest: When tokens are used as bonds for storage, the interest paid on those tokens is given to miners. Similar to the block reward the total amount of interest from bonded storage will be distributed in proportion to the actually received base reward of each block.

Although the details of block rewards are non-trivial to describe, the basic principle is the same as in any public PoW network: miners provide computing power, the more power they provide the more likely they are to win a block, the more blocks they win, the higher is their income, and so forth.

In the next section, we present a calibrated model of user uptake and inflation to provide guidelines for the expected mining revenue.

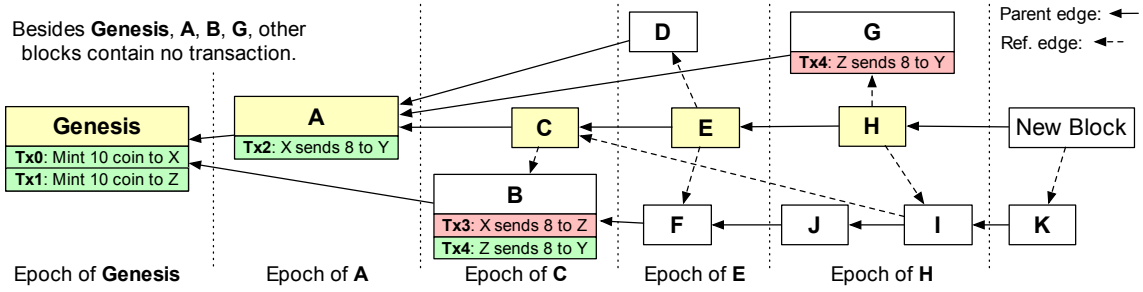


Figure 1
TreeGraph structure example in Conflux

Anti-cone Penalty Ratio: The mining block reward of a block is modified by an anti-cone penalty ratio in Conflux. In this paper, we define the penalty ratio of block b:

$$\max\left\{0, 1 - \left(\frac{|\text{Anticone}(b)|}{100}\right)^2\right\}$$

where Anticone(b) denotes the set of blocks that are not in the past sub-graph of b (i.e., reachable via parent and/or reference edges from b) and that are not in the future sub-graph of b (i.e., reachable via parent and/or reference edges to b). For example, Anticone(F) $= \{A, C, D, G\}$ in Figure 1. Because the anti-cone of a block may keep growing, Anticone(b) here only includes blocks that are within 10 epochs after the epoch where b resides in. Note that for simplicity, we exclude difficulty adjustment from the consideration of the formula and assume the difficulty remains constant. See Li and Yang (2020) for the full formula.

For a new block, the base reward is the maximum block reward the generator can possibly receive. For every anti-cone block of the new block, a portion of the block reward will be deducted till zero. Intuitively, this block reward formula encourages the generator to conform with the honest behavior as defined by the consensus protocol. It

encourages the generator to refer as many blocks as possible to avoid anti-cone blocks due to unreferenced blocks. It also encourages the generator to propagate the new block as soon as possible to avoid anti-cone blocks due to network delay. Unlike the winner-take-all mining game for the longest chain in Bitcoin, all blocks in Conflux receive block rewards and miners who cooperate with one another minimize the anti-cone. This makes Conflux secure against selfish mining attacks which exploit the winner-take-all nature of Bitcoin mining; see Eyal and Sirer (2013).

In our calibrations, we abstract from the anti-cone and set it to zero; the implicit assumption is that all miners reference all previous blocks correctly and make no errors.

I. Evolution of the Conflux Rate

The market price of the freely traded CFX tokens due to the permissionless nature of the network is evidently beyond the control of Conflux. Although one cannot prevent speculation, eventually one could argue that (like any other asset or commodity) the price of the token will be driven by demand for Conflux services. In what follows we provide a formal model to underline the relationship between service usage and price.

Fundamentally, the price of CFX depends on two main parameters: the built-in inflation of the system, and the impact of market price in the outside world. It is analogous to *covered interest parity*, which is an economic concept to describe exchange rate changes over time. If we use p_0 to denote the price for CFX today in fiat currency (i.e., how much in fiat one pays for one CFX), p_1 for the price of the token one year into the future (formally, the 1-year forward rate), $r_c + r_b$ for the real interest rate in Conflux (caused by both block rewards and storage interest payments), and r for the compounded-average real interest rate of the fiat-economy (*e.g.,* over a basket of major

fiat currencies)

$$p_1 = p_0 \times \frac{1+r}{1+r_c+r_b}.$$

In other words, if Conflux pays a higher interest rate than what is available in fiat markets, then the price of CFX is expected to mechanically *decrease* over time.

V. Calibrated Model for Miner Rewards

A. Overview

One important factor for a PoW network to function is that miners are willing to spend resources on mining blocks in exchange for some form of compensation. The security of such a network is directly related to the computational power provided by participating miners. As computational power can be costly, sufficient miner compensation is required to sustain the involvement of miners, and hence crucial to the security of the chain. In this section, we develop our approach to determine the expected revenues that miners gain from participating in such a system. We calibrate our model based on our technical specification as well as observations from a blockchain project, Ethereum given the similarity in available features.

Miners receive direct revenue from three sources: block rewards, user fees, and interest paid on the tokens that users need to deposit as bonds when they want to store data on the blockchain.

Block rewards are newly minted tokens and therefore, they increase the monetary base of Conflux. Ignoring changes to the price of Conflux tokens, an increase in the monetary base lowers the value of each Conflux token and block rewards are therefore a value transfer from native token holders (who receive "security" and ledger consistency

as a service) to miners. As such, it is our view that the appropriate way to think about block rewards is in terms of the annual inflation rate they create. We will formally discuss how block rewards and block inflation interact in the next subsection.

User fees depend on the ultimate usage of the blockchain, and therefore to determine user fees, we need to develop a model of user uptake; we do this in Subsection C. and then we derive the associated fee revenue in Subsection D.. Interest payments also increase the monetary base and we develop a model for these payments in Subsection E.. Moreover, interest payments to miners depend on how much storage users choose to occupy; we build a model for this in Subsection F. and then derive interest payments to miners in Subsection G.. Miners likely have to pay their bills (for electricity and h/w equipment) in fiat. Therefore, one needs build a model for the price of CFX to accommodate this pricing, a topic that is discussed in Subsection H.

In Subsection I. we align all these components to determine the total revenue that miners will obtain. As the final part of this exercise, we present simulation results for this revenue and different parameters in Subsection J.

All notations introduced in this Section is summarized in Table I below.

Table I
List of Symbols for Section V.

Symbol	Meaning
G	genesis tokens, 5B
D	number of seconds in a day, $60 \times 60 \times 24$
d	days since main-net launch
B	block reward
$b(d)$	block rewards per day, defined in equation (1)
r_b	annual inflation rate from block rewards
$u(d)$	user uptake rate $\in (0, 1)$; estimated from Ethereum data using equation (2)
u^{ETH}	estimated user uptake rate using Ethereum as a benchmark, described in equation (3)
$u^{\text{fast}}(d),\ u^{\text{slow}}(d)$	user uptake rates, modelled based on Ethereum but one where shift in growth occurs faster and another where it occurs slower; defined in equations (4) and (4)
$T(d)$	transactions on day d; computed as $u(d) \times D \times 4000$ (maximum theoretical throughput)
f	average transaction fee paid in fiat-equivalent terms
$F(d)$	total transaction fees paid to miners on day d, defined in equation (6)
α	fraction of tokens that an average user locks up to receive interest payments
r_c	annual rate of inflation created by interest payments in the Conflux network
R	daily interest rate for compound transactions; derived in equation (7)
$\gamma(d)$	fraction of gas used by computations that are not plain token transactions; estimated using equation (8) and defined in equation (9)
β	system required fraction of tokens that need to be put in bonded storage for occupying space
$I(d)$	interest income from bonded tokens for miners; defined in equation (10)
$p(0)$	price of CFX on day on main-net launch
$p(d)$	inflation adjusted price on day d, defined in equation (12) and in reduced form in equation (13)
$G(d)$	number of coins outstanding on day d; it is genesis plus interest tokens plus block reward tokens, described in equation (11)
$m(d)$	total revenue for miners on day d, derived in equation (14)
$\bar{m}(d)$	total miner revenue averaged over 1 year
g	hypothetical daily growth rate of the CFX price so that after 3 years, the market value of all Conflux tokens is the same as the market value of all ETH at the beginning of 2020

B. Miner Block Rewards

Miners receive a reward per block mined and the exact amount depends on where the block is in the chain relative to the pivot chain and its anti-cone. Notably, for the calibration presented, instead of presenting the exact *per block* reward, we compute the aggregate *daily* block award amount.

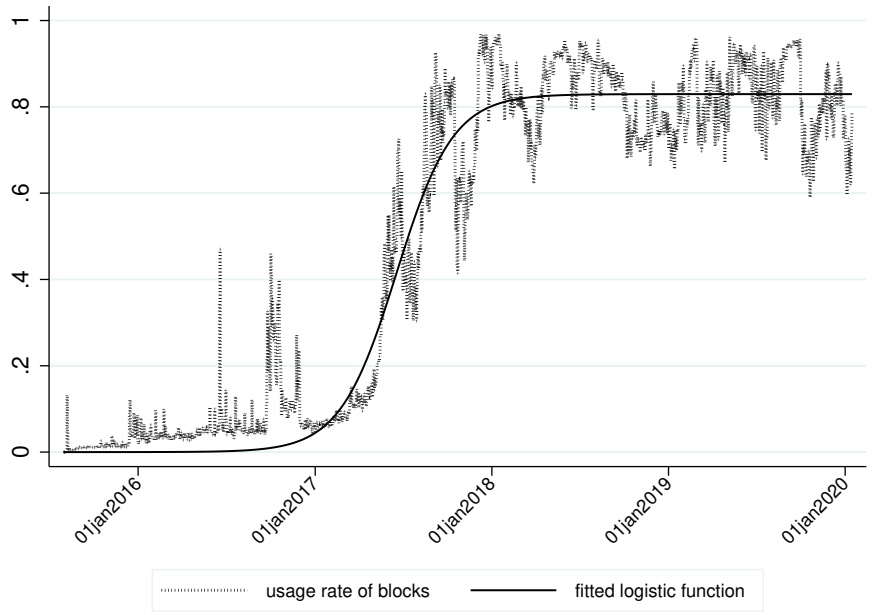
According to the technical specifications, there the network produces two new blocks per seconds, and thus $60 \cdot 60 \cdot 24 \times 2 =: D \times 2$ new blocks per day. Assuming a constant mining rate, there are $D \cdot 730$ blocks mined per year. As such, if B denotes the number of newly minted tokens created as block reward to the miners, the system needs issue $B \cdot D \cdot 730$ new tokens annually as block rewards. Block rewards increase the monetary base and create inflation. In other words, by setting a block reward rate the system can directly determine the inflation rate created by newly minted blocks. This inflation is a transfer from coin holders to miners, and in setting the block rate Conflux can pivot how much wealth it redistributes during a given year. Specifically, Conflux's objective is to set the block reward based on an annual inflation target rate of $r_b \in (0, 1)$. Therefore, for target value r_b, the block reward must solve

$$B \cdot D \cdot 2 \cdot 365 \equiv G \cdot r_b \quad \Leftrightarrow \quad B = \frac{G r_b}{730 D}.$$

Note, in Conflux blocks are created continuously and may in fact be empty when there are no valid transactions. Overall, on any given day d, total block rewards, denoted by $b(d)$ are therefore

$$b(d) = \frac{G r_b}{365}. \tag{1}$$

Figure 2
Adoption Rate for Ethereum and the fitted logistic function



C. User Uptake

User adoption of the network will determine the demand for transactions and computations, the fees paid by users, and the storage rent distributed to miners. We discuss these quantities in later subsections as here our objective is to develop a model concerning user adoption.

A common feature of new technologies is that their adoption follows a S-shaped pattern with slowly increasing usage early on and then a sudden jump of activity. An example is the uptake of the Ethereum network, depicted in Figure 2, where we plot the average daily fraction of the gas limit that has been used; this graph is based on data

from `https://etherscan.io/charts`.[7] As Conflux is a new technology, it is reasonable to expect that uptake of Conflux will also follow an S-shaped pattern provided the network is successful. Conflux and Ethereum have many similar features and we will therefore use Ethereum's historical adoption data to estimate what we believe to be a reasonable uptake rate for Conflux.

As a first step, we characterize the Ethereum's user uptake rate in form of a parametric functional. There are multiple ways to describe an S-shaped function (also known as a sigmoid curve), a standard one being logistic function which has the form:

$$Y = \frac{\xi_0}{1 + e^{-\xi_1 \cdot (X - X_0)}}, \tag{2}$$

In the equation above, Y is the uptake rate at time X, ξ_0 is the maximum value for uptake, ξ_1 is the growth rate, and X_0 is the time-value of when the curve reaches 50% of its supremum value (formally, the value of the horizontal axis at the sigmoid's midpoint). Our estimation results are in Table II, Figure 2 also plots the fitted function.

Blocks can theoretically be filled up to 100% of the gas limit, yet the estimate for ξ_0 indicates that the Ethereum blockchain's usage rate currently maxes out at 83%. There could be several explanations for this: one is that miners collude so to not include transactions that offer low transaction fees. Another is that the 83% usage rate is a steady-state, day-to-day "technological" upper bound of what miners can actually include taking account of validation and transaction submission latency. Finally, it is possible that once the network becomes congested, users no longer send new transactions

[7] A graph of daily transactions would have a similar shape. We note that there is an upper bound in transactions because the total amount of gas per block is limited.

Table II
Logistic Curve-Fitting for Ethereum's User Uptake Rate

The table contains the results for the non-linear least squared regression of (2) using data for Ethereum's user uptake rate Y, measured as the fraction of the gas limit used per block and day X. T-stats are in parentheses. *, **, *** indicate statistical significance of the coefficients at the 10%, 5%, and 1% levels.

	ξ_0	ξ_1	X_0
Estimate	0.83***	0.02***	690.54***
	(244.800)	(30.809)	(316.067)
Observations	1,631	1,631	1,631
R-squared	0.978	0.978	0.978

to the chain because of the long delay; this would create an endogenous upper bound on demand (reflected in the size of the mempool) for transaction processing.

Following `https://bitinfocharts.com/ethereum/`, transaction fees consistently account for less than 3% of miner revenue per block and it appears that miners are likely not too concerned about using the entire space in a block.

We will henceforth use the estimations from Table II as our benchmark for modeling user uptake $u(d) \in (0, 1)$. In other words, we assume (predict) that on day d a fraction $u(d)$ of Conflux's total capacity is used. In the testnet, Conflux has a transaction throughput of 4,000 per second. As a day has $86,400$ seconds, on day d, there will be $u(d) \times 4,000 \times 86,400$ many transactions. Using the results from Table II, we obtain:

$$u^{\text{ETH}}(d) = \frac{0.83}{1 + e^{-0.017 \cdot (d - 690)}}. \tag{3}$$

Under this model, it will take 718 days until Conflux reaches a network capacity of 50% and 793 days (*i.e.,* approximately two years) to reach capacity 70%.

Undoubtedly, the uptake of Conflux may vary from the model described above in terms of the time needed to reach a specific adoption rate. Ecosystem investments and dApp development may enable a faster uptake. Conflux's smart contract platform is compatible with Solidity, one of the main programming languages for smart contracts on Ethereum. This interoperability implies that many current blockchain dApp developers from the Ethereum community face a shallow adoption curve. In contract, when Ethereum was launched, there was a significantly smaller community of developers proficient in Solidity. Hence, it is reasonable to expect a faster user uptake of Conflux comparing to Ethereum.

In calibrating our model, we provide analysis under two different adjustments to suggested model. Firstly, we shift the adoption curve 180 days to the right, meaning that adoption is delayed by a quarter. In the second, we shift the adoption curve 180 days to the left, meaning that adoption is sped up by a quarter. Formally, this shift is an increase/decrease in parameter X_0 to 870 and 510 calendar days, respectively, so that:

$$u^{\text{fast}}(d) = \frac{0.83}{1 + e^{-0.017 \cdot (d-510)}}, \tag{4}$$

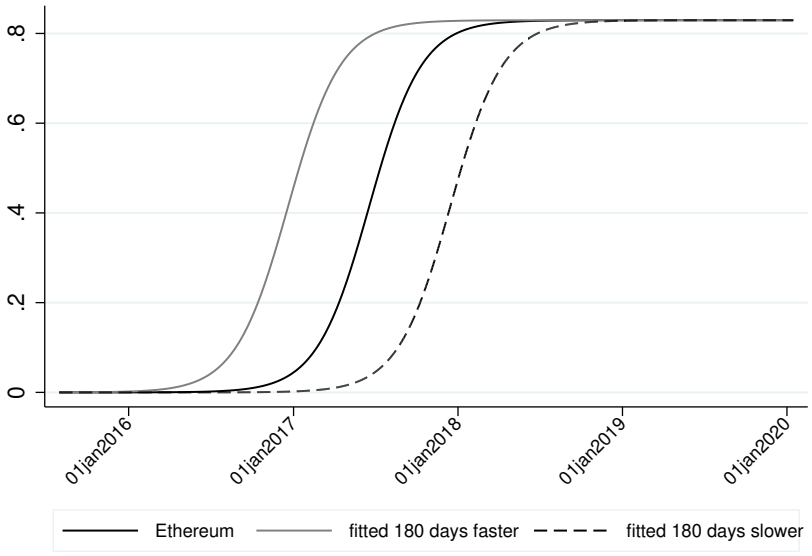
$$u^{\text{slow}}(d) = \frac{0.83}{1 + e^{-0.017 \cdot (d-870)}}. \tag{5}$$

Figure 3 illustrates the three different adoption rate models, labelled as *fast* ($u^{\text{fast}}(d)$), *Ethereum* ($u^{\text{ETH}}(d)$), and *slow* ($u^{\text{slow}}(d)$).

At capacity, Conflux processes 4,000 transactions per second. With a long-run adoption rate of $u(d) = 80\%$, this amounts to an expected 3,200 tps utilization. With an uptake rate of $u(d)$, the average daily number of transactions is

$$T(d) = u(d) \cdot 4,000D = u(d) \cdot 345.6 \times 10^6.$$

Figure 3
The Three Calibrated Adoption Rates



We note that we use data from Ethereum to estimate the fractional usage of the maximum capacity, and we expect that the actual update rate in Conflux will exceed the previously stated number. We justify this opinion as follows: Ethereum is arguably at capacity most of the time (see Figure 2 and its mem-pool of unsettled transactions is non-empty). Since Ethereum is at capacity, there is a limited incentive for developers to introduce new dApps, especially for enterprise-scale use-cases. Conflux's higher throughput mitigates the concerns that the transactions do not get confirmed timely, and since Conflux is compatible with Solidity, developers face a flat learning curve. Together this should contribute to a fast adoption of Conflux.

D. User Fees

Users pay for computational cycles, aka gas used. It is a common practice to denominate blockchain capacity by transactions per second, where a transaction refers to a simple transfer of the native token from one address to another. Such a transaction require a fixed amount of gas; e.g., on Ethereum, it is 21,000 gas. We therefore follow this convention and equate user fees with the fees that users pay for address-to-address transfers.

We assume that users on average pay a transaction fee of value f. Therefore, average daily fees, as a function of *day* $F(d)$, are calculates as follows:

$$F(d) := \underbrace{f}_{\text{average daily fee}} \times \underbrace{T(d)}_{\text{number of transactions on day } d} = F \cdot u(d) \cdot 4,000 \cdot D. \tag{6}$$

The table below presents examples for the annual fee income on the Conflux Network that "at capacity" usage rate provides to miners for different levels of the average fee f.

average	per day	annual
\$0.001	\$276,480	\$88,300,800
\$0.005	\$1,382,400	\$441,504,000
\$0.010	\$2,764,800	\$883,008,000
\$0.020	\$5,529,600	\$1,766,016,000
\$0.050	\$13,824,000	\$4,415,040,000

For Ethereum, at its current block reward and thoughput, total rewards are on the order of \$2.3M daily or about \$840M annually, including both the block rewards and the

user fees. As a result, user fees account for less than 3% of the rewards.[8] In Conflux, with a similar block-usage rate, user fees would provide the same total fee income as the *total* revenue (fees plus block rewards) in Ethereum as long as user are willing to pay on average \$0.01 per transaction. Even for a moderate willingness of users to pay fees, annual income can be substantial. In comparison, the median transaction fee on the Ethereum blockchain for January–February 2020 has been between \$0.08 and \$0.15 (source: `ycharts.com`).

It is also of interest to compare these numbers to the fees in the traditional retail payment networks. For example, in credit card transactions, the different entities involved in a transaction, credit card companies such as Visa or Mastercard as well the the payment processing banks, currently charge between 1%-3% of the transaction value for retail transactions. Namely, any transaction value greater than \$2.5 incurs a minimal fee of \$0.05.[9] On another payment platform, FinTech company Square charges a flat fee of 2.75% per transaction; in other platforms that charge a flat rate per transaction, users usually encounter a transaction fee of at least \$0.15.

E. Interest Payments to Users

Conflux plans on paying users interest to whom their tokens are on hold. As we outlined in the preceding section, the issued tokens exist in two forms: liquid and illiquid. In the liquid form, they are "free," and can be immediately transferred and used on the

[8] As most of the empirical analysis in this paper, these figures are based on the state of the Ethereum blockchain in early 2020. Over the second half of 2020, however, usage fee on Ethereum have skyrocketed as a result of the congestion of the chain, caused by a strong uptake in decentralized finance applications. Our view at this point in time is that this congestion is not a steady state but most likely a temporary phenomenon. We thus based our analysis on the more conservative assessment that we present here.

[9] This is different for debit card transactions. In the U.S., the Durbin Amendment of the Dodd-Frank Act restricts the interchange fees for debit transactions to 0.05% + \$0.21; before this law came into effect by 2011, average fees were about \$0.44. In addition to these fees, payment processors usually charge a markup in the range of \$0.10-\$0.20 plus a percentage of the transaction value.

Conflux chain. These liquid tokens receive no interest. This state is similar to money kept in a "chequing" or "current" account at a bank: in most western countries today such funds do not earn interest but they are available for immediate use.

User can also designate their tokens as "stake". In that case, they are locked, not available for immediate use, and therefore illiquid. Such staked tokens receive interest payments in the form of newly minted tokens. This interest per token accrues while the token is staked and it will be paid at the time when the user unlocks their token and converts it to the liquid form. The staking/locking and un-staking/unlocking process, however, takes time and consumes gas costs. It is analogous to money kept in a savings account: such funds receive interest payments but are usually not available for immediate use and/or may incur fees while releasing them. The technical details of staking/unstaking can be found in the technical white paper of the Conflux network.

We present an analysis on interest payment in the following content. For the sake of simplicity, we assume that the locked genesis tokens are released at a constant rate daily over a 4-year period (they are released at quarterly intervals). Let $G = 5,000,000,000$ be the amount of genesis tokens that are locked at main-net launch. To simplify the analysis, we assume that these are released at a constant rate of n per day since the launch such that $n \cdot 365 \cdot 4 = G$.[10] In other words: $n \approx 343K$ tokens are released each day.

Assume that users (including those who hold released genesis tokens) will lock/stake on average a fraction α of their tokens. Then $\alpha \cdot d \cdot n$ tokens are eligible to receive interest payments on day d, while the remaining $(1 - \alpha) \cdot dn$ tokens are liquid and available for transactions. For much of our analysis, we assume that users stake all their tokens,

[10]Most of these tokens are released at fixed, contracted intervals.

$\alpha = 1$, so that they receive interest whenever possible and unstake only right before they want to use their tokens.

Conflux pays a daily amount of accrued interest R per staked token in the form of newly minted tokens. Those tokens expand the monetary base and therefore lead to inflation. We also assume that Conflux will set a goal for the annual rate r_c such that over a year, $G \cdot r_c$ newly minted tokens from interest payments are added to the monetary base. To simplify the exposition, we further assume here that the newly minted interest tokens are returned to miners as liquid tokens.

Since interest is compounded per block creation during which the tokens are locked, for an annual equivalent rate r one needs to find the value for R such that the total interest payments add up to $G \cdot r_c$ tokens

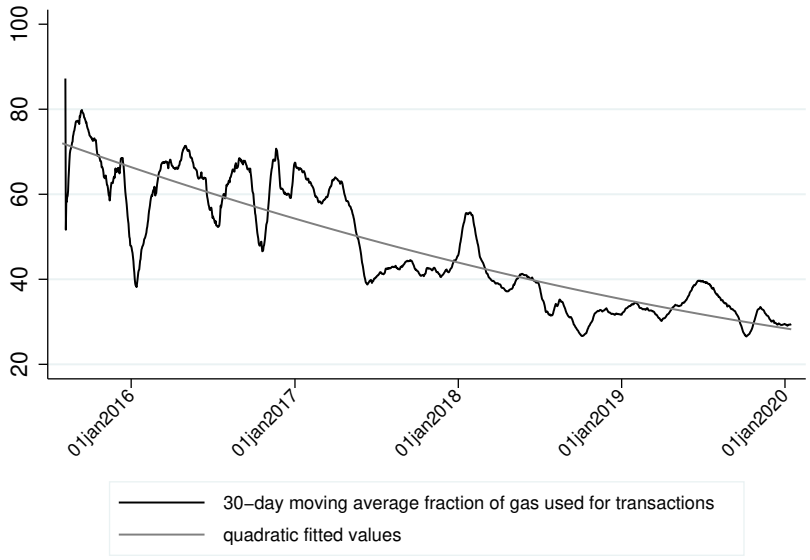
$$\underbrace{G \cdot r_c}_{\text{total annual interest}} = \underbrace{\sum_{d=1}^{365} R \cdot \alpha \cdot d \cdot n}_{\text{sum of individual interest payments}} \quad \Leftrightarrow \quad R = \frac{8}{366} \cdot \frac{r_c}{\alpha}. \tag{7}$$

F. Transactions vs. Computations

In the description so far we treat transactions as a synonym of the usage of the underlying network. However, notably, a Turing-complete blockchain can do much more than process transactions. To understand this issue, consider Figure 4. The solid black line plots the daily transactions on the Ethereum blockchain. The gray line plots the fraction of Gas attributable to transactions in percentile.[11] As the figure illustrates, over time plain vanilla token transactions account for a decreasing proportion of transactions.

[11] Formally, we derive this line as follows. We obtain from `etherscan.io/chart` the data series for daily transactions and daily Gas used. A simple transfer of ETH transaction requires 21,000 Gas, and we therefore obtain the non-transaction Gas amount by subtracting the number of transactions times 21,000 from the total gas.

Figure 4
Transactions vs. Computations



As with user uptake, we use the Ethereum blockchain activities as a benchmark for the expected behavior on the Conflux network. Specifically, we run an OLS regression for a quadratic fit for the non-transaction rate:

$$\%\ \textit{non-transaction gas} = \alpha + \beta_1 \cdot d + \beta_2 \cdot d^2 + \epsilon, \tag{8}$$

where d is the number of days since main-net launch. The goal here is to measure the $\%$ *non-transactional gas* as a quantity $\in [0, 100]$. Table III contains our estimation results. In additional to the raw rate, which is very noisy at the beginning of the sample, we use the 30-day moving average of the fraction of non-transactional gas used. The results are

Table III
Quadratic Curve-Fitting for Ethereum's Non-Transaction Gas Usage Rate

The table contains the results for our non-linear least squared regression of (8) using data for Ethereum's the fraction of daily non-transaction gas usage on Ethereum. MA refers to a 30-day moving average. T-stats are in parentheses. *, **, *** indicate statistical significance of the respective coefficients at the 10%, 5%, and 1% levels.

	% non-transactions	MA(% non-transactions)
β_1	-0.04***	-0.04***
	(-17.952)	(-26.239)
β_2	0.00***	0.00***
	(5.598)	(7.710)
α	71.88***	72.07***
	(94.875)	(141.995)
Observations	1,623	1,623
R-squared	0.615	0.782

very similar. We note that the parameter estimated for the quadratic term, β_2, is very small, around 7.05×10^{-6}, owing to the size of the associated variable.

So far in this subsection, we have discussed the usage of gas for non-transaction purposes. In what follows, we need to determine the amount of interest that miners receive for storing smart contract code. We measure miner income against transactions because user fees are paid per transaction and a block has a fixed capacity in terms of number of transactions. A more intuitive approach would be to measure this quantity against gas usage. To keep the analysis coherent, we convert the fraction of non-transactional gas into hypothetical transactions and then we make the interest payments a function of these hypothetical transactions. Specifically, let $\gamma(d)$ denote the fraction of gas usage that is not attributable to remittance-like CFX transactions. Following Table III,

we obtain:

$$\gamma(d) := 1-\left(72 - 0.04 \cdot d + 7.05 \cdot 10^{-6} \cdot d^2\right)/100 = -0.0000000007(d-2,837)^2+.85. \quad (9)$$

Therefore, when there are $T(d)$ transactions on day d, we say that $(1-\gamma(d)) \cdot T(d)$ of these are simple coin transfers and $\gamma(d) \cdot T(d)$ involve smart contract executions that require data storage on the chain.

G. Interest Payments to Miners

When using the chain to store information (such as smart contract code), users have to put a certain number of tokens into bonded storage. These tokens earn interest, and the interest is paid to the miners (and not to those who put the tokens into storage).

In calibrating the model, there is a possible scenario that a user buys storage (*i.e.,* put tokens into bonded storage) but never executes the contract hereafter. To tackle this, we make the assumption that users make the decision of whether to keep tokens in bonded storage each day and, therefore, that the total transactions fully reflect the extent of interest payments. In other words, we account for only "new" bonding of tokens. As such, the calibration model likely *conservatively underestimates* the interest income to miners.

Conflux determines how many tokens users must put into bonded storage relative to the amount of space that the contract occupies. We assume that this amount is proportional to the gas usage of the contract or, as one may argue, the number of actual transactions since each of them requires gas.

As such, for x transactions, users need to put $\beta \cdot x$ tokens into bonded storage and on day d it is $\gamma(d) \cdot T(d)$ transactions that require users put tokens into bonded storage.

In total, the required amount is $\beta \cdot \gamma(d) \cdot T(d)$. We conclude that each day the miners receiving interest paid on these bonded tokens as described in (7) is the below:

$$I(d) := \beta \times \gamma(d) \cdot T(d) \times R. \tag{10}$$

H. CFX Price

Roughly speaking, the market cap of the Conflux network is the market price of the tokens multiplied with the number of outstanding tokens. In addition to market-driven changes to the token price, CFX changes subject to built-in inflation because the price per token relative to fiat money, ceteris paribus, falls when the number of outstanding tokens increases. This is not to say that the network becomes less valuable, it merely means that there are now more tokens available for usage in the network. This inflation rate is caused by the expansion of the monetary base in the forms of block rewards and interest payments.

Let $p(0)$ denote the initial price of a CFX token. At the launch of the mainnet, the number of tokens outstanding is $G = G(0)$. After d days, the number of tokens has increased by the block rewards and interest payments as illustrated below:

$$G(d) = G(0) + \underbrace{b(d) \cdot d}_{\text{block rewards}} + \underbrace{\sum_{j=1}^{d} R \cdot \alpha \cdot j \cdot n}_{\text{interest payments}}, \tag{11}$$

where the interest payments simplify to

$$\sum_{j=1}^{d} R \cdot \alpha \cdot j \cdot n = \frac{d(d+1)}{365 \cdot 366}\, G(0) \cdot r_c.$$

Assuming no exogenous forces, the market driven changes to the price of CFX token on day d is:

$$p(d) = p(0) \cdot \frac{G(0)}{G(d)}. \tag{12}$$

Using the derivations in (1) and (7), the price of CFX is therefore:

$$p(d) \;=\; p(0) \cdot \left(1 + \frac{d}{365}\, r_b + \frac{d}{365}\frac{d+1}{366}\, r_c\right)^{-1}. \tag{13}$$

Based on our current information, at main-net launch a CFX will have nominal value of \$0.1 and the aggregate value of the network is \$500M. As of the beginning of 2020, the Ethereum network had a market cap of around \$16B, that is, x32 times that of Conflux. Notably, Ether's price started to trade around \$1 at launch and it is now above \$300. In the later part of this paper, we develop an equilibrium model of token usage and mining costs that helps underpin how the token price depends on the *utility* that the network (and therefore, the miners) provide to users.

I. Total Miner Revenue

To summarize, total miner revenue,[12] denoted by $m(d)$, consists of *(a)* the block reward from equation (1), *(b)* interest income from bonded tokens as shown by equation (10), and *(c)* user fees expressed by equation (6):

$$\begin{aligned} m(d) &= p(d) \cdot b(d) + p(d) \cdot I(d) + F(d) \\ &= p(d) \cdot \frac{G r_b}{365} + p(d) \cdot \beta \times \gamma(d) \cdot T(d) \times R + f \cdot T(d). \end{aligned} \tag{14}$$

[12]We assume that block rewards and interest income is converted to fiat equivalent using the price of CFX as derived by equation (13).

In the next subsection, we provide simulations to illustrate possible revenue levels with reasonable model parameters.

J. Calibration of Miner Revenue

Before presenting the calibration results for Conflux miner revenue, we shed some lights on what Ethereum miners currently earn for their work. There are around 6,500 blocks created per day, paying around 13,500 ETH so that the total average daily block rewards is a just shy of $3M USD (based on ETH prices of early 2020).[13] For Ethereum, user-paid transaction fees play a negligible role in miner income, whereas for Conflux user fees are expected to play a more significant role due to its high throughput. However, as early on, there will be few transactions while the network gains traction. Therefore, for our calibration we average miner income over relatively long horizons. Below, we compute year-long averages in 91-day intervals:

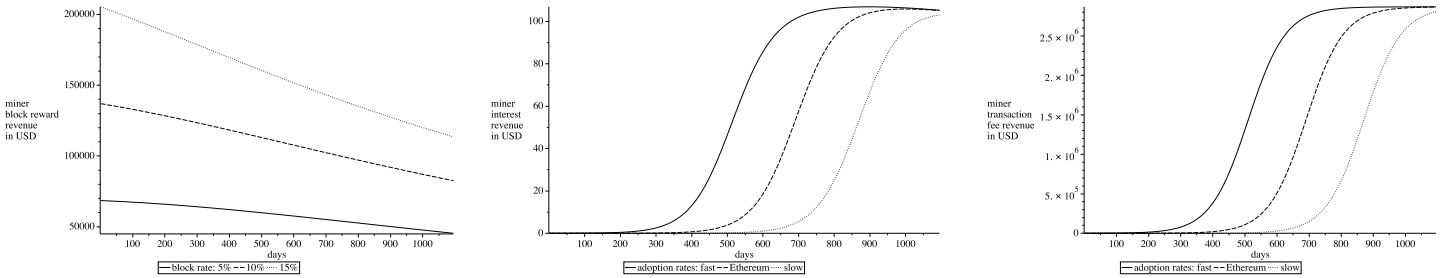
$$\bar{m}(d) = \frac{1}{365} \sum_{d'=i\cdot 91+d}^{(i+4)\cdot 91+d} m(d'), \quad i = 0, \ldots, 7.$$

We use four values for average transaction fees, $f \in \{.005, .01, .02, .08\}$, where the highest number $0.08 corresponds to the low-end median fee paid on Ethereum in early 2020, as we discussed earlier. For the uptake rate, we consider the three benchmark rates $u^{\text{fast}}(d)$, $u^{\text{ETH}}(d)$, and $u^{\text{slow}}(d)$ from Subsection C. For the required amount of bonded storage, we use $\beta = 1\%$ meaning that if the user occupies space on the blockchain for future computation that is equivalent to what 1 virtual-machine opcode transaction occupies, then this user has to put 1/100 of a CFX token into bonded storage.

[13] Source: `bitinfocharts.com/ethereum/`.

In the below, we make no assumptions about market-driven price appreciations except where explicitly stated.

As a first step, we separately plot the three components of miner revenue: block rewards, interest income, and user fees. Figure 5 plots these daily revenues. These figures use an annual interest payments of $r_c = 4\%$, and average fees of \$.01.



Panel A: Block Rewards *Panel B: Interest Income* *Panel A: Transaction Fee Revenue*

Figure 5
Miner Revenues over time as a Function of the Adoption Rate

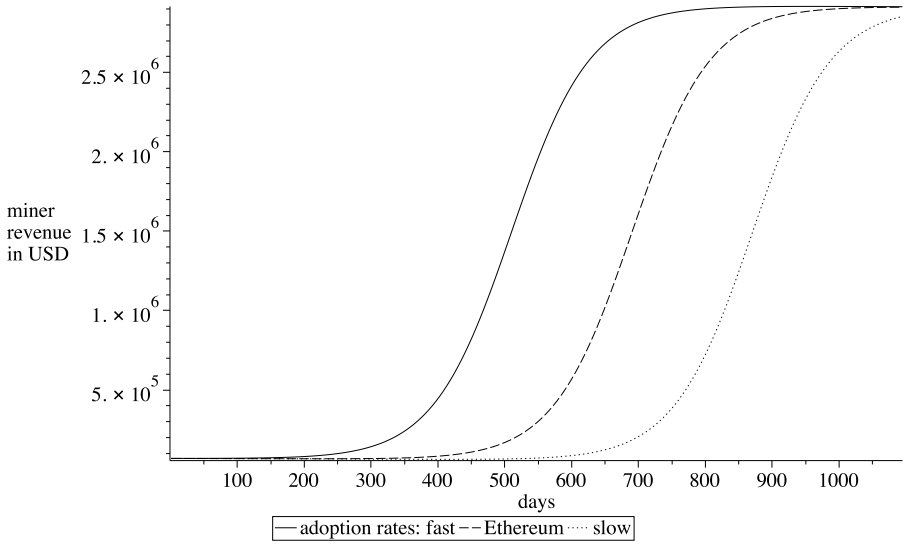


Figure 6
Miner Revenues over time as a Function of the Adoption Rate

In Figure 5, the $-value of block rewards (Panel A) declines because the price declines due to inflation; note that we assume that the number of tokens given as a block reward is constant within the interval. For the remaining two panels, we set the annual block inflation rate to $r_b = 5\%$. Interest income (Panel B) rises with blockchain usage, but it is small in magnitude. Finally, user fee revenue (Panel C) plots fee income. The values recorded on the vertical axis indicates that these fees are expected an order of magnitude larger than interest income or block reward income, except immediately after the launch of the main-net.

Combining these three figures, Figure 6 plots expected daily miner revenue $m(d)$ over three years following the launch of the main-net for the three different user uptake speed scenarios. This figure uses an annual block inflation rate of $r_b = 5\%$, annual interest payments of $r_c = 4\%$, and average fees of $.01.

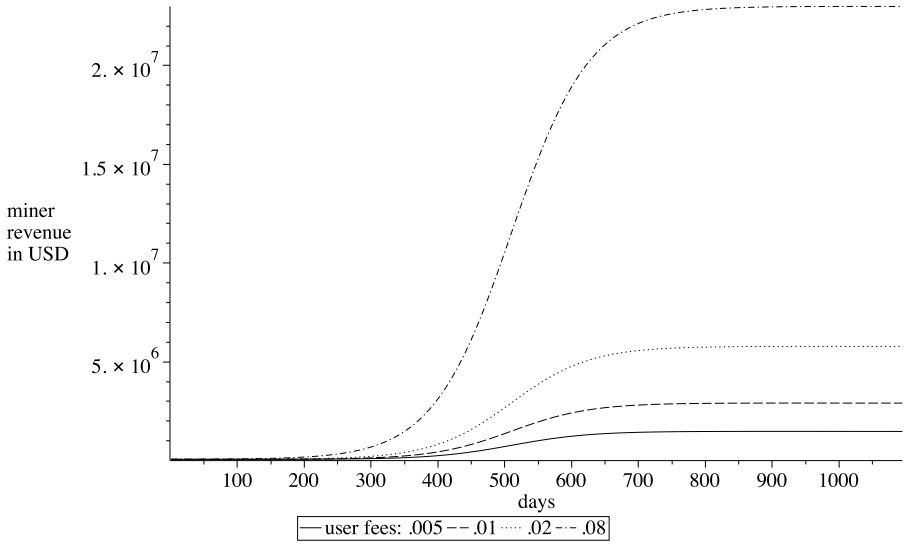


Figure 7
Miner Revenues over time as a Function of Average Fees

Figure 7 shows the time series of expected miner revenues per day with the four different average transaction fees. When Conflux is at capacity, even for moderate fees of \$0.02, miner revenue will be around \$2.5M. This figure uses block inflation rate of 5%, interest payments of 4%, and Ethereum-like adoption rates.

For the sake of the argument, we also consider a situation when market forces lead to increases in the price of CFX tokens such that in three years Conflux has the same market valuation as Ethereum today, that is, roughly a \$15B market-cap. Further assume that the price change follows linear growth at some rate g such that the price at time d is $p^{\text{ETH}}(d) = p(0) \cdot (1+g)^d$. The rate g that ensures that the market evaluation of Conflux three years after launch is the same as Ethereum at the beginning of 2020 is $g \approx 0.0031$. We now compute total miner revenue using the "speculative" price $p^{\text{ETH}}(d)$, i.e., in (14),

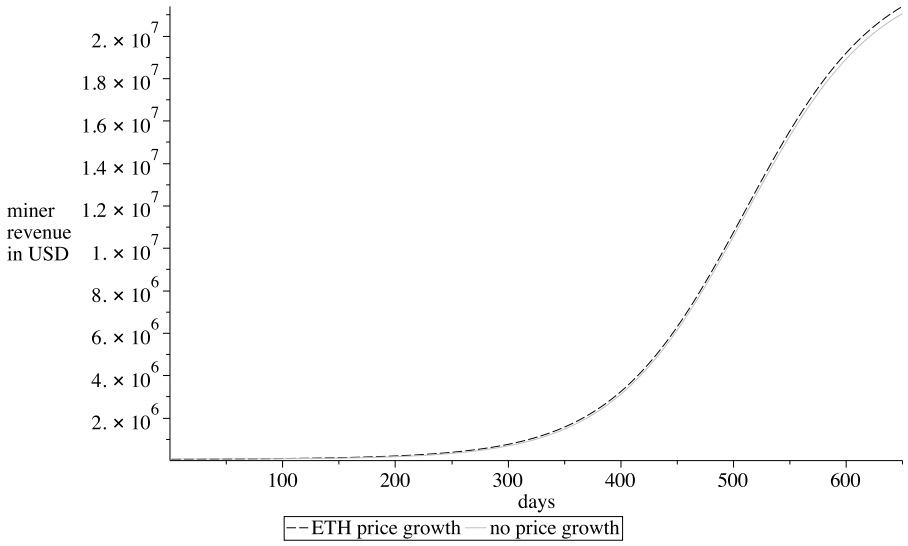


Figure 8
Miner Revenues if prices would grow to ETH levels

we substitute $p(d)$ with $p^{\text{ETH}}(d)$ so that we obtain:

$$m^{\text{ETH}}(d) \quad = \quad p^{\text{ETH}}(d) \cdot b(d) + p^{\text{ETH}}(d) \cdot I(d) + F(d) \tag{15}$$

Figure 8 shows the time series of expected miner revenues per day for this alternative price path, p^{ETH}, where we plot only the first 650 days. In this Figure, we use a block inflation rate of 5%, interest payments of 4%, Ethereum level adoption rates, and willingness to pay fees at current Ethereum rates ($0.08). We also include the revenue case when there is no price growth (it corresponds to the most "optimistic" case in Figure 7) as a point of reference. The *key* takeaway from this figure is that when we assume that prices rise significantly, miner income in the medium run is not affected, simply because transaction fees continue dominate.

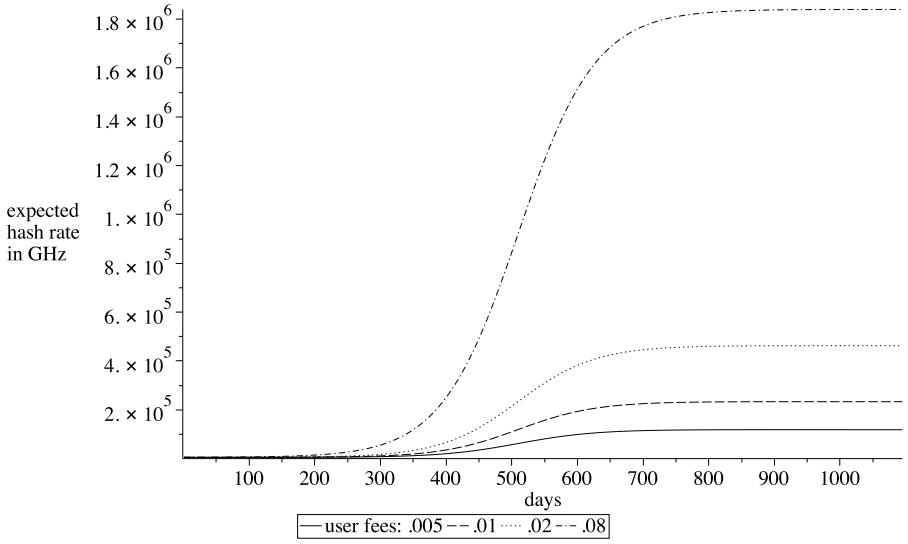


Figure 9
Hashing Power over time as a Function of Average Fees

Since miners compete to build blocks and incur a notable cost of computation power, the expected revenues relate directly to the miners' willingness to provide hash power. At current prices, miners receive on average \$12.5 per GigaHz of hashing power.[14] Figure 9 transfers Figure 7 by relating the hashing power that miners would be willing to provide given the predicted the mining rewards.

Finally, we show how inflation from block rewards and interest payments affect mining revenue. Figure 10 plots the average mining revenue as a function of the block reward, measured through block inflation. We plot the curves for the first year (all medium-gray lines), and then for the second to fifth quarter (black), and third to sixth quarter (light gray). We use interest payments of 1%, 5%, and 10%, and average fees of \$.01. Adoption is based on the Ethereum adoption levels (u^{ETH}). The figure indicates

[14]To obtain this number, we use data from `etherscan.io` on total daily hashing power of the network and average block revenue.

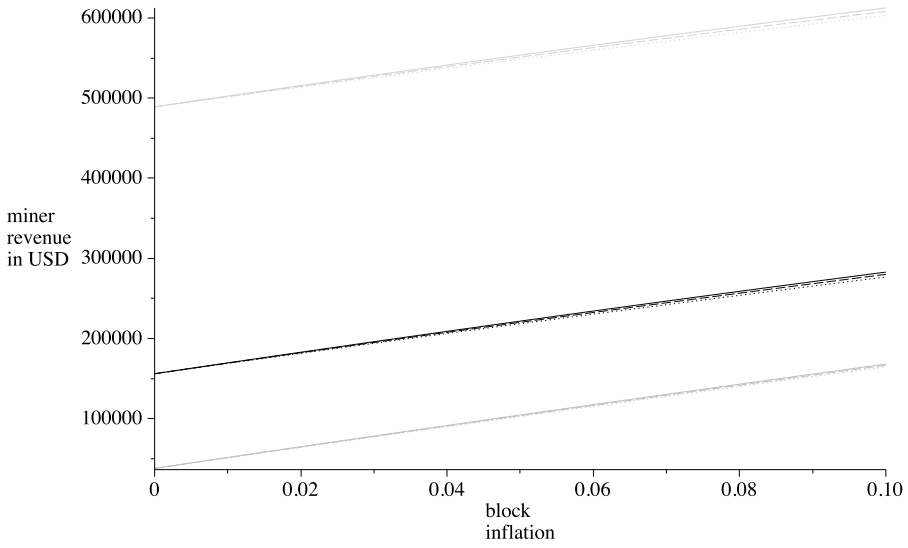


Figure 10
Average Revenue and Block Inflation

that block rewards have a significant effect on miner income, while the interest rate has limited impact.

Figure 11 confirms these latter insights. In this Figure, we plot the average mining revenue as a function of the interest rate. Again we plot the curves for the first year (all medium-gray lines), then for the second to fifth quarter (black), and finally third to sixth quarter (light gray). For this, we use block inflation rates of 1%, 5%, and 10%, and average fees of \$.01. Adoption is again based on the Ethereum adoption levels (u^{ETH}). The lines are essentially flat, as indicated by the earlier figures, simply because miner income from interest rate is so small. We conclude that early on, block rewards play the most important role in miner income at the beginning, whereas, once a certain adoption rate is reached, user fees will be the most important source of income. We emphasize, however, that this is not to say that interest is irrelevant for user decisions.

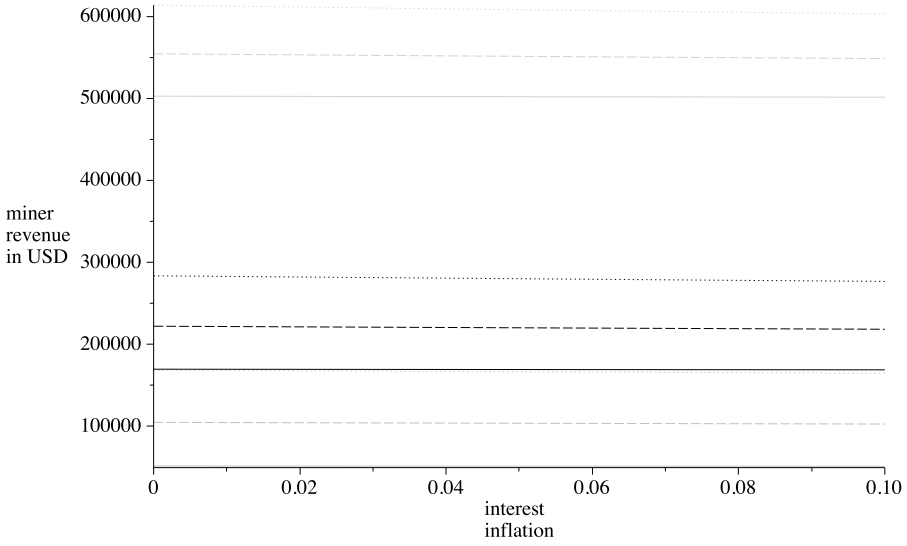


Figure 11
Average Revenue and Interest Rates

Instead, there will be many users who each have to pay a small but possibly for their case significant implicit fee for storing data on the network.

VI. Economic Limits against Attacks

In this section, we examine the limits of the Conflux network under two different attacks, the selfish mining attack and the double-spending attack.

A. Selfish Mining Attacks

If a participant in Bitcoin holds more than 23.21% of the network computation power, she can gain more mining profit by strategically withholding her mined block for a period of time before broadcasting them to the network (Sapirshtein, Sompolinsky, and Zohar 2015). This is because Bitcoin only gives reward to the blocks in the longest

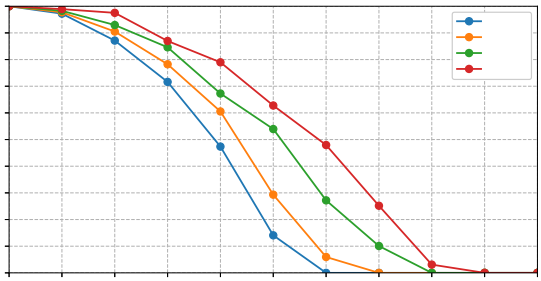


Figure 12
Penalty of attackers on different attacker ratios of block generation power (A)

chain. When she withholds the newly mined block, she has the exclusive privilege to mine under her new block which is the current longest chain. Of course, withholding the block brings the risk that someone else may mine a new block concurrently to become the new longest chain, but the study shows that if the participant has more than 23.21% of the network computation power, the benefit of withholding will outweighs the risk; see Sapirshtein, Sompolinsky, and Zohar (2015). Because Bitcoin mining is a winner-take-all game, honest miners expect to get less reward comparing to their computation power when the selfish participant launches such fairness attacks.

Conflux is more resilient against selfish mining attacks because withholding a block leads to less reward. Unlike Bitcoin, all blocks receive reward in Conflux and the reward of a block is discounted by its anti-cone size. Withholding the block will prevent future new blocks from referencing it. Therefore, it increases the anti-cone size of the block and consequently decreases the block reward. Given all network participants are rational, honest mining is incentive compatible.

Figure 12 presents our experimental results to illustrate the resilience of Conflux against selfish mining attacks. We run a Conflux network simulation with 10000 nodes. One of them is the attacker which will withhold her generated block for a certain period of time. In the simulation, normal nodes have the network delay (4.1 seconds in average). The attacker, however, has the capability of instantly receive and send its block to all other nodes. We run the simulation for 2000 blocks and measure the reward ratio the attacker receives comparing to the normal honest strategy for the last 1000 blocks under different the block generation power and the block withholding period. Our results show that the attacker consistently receives less reward than she would with the normal honest strategy (i.e., the reward ratio is less than 1). The longer she withholds the blocks, the less reward she will receive. More computation power will help the attacker to receive more reward, but even with 40% of the computation power of the whole network, the attacker would still get more reward if she just participates the network honestly.

B. Double Spending Attacks

Several works in the economics literature highlight that PoW networks face fundamental constraints in terms of the economic incentives that can sustain ongoing security of the network (Auer 2019). The Conflux network is no different but in what follows, we argue that the constraints of Conflux are "looser" when compared to existing networks. In this section, we impose the limitation that the attacker is not capable of reversing cryptographic functions, therefore honest miners behave correctly even with the presence of an attacker. We focus on double-spending attacks with selfish mining through withholding of blocks.

We first repeat the arguments from Budish (2018) which apply to serial blockchains. We assume that the mining of each block involves a cost c (including physical equipment and electricity) and that there are N identical miners who compete. For the scenario with negligible user fees, the most significant revenue is the block reward B per block. The miners' participation constraint requires the expected gain to exceed the expected cost, that is:

$$\text{probability of winning the block} \times B \geq \text{cost} \quad \Leftrightarrow \quad B/N \geq c.$$

This condition holds for all identical miners, and in equilibrium it must hold that the aggregate cost of mining agrees with the aggregate benefit:

$$c \times N = B. \tag{16}$$

Now suppose an attacker wants to double-spend a transaction of value V. The attack proceeds in the sense that the attacker builds an alternative chain faster than all remaining miners. Assume that to gain 50% power, the attacker has to pay $c \times N$, and to gain a majority they have to pay in excess of this. If the attacker spends $A \times c \times N$ on equipment, with $A > 1$, they gain an advantage of $A/(A+1) > 50\%$; the larger A, the larger the advantage (and thus the faster they finish the attack). For a successful attack, they earn value V, which is the amount that they can double spend. Assume that, conditional on the equipment advantage A, it takes t blocks (in expectation) to complete the attack, that is creating a longer chain than the chain honest miners collaboratively generating. Then the cost of the attack is:

$$t \times A \times c \times N.$$

Once successful, however, the attacker earns not only the attack value V but also rewards for the t blocks. Therefore, for attacks to be *unattractive*, it must hold that:

$$t \times A \times c \times N > V + t \times B. \tag{17}$$

Using equation (16), we obtain the following:

$$t \times B(A-1) > V. \tag{18}$$

Therefore, for an expected attack time t, there exists a value $\mathcal{V}$ such that for all $V > \mathcal{V}$, $t \times B(A-1) = \mathcal{V} < \mathcal{V}$, and the transaction of value V cannot be secured. Inequality (18) is a firm constraint on the economics (and the security) of a serial chain such as Bitcoin.

Conflux subjects to a different lower bound for V. First, to be successful in an attack, the attacker's alternative chain must become the pivot chain. Since any epoch may contain multiple blocks, not only the attacker needs to create blocks faster, but also to generate a "heavy" chain, which will require relatively more time (and thus more resources). To simplify the argument, we abstract from this issue and assume, as before, that the honest chain contains a single block per epoch.

Next, when creating the alternative chain, an attacker does not receive the full reward because block rewards are assigned based on the relative position in the block's anti-cone in the next 10 epochs. As before, suppose the attack succeeds after t periods, and there is a single attacker in the system. Then the attacker's first block in the alternate chain has an anti-cone of size $\min\{t-1, 10\}$, the second of $min\{t-2, 10\}$, and so forth. Therefore, the block reward for block a since the start of the attack is

$B \times \left(1 - (\min\{t-a, 10\}/100)^2\right)$ assuming a fixed per block reward B. For the longest chain (now the pivot chain) of length t since the start of the attack, the attacker will therefore earn:

$$\underbrace{B \cdot \sum_{i=1}^{t} \left(1 - \left(\frac{\min\{t-i, 10\}}{100}\right)^2\right)}_{\Pi_t} < t \times B.$$

Using the same argument as above, and therefore, the economic constraint for Conflux becomes:

$$B(tA - \Pi_t) > V \tag{19}$$

In other words, there exists a value $\mathcal{V}'$ such that for all $V \in (\mathcal{V}, \mathcal{V}']$, the following holds:

$$B(tA - \Pi_t) > V > B(tA - t)$$

The implication of this relationship is that the set of transaction values V that can be secured on the Conflux network is strictly larger than in "traditional" serial blockchains such as Bitcoin.

VII. The Storage Cost Model of Conflux

In this section, we develop a simple model to understand Conflux's storage cost rules.

We begin with the observation that users have the choice between consuming a service on Conflux or choosing to do so with an alternative technology. The latter does not have to be an alternative blockchain but could be, for instance, a financial service or a computing service in traditional economy. Users in this model, for all practical purposes, are developers who use Conflux as an infrastructure. In our theoretical model, we abstract from many complications, such as price fluctuations and other external forces

beyond the network's control, and focus on two groups of constituents: miners and users. Explicitly, the model does not consider holding of CFX for speculative purposes.

We write the model in static form with an implicitly assumption of a steady-state outcome. For instance, we assume that there are existing users who are paying for storage, so that miners receive storage rewards.

A. Miners

This portion of our model is inspired by He, Tang, and Wang (2019).[15] Miners buy or rent equipment to mine and they incur per block costs for mining and data storage, such as electricity and equipment; we denote these costs c as in the preceding section. Miners are non-strategic (i.e., they are price takers) and identical.

Miners receive income from three sources: the block reward B of newly minted tokens, user fees, and interest on user storage, I. We measure these items in Conflux tokens, and use p for the exchange rate of fiat money per token (i.e., the USD price of a token); consequently, $p \cdot B$ is the miner's income in fiat from receiving a block reward B. In our analysis here, we abstract from transaction fees to simplify the exposition.

When users consume quantity x of the blockchain good (e.g., contract executions, gaming transactions, all measured in tokens units), they need to put a fraction q (to be determined by the system) of tokens, i.e., $\beta \times x$, into bonded storage. These tokens (as well as all other tokens in the system) receive interest $\beta \times x \times r_c$, where r_c is the inflation rate set by the system. As we outlined above, this interest payment is distributed to the miners.

[15] They employ a standard economic model to analyse whether the Bitcoin chain is viable in the absence of block rewards, which is similar to our analysis.

We assume that miners are identical in terms of the hashing power that they are providing. Therefore, they have an equal chance of mining a block. There is free entry into mining, and therefore the aggregate hash rate H is akin to the total number of miners. If miners use hashing power h, they win the block with chance h/H. Since miners are identical, we set $h = 1$ to simplify the notation. In competitive mining, costs balance benefits and therefore

$$c = \frac{1}{H} \times p(B + I) \quad \Leftrightarrow \quad H = \frac{p(B + I)}{c}. \tag{20}$$

B. Blockchain Users

Users dedicate a total of w to the particular service that the blockchain or its alternative provide. The analysis is therefore a partial-equilibrium because we begin when the user has already made the decision to devote a certain portion of her budget to this service. The user chooses the amounts of the normal good and special (aka blockchain) goods to maximizes her utility. We denote the consumption of normal goods c and the requested blockchain service x is measured in CFX. Our implicit assumption is that all consumption occurs (or rather, it is assessed by the user) in fiat currency and therefore the user consumes $p \times x$ of the blockchain good in that fiat.

When deciding to use the blockchain good, the user needs to obtain tokens for direct payment and additionally $\beta \times x$ tokens to put into bonded storage.

After one period, the users consumes the residual amount that was in bonded storage in the form of the alternative good.[16] Since the Conflux chain creates new tokens in the interim, the purchasing power of these tokens (*i.e.,* the value of the tokens measured

[16]The inspiration here is that of an overlapping generations model where a user can consume one type of good only when she is young.

in fiat) declines and the stored tokens is worth only $p \times \beta \times x/(1 + r_c)$, measured in today's prices. Here, $p/(1 + r_c)$ is effectively tomorrow's price of CFX. Moreover, future consumption gets discounted at a rate $\delta < 1$.[17]

Miners receive interest from the bonded storage, where we implicitly assume a stationary equilibrium in the sense that at the time of forming the block, a past (representative) user has put an equivalent amount of tokens into storage as the current user. Blocks are produced at rate b over a common storage horizon, usually 1 year if we use annual rates for δ and r_c. Therefore,

$$I = \beta x \times r_c \times b.$$

Miners ensure the security of the chain, and we assume that chain security is increasing in the hash rate H. Security becomes relevant for the second period consumption in the sense that this consumption occurs with probability $\mathsf{Pr}(\text{secure}|H) = \mu(H)$, $\mu \in [0, 1)$, $\mu' > 0$, $\mu'' < 0$.

We assume the following additive form of the user's utility function:

$$U(c, x) = u_c(c) + u_b(x \times p) + \delta \mathsf{E}[u_c(\beta \times x \times p/(1 + r_c))|H], \tag{21}$$

with $u' > 0, u'' < 0$ and $\mathsf{E}[u_c] = f(H)u_c$. The user's budget of consumption c, tokens for usage x, and tokens for bonded storage βx must satisfy:

$$c + xp + \beta xp \leq w. \tag{22}$$

[17] In a competitive equilibrium, the real interest rate r in the fiat money market will capture time discounting and then $\beta = 1/(1 + r_{\text{fiat}})$.

Taken together, the user maximizes their utility by choosing the blockchain good consumption as

$$\max_x U(x) \quad = \quad u_c(w - xp(1+\beta)) + u_b(x \times p) + \delta f(H) u_c(\beta \times x \times p/(1+r_c)). \tag{23}$$

The solution to this maximization problem equals to:

$$0 = -p(1+\beta)u_c' + pu_b' + \delta f(H) u_c' \beta \times p/(1+r) \quad \Leftrightarrow \quad 1 + \beta\left(1 - \frac{\delta f(H)}{1+r_c}\right) = \frac{u_b'}{u_c'}.$$

C. Equilibrium Market Clearing

The total number of coins outstanding is $M > 0$. To simplify to analysis, without loss of generality here we assume a single representative consumer who behaves as a price taker. In equilibrium, the market must clear so that:

$$x^*(1+\beta) = M$$

As such, users must choose the quantity of tokens x^* that maximizes their utility, and miners must pick the break-even hash rate H^*.

D. Equilibrium Illustration and Comparative Statics

As a simple example of a utility function of consumption the logarithmic function $u_c(c) = \ln(c)$ and for $u_b(c) = \theta \cdot \ln(c)$. This then gives rise to the equilibrium conditions

$$p^* = \frac{w}{M} \frac{\delta\theta + f(H)}{\delta\theta + f(H) + 1}, \tag{24}$$

and equilibrium quantity

$$x^* = \frac{w}{p^*} \frac{1}{1+\beta} \frac{\delta\theta + f(H)}{\delta\theta + f(H) + 1}, \tag{25}$$

and for the hash rate

$$H = \frac{p^*(B + \beta r_c x^*)}{C}, \tag{26}$$

while normalizing b to 1.

The amount w can be interpreted as the overall size of the economy that the blockchain tries to replace, and w/p is the size of the economy measured in tokens. The linear log-utility formulation ensures that the hash rate and the inflation rate do not directly affect the user's choice. Implicitly, the inflation rate and the required bonded storage β and r_c have similar effects as both raise the cost for the user and it is intuitive that one is sufficient as a policy variable.

From the above equilibrium conditions we can obtain by differentiation of the equilibrium variables some first order effects.

1. The hash rate and demand are positively associated and positively re-inforcing. (e.g., demand increases in the hash rate, and the hash rate increases in demand).

2. An increase in the monetary base lowers the price.

3. An increase in the fiat market's interest rate (a decline in δ) decreases demand.

4. An increase in the Conflux inflation rate leads to an increase in the hash rate and thereby an increase in the token price (we note that miners do not account for holding costs of tokens — the implicit assumption is that they convert tokens into fiat immediately to pay their costs).

5. An increase in the money allocated to blockchain like activities or an increase in user preferences for blockchain goods (an increase in w or θ) increases the price and the hash rate.

6. An increase in the bondage requirement β depresses demand directly but increases the hash rate. The total amount is indeterminate and depends on the relative size of the aggregate marginal storage return, $M \cdot r_c$, and the block reward B.

VIII. Conclusion

Proof-of-work blockchains need to be carefully designed so as to create the proper incentives for users participate and use their resources mindfully: miners must be willing to secure the network, and users/developers must be incentivized top use the blockchain services. This paper describes how the engineering of the Conflux Network, a high throughput proof-of-work blockchain, leads to sound economic incentives that support a socially desirable behavior. In this paper, we parameterize the level of income, and thus network security, that Conflux can generate, and describe how this depends on user behavior and "policy variables" such as block and interest inflation. We also discuss how the underlying economic engineering design extends the Conflux Network beyond legacy PoW blockchains.

We emphasize that we are describing our understanding of the economic effects that the engineering of the network generates. We do not know, however, how users will ultimately behave.

There are some questions that are beyond the scope of this text. For instance, it remains to be determined how the community, eco-system, and public funds will operate. It is imaginable that they will all get merged. Although the system has provisions of

DAO-like voting, the respective funds has not yet been set up. In the long run, the protocol needs to be developed further, and maintenance of network components will be necessary. It is imaginable and advisable that Conflux sets up a regular source of income to support the long-term viability of protocol development. One example is to divert a de minimis portion of the gas payments from transactions to the fund, similar to a value-added-tax.

REFERENCES

Auer, Raphael, 2019, Beyond the doomsday economics of "proof-of-work" in cryptocurrencies, Discussion paper, BIS Working Papers No 765.

Bakos, Yannis, and Hanna Halaburda, 2018, The role of cryptographic tokens and ICOs in fostering platform adoption, Working paper New York University https://ssrn.com/abstract=3207777.

Budish, Eric B., 2018, The economic limits of bitcoin and the blockchain, Chicago Booth Research Paper No. 18-07 University of Chicago https://ssrn.com/abstract=3197300.

Canidio, Andrea, 2018, Financial incentives for open source development: the case of blockchain, Working paper IMT Lucca, INSEAD.

Chiu, Jonathan, and Thorsten V. Koeppl, 2017, The economics of cryptocurrencies – bitcoin and beyond, Working paper Queens University https://ssrn.com/abstract=3048124.

Cong, Lin William, Ye Li, and Neng Wang, 2018, Tokenomics: Dynamic adoption and valuation, Working Paper No. 2018-49 Becker Friedman Institute for Research in Economics https://ssrn.com/abstract=3222802.

Eyal, Ittay, and Emin Gun Sirer, 2013, Majority is not enough: Bitcoin mining is vulnerable, .

Fisch, Christian, 2019, Initial coin offerings (ICOs) to finance new ventures, *Journal of Business Venturing* 34, 1–22.

He, Ping, Dunzhe Tang, and Jingwen Wang, 2019, Proof-of-work (pow) blockchain network and its viability as a payment system, Working paper Tsinghua University https://ssrn.com/abstract=3441605.

Li, Chenxing, Peilun Li, Dong Zhou, Wei Xu, Fan Long, and Andrew Yao, 2018, Scaling nakamoto consensus to thousands of transactions per second, .

Li, Chenxing, and Guang Yang, 2020, Conflux protocol specification, .

Li, Jiasun, and William Mann, 2018, Initial coin offering and platform building, Working paper George Mason University https://ssrn.com/abstract=3088726.

Sapirshtein, Ayelet, Yonatan Sompolinsky, and Aviv Zohar, 2015, Optimal selfish mining strategies in bitcoin, .

Times, Statistic, 2019, Projected gdp ranking, data retrieved from `http://statisticstimes.com/economy/projected-world-gdp-ranking.php`.