Indie Protocol

A fast and incentive driven blockchain protocol for the indie digital age.

December 2023

Abstract

Indie is a blockchain protocol that supports community building and content publishing with cryptocurrency rewards. It combines concepts from Steem/Hive social medias with lessons learned from building decentralized applications and their communities. An important key to inspiring participation in any community, currency or free market economy is a fair accounting system that consistently reflects each person's contribution. Indie protocol is the first to attempt to accurately and transparently reward an unbounded number of individuals who publish *content*, without requiring paywalls or advertizing models, and shifting the source of monetization from the audience, and to the business chain that extracts economic value from the content.

Table of Contents

Intruduction

Indie Protocol was launched on 13th October 2015 with an agile community efforts since 2013 to build an industrial-grade decentralized Blockchain platform that is capable to process high-performance financial technologies that serves the individual financial freedom.

Furthermore, Indie Protocol represents the first decentralized autonomous cooperation or the concept of Blockchain as Organization (BaO) which enables Bit Shares holders of the core utility token (IND) to decide the future direction and governance aspects of Indie Protocol. For sake of clarity and to avoid confusion with other smart contracting platforms, Indie Protocol implements its contracts in form of operations. Even though Indie Protocol comes with over 50 implemented different operations, this document focuses on the description of Indie Protocol as a platform, its architecture as well as its governance system using the native core utility token (IND).

Indie Protocol is a technology that supports the digital generation entrepreneurs, investors, and developers with a common interest in building and participating in free market solutions by leveraging the power of globally decentralized consensus and decision making. Consensus technology has the power to do for economics what the internet did for information. It can harness the combined power of all humanity to coordinate the discovery and aggregation of real-time knowledge, previously unobtainable. This knowledge can be used to more effectively coordinate the allocation of resources toward their most productive and valuable use.

Bitcoin was the first fully autonomous system to utilize distributed consensus technology to create a more efficient and reliable global payment network. The core innovation of Bitcoin is the Blockchain, a cryptographically secured public ledger of all accounts on the Bitcoin network that facilitates the transfer of value from one individual directly to another. For the first time in history, financial transactions over the internet no longer require a middle man to act as a trustworthy, confidential fiduciary.

Indie Protocol looks to extend the innovation of the Blockchain to all industries that rely upon the internet to provide their services. Whether its banking, stock exchanges, lotteries, voting, music, auctions or many others, a digital public ledger allows for the creation of distributed autonomous companies (or BaO) that provide better quality services at a fraction of the cost incurred by their more traditional, centralized counterparts. The advent of (BaO) ushers in a new paradigm in organizational structure in which companies can run without any human management and under the control of an incorruptible set of business rules. These rules are encoded in publicly auditable open source software distributed across the computers of the companies' shareholders, who effortlessly secure the company from arbitrary control. Indie Protocol does for business what bitcoin did for money by utilizing distributed consensus technology to create companies that are inherently global, transparent, trustworthy, efficient and most importantly profitable.

Indie Protocol has went through many changes and has done its best to stay on top of Blockchain technology. Indie Protocol is using Consensus as the mechanism by which organized people decide upon unitary rational action. While not considered technology in the traditional since, consensus "technology" is the basis of democratic governance and the coordination of free market activity first coined by Adam Smith as the "Invisible Hand." The process of consensus decision-making allows for all participants to consent upon a resolution of action even if not the favored course of action for each individual participant. Bitcoin was the first system to integrate a fully decentralized consensus method with the modern technology of the internet and peer-to-peer networks in order to more efficiently facilitate the transfer of value through electronic communication. The proof-of-work structure that secures and maintains the Bitcoin network is one manner of organizing individuals who do not necessarily trust one another to act in the best interest of all participants of the network. The Indie Protocol ecosystem employs Delegated Proof of Stake in order to find efficient solutions to distributed consensus decision making.

Blockchain Architecture

Indie Protocol constitutes the following components which are described individually:

Transactions

When users want to interact with Indie Protocol, they construct so called transactions and transmit to the network. These present messages that contain instructions about what operation(s) a user wants to use. A common operation is the simple transfer operation that comes with transfer-specific instructions that provides the necessary information for this action, such as the sender, receiver, the amount to transfer as well as an optional encrypted memo. To allow multiple operations to take place subsequently, multiple operations can be bundled into a single transaction. To identify against the system, transactions are cryptographically signed by the users. These signatures authenticate a user and provide authorization for the operations in the transaction.

Blockchain

Indie Protocol serves as a journal (e.g. a ledger) of user-signed instructions that become a binding agreement as soon as they are included into a block. After inclusion into a block, the agreements are stored indefinitely by means of a hash-linked-list (the Blockchain). From this ordered sequence of transactions, a current state (think: account balances) can be determined by processing all transactions consecutively starting at the very first block. As we will see later, the software will ensure that instructions that are stored in the Blockchain have been successfully authenticated and validated. For validating and processing of operations, a common set of rules define the consequences of particular actions, which are part of the of the Blockchain protocol.

Networking

Indie Protocol merely defines a means of storage and can be used in a non-distributed, single-participant fashion as well as in a distributed internet-based mesh network often referred to as Peer-2-Peer (P2P) network. In the latter case, multiple parties are connected with each other in a way that incoming transactions are forwarded to every other connected participant. A transaction ultimately reaches a so called block producer. A block producer verifies incoming transactions against a hard-coded protocol and bundles them into a single block that is added to the existing Blockchain. At this point, a transaction is considered confirmed and executed. The effects of an executed operation on the current state are defined in the Blockchain protocol.

Consensus

Consensus is the process by which a community comes to a universally recognized, unambiguous agreement on a piece of information. In the context of Blockchains, consensus means agreement about the validity rules for transactions (i.e., the protocol), and the order in which they have been observed by the Blockchain. This ultimately results in an agreement about the state that is build deterministically from the those validity rules and the sequence of transactions. The most commonly known consensus scheme is Proof-of-Work (PoW), that is used by many Blockchains. Most dominant disadvantage is the heavy power consumption and the scalability in terms of transactions per second and confirmation times.

Indie Protocol makes use of a lesser known algorithm called Delegated Proof of Stake (DPoS) that was developed specifically to replace the wasteful ‘mining’ process, increase throughput and reduce reaction times of the Blockchain. It is a tremendous improvement when it comes to consumption of electricity.

DPoS allows to generate a new block at fixed rate (block production/confirmation time) with minimal computational requirements. This means that the Blockchain can process more transactions in significantly less time and at almost no cost when compared to PoW-based Blockchains1. Block production is performed by a set of so called block producers that take turns. After every turn, the order of block producers is randomized in a deterministic manner such that all parties agree on the new order.

Protocol

The most essential part of Blockchain technologies is here referred to as Blockchain protocol. It defines the behavior of the entire system including consequences and side-effects when processing transactions. Users utilize particular features by crafting a transaction that contains a particular letter-of-interest (also referred to as operation).

Since the Blockchain, as a storage, only stores incremental changes (e.g. transfers), the final balance of each account together with other information needs to be tracked separately in the so called current state. It is important to note that the protocol is deterministic in the sense that the very same state is generated when applying the same sequence of operations (as provided by the Blockchain). This makes Blockchain technologies tamper proof and auditable.

In Indie Protocol, over 50 operations are available (as of early 2018). Each of them hooks into the Blockchain protocol at least three times:

- Validation: During validation, the raw instructions (sometimes referred to as payload) are checked for consistency. E.g., in case of a transfer, we ensure that the amount to transfer is positive.
- Evaluation: In the evaluation step, the operation-specific instruction is validated against the current state of the Blockchain. In case of a transfer, we here ensure that the amount to be transferred is available in the account of the sender.
- Application: This step takes action in the sense that it modifies the current state. In the case of a transfer, we here reduce the account balance of the sender and increase the account balance of the receiver according to the amount of tokens transferred.

Example: Transfer operation

Consider a simple transfer operation that sends funds from one account to another. Here, the protocol defines the validation rules such that negative amounts are prevented. The evaluation ensures that the sender cannot transfer more than what is in his account balance. When applying a transfer from Alice to Bob, Alice is credited the transferred amount while Bob receives the amount. Here, transfer refers to the operation type, while the sender, receiver, and amount refers to the operation-specific instructions. Obviously, different operation types come with different instructions.

Extensibility

The Software behind Indie Protocol is extensively modularized and implements its operations independently of each other. This allows for adding new features once the corresponding code, which the implements validation, evaluation and application methods, reaches maturity. In a sense, operations on Indie Protocol are smart-contracts and allows for extending the range of functions of the system. In contrast to other smart-contracting platforms, however, Indie Protocol requires new features to be vetted by the core developers and approved by the IND holders before they can be installed by means of a network-wide protocol upgrade. As a consequence the platform is considered much more solid as new features require to go through multiple stages of quality assurance. These protocol upgrades are well coordinated and already happened 27 times (Q1/2018) in the past.

Performance and Scalability

Indie Protocol publicly demonstrated sustaining over 3,000 (three thousand) transactions per second and over 22,000 operations per second on a distributed test network. This technology can easily scale to over 100,000 (hundred thousand) or more transactions per second with relatively straightforward improvements to server capacity and communication protocols.

To achieve this industry-leading performance, Indie Protocol has borrowed lessons learned from the LMAX Exchange2, which is able to process 6 million transactions per second. Among these lessons are the following key points:

- Keep everything in memory.
- Keep the core business logic in a single thread.
- Keep cryptographic operations(hashes and signatures) out of the core business logic.
- Divide validation into state-dependent and state-independent checks.
- Use an object oriented data model.

By following these simple rules, Indie Protocol is theoretically able to process >10,000 (ten thousand) transactions per second without any significant effort devoted to optimization. To put things into perspective3, at peak times, the Ethereum and Bitcoin Blockchain jointly process roughly 0.7% of the peak capacity of Indie Protocol (Q1/2018) as prove from distributed stress testing.

Identity

Indie Protocol makes use of human-readable account names that have to be registered together with public-keys in the Blockchain prior to its usage. Thus, the Blockchain acts as a name-to-public-key resolver similar to the traditional domain name service (DNS). These named accounts enable users to easily remember and communicate their account information instead of using error-prone addresses. Depending on individual needs, applications making use of Indie Protocol can create environments which have full KYC (Know Your Customer) support through so called "whitelisting" which enables a maximum of control or transparency when so desired.

Permissions

Indie Protocol designs permissions around accounts, rather than around cryptography, making it easier to use. Every account can be controlled by weighted combination of other accounts and/or keys. This creates a hierarchical structure that reflects how permissions are organized in real life, and makes multi-user control over funds easier for users. Hence, Indie Protocol does technically not have multi-signature accounts, but has multi-account permissions. That said, each public/private key pair is assigned a weight, and a threshold is defined for the authority. In order for a transaction to be valid, enough entities must sign so that the sum of their weights meets or exceeds the threshold.

Authorities

Indie Protocol employs a first of its kind hierarchical private key system to facilitate regular keys and backup keys. Regular (active) keys are for day-to-day usage, while a separate backup (owner) key can be used to recover access to an account in case of loss of the regular keys. Ideally the owner key is meant to be stored offline, and only used when the account's keys need to be changed or to recover a lost key. Most software that supports Indie Protocol also facilitates the use of a Master Password that encrypts the client's keys locally.

Encrypted Memos

An account on Indie Protocol has a so called memo public key associated with it that allows for initiating encrypted communications between two parties by means of a shared secreted4 obtain via the Elliptic-curve Diffie-Hellman Algorithm. This allows to attach encrypted messages to transfers that only sender and receiver can decrypt.

A shared secret is a term known from cryptography and describes a piece of data, known only to the parties involved in a specific secure communication. The secret can be a password, a passphrase, a big number or any data as long as it is randomly chosen.

Referral Program

Furthermore, Indie Protocol has an integrated one-level referral system. Basically, everyone interacting on Indie Protocol needs to deduct a transaction fee. From that fee (currently) 20% go into the Working Budget (for future funding of development etc.) and the other 80% go into the referral program from where, the registrar (who arrange the registration fee and assisted the registration process) as well as the referrer (who brought the user to the registrar) receive a reward. To opt-out of the referral program, an account can be upgraded to a so called Life-Time Member (LTM) which replaces registrar and referrer for the original user to receive a 80% refund on his fees.

Fees

Similar to most other Blockchains, interacting with Indie Protocols comes with a fee for using its features (i.e. operations). Each operation comes with its own fee. However, any other token that is registered on Indie Protocol, next to the core native IND token, can be used as fee, if the governor of the other token chooses to support that. Additional to block production and project funding which can drain tokens from the working budget, there are transaction fees paid by users of Indie Protocol that go back into the working budget.

As a consequence, the total amount of IND in the working budget as well as the total in- and out-flow highly varies over time. However, if compared to most proof-of-work-based Blockchains that constantly reward a (more or less) fixed amount of tokens to miners, Indie Protocol has a chance to have the working budget grow and consequently the circulating supply shrink. This is the case if the total transactions fees outweigh the tokens used for block production and project funding.

While, the IND holders have choices to either increase or decrease the funds used for block production and project funding, the committee has the choice to adapt the transaction fees by means of updating the fee schedule. In contrast to other Blockchains, Indie Protocol comes with fixed fees instead of a fee market. The schedule defines which feature of the Blockchain requires which amount of transaction fee for using it.

Core Token

The native utility core token of Indie Protocol is IND, it serves as a utility token and is offering governance properties to its holders. Governance describes the progress of governing the Blockchains many variable aspects in a way it it can adapt to future changes more easily.

Governance

On Indie Protocol, decisions are made by the holders of IND core native token weighted by the amount of IND owned. In order to improve voting participation and simplify the life of IND holders, voters can either vote directly or delegate voting power to so called proxies. This is similar to a representative democracy, where selected persons decide the course of action. Those leaders have to account for their actions and can be unelected by the core token holders. Unwanted actions includes censoring, favoring, or simply failure to produce blocks in a timely manner. However, the difference to a democracy is that voters in the community have their vote weighted by the amount of IND that they own in their account.

At any time, voters have to decide on the following aspects of Indie Protocol:

Members for Block Production

Block production in Indie Protocol is arranged through DPoS which requires block producers to run for witness and campaign for sufficient votes from IND holders before they can produce blocks on the Blockchain and consequently get rewarded per produced block. Given the governance system and quick re-tallying of votes, a misbehaving block producer can be dismissed within hours. Next to the actual selection of block producers, the voters also have a say over how many block producers should exist.

Committee

The Committee comprises a board that has control over a few Blockchain parameters such as block size, block time, witness reward, and over 30 others. Additionally, the committee can change the fee schedule which defines the minimum fee for each operation offered by the system. Voters can cast a vote for how many members the committee should constitute as well as vote for a particular set of members.

Workers

Last but not least, the voters have control over who receives funding from the Working Budget of the Blockchain. A worker applies for project funding and needs to campaign for sufficient votes before being rewarded. Similar to block producers and committee members, the rigorous voting system allows almost immediate removal by IND holders and proxies.

A certain amount of the daily available tokens can be allocated to make development possible by means of workers for projects funding. Anyone can set up a worker on Indie Protocol and ask for a daily allowance in IND. If the IND holders approve a particular worker, the IND are transferred from the daily budget. A Soft-limit defines the maximum amount of the daily budget that is given to all approved workers. Consequently, those workers that have received more votes from IND holders will receive their funds first. This means that workers, even if approved, may not be funded if the aforementioned threshold is hit. Furthermore, workers constantly stand under the scrutiny of the IND holders who can disapprove (e.g. fire) workers that do not deliver.

Supply

In this section, we would like to discuss the actual supply of the core IND token in more detail. Firstly, we define the max supply as that supply that can at most be in circulation, similar to how there will only ever be up to 21 million BTC on Bitcoin Blockchain. Furthermore, the circulating supply represents that amount that currently is in circulation and

held by participants on the Blockchain. Obviously, the circulating supply will always be smaller than or equal to the max supply. Furthermore, for voting, only the circulating supply applies.

Initial Allocation

Indie Protocol will be launched without any ICO, token sale or any pre-mint. Indie Protocol will be initiated by the community when they decide that the core functionality reached a ready state. It was based on code developed for Bitshares and given to the world for anyone to use under the MIT license.

In the genesis block of Indie Protocol a total of XXX,000,000,000.00000 IND will be allocated to the blockchain reserves (treasury). These IND can still be claimed by proving ownership of the corresponding private key. The IND token comes with a limited supply that is different from circulating (liquid) supply.

A max supply of XXX,000,000,000.00000 IND has been put in place on the Blockchain. This can never change. The supply is set aside for future project funding and rewarding block producers, and is only accessible with approval by the IND holders through the worker system. This so called working budget is also often referred to as reserves. It is worth noting that revenues made from transactions fees are not shared with holders of IND but instead go back into the working budget to further allow future development. There is no reward for holding the core IND token in any way.

Working Budget

The difference between max supply and circulating supply is called the Working Budget and has often in the past been referred to as the reserves.

Indie Protocol has a daily budget to use for development. This budget has a hard-coded upper limit of Total funds in the working budget / 2924

From this daily budget, block production as well as for project funding are made. Of course, the IND holders have the choice and need to approve IND tokens leaving the working budget.

Block Producers

Block production comes at a cost for running and maintaining equipment. Indie Protocol acknowledges this fact by rewarding block producers in core IND tokens per produced block. Depending on the valuation of IND, the committee can modify the amount of IND rewarded per block. As of Q1/2018, each block is rewarded with 1 IND. Those IND are taken from the working budget.

Legality

As an infrastructure; Indie Protocol is a platform built using an open source code, running by elected nodes (block producers) from all over the world, it is similar to Bitcoin and Ethereum as an infrastructure, Indie Protocol is not a company nor a trademark or a brand, Indie Protocol doesn't have a legal responsibilities as a platform nor as code; users of Indie Protocol might have responsibilities or legal obligations for using it toward their legal jurisdiction depending on their own usage and the means behind it.

Legal entities cannot claim legal responsibilities of an open source code nor a decentralized Blockchain platform, they can operate client interfaces that is interfacing with the Blockchain and can bind to a legal partnerships for the sake of validating Blockchain certain data or can provide services on top of Indie Protocol platform through their own client interfaces which is interfacing with Indie Protocol using their own channels, internet domains, witness nodes or API nodes.

IND the utility token of Indie Protocol is used as utility for Blockchain operations fees and as power to participate in assigning active committee Blockchain users, assigning active witness nodes of Blockchain users and vote to issue utility token for development workers which are submitted by Blockchain users.