BasicIncomeToken

BIT Protocol White Paper (Draft)

"The Bit protocol is a DAO-based Protocol that implements a Universal Basic Income"

Introduction

Universal Basic Income is a critical societal movement that must exist for the world to continue to function as jobs continue to be replaced by automation. We live in a world with more abundant resources than ever before, yet there are still people who struggle to make ends meet. It is our duty as humans to ensure that every person has access to the core necessities of life. The Swift Protocol is a proposal that lays the framework for a DAO with the purpose of distributing Universal Basic Income. Worldwide adoption of the BIT Protocol will allow the dream of Universal Basic Income to become realized. The protocol has been designed with practical and proven solutions, with additional functionality to aid mass adoption.

Account Type

To create a transactional currency that provides basic income, some form of structure is required to ensure the following remain true:

1. A unique individual should only be allowed to have one account that receives basic income.
2. Accounts not tied to individual identities must be permitted to exist for business and privacy reasons.
3. The system must remain decentralized to avoid single points of failure.
4. Rules must be able to be modified over time to allow for the changing needs of an active economy.

To solve these issues the Swift Protocol proposes 4 different account types that together, fill these different responsibilities.

BIT Citizens

BIT Citizens are unique individuals that have been validated by an Identity Provider. Citizens have the ability to add claims to the blockchain once every day (days begin and end at midnight UTC). Bits will be awarded based on the number of days passed--with a maximum of seven. For example, if the three days have passed and a user makes a claim with the current production rate at 100 Bits, 300 Bitss will be awarded.

BIT Entities

Bit Entities are not connected to a personal real-world identity and therefore do not receive Basic Income. These accounts still must be approved by Identity Providers before being created. An Identity Provider must be linked to all Bit Entities, however Identity Providers are not allowed to make transactions on behalf of a Bit Account. Delegated Nodes and Identity Providers both inherit from the Bit Account type.

Delegated Nodes

Delegated Nodes are responsible for maintaining full nodes and creating new blocks. Each election cycle Swift Citizens will sign votes to help choose which Delegated Nodes they would like to represent them. This means that Delegated Nodes act as elected officials with the capability to vote on proposals to add/remove other Delegated Nodes and Identity Providers.

Identity Providers

Identity Providers are responsible for validating the identity of Bit Citizens and creating new citizens by generating a keypair for each new Bit Citizen and including the identity on the blockchain. Identity Providers have the added responsibility of protecting Bit Citizens whose keys they control with buyer and seller protections.

Income Distribution

The goal of the Bit Protocol income distribution model is to provide a fair method of providing Bits to all Bit Citizens. The distribution method also must ensure that the amount of Bits entering the system should never cause a decrease in value. To more quickly reach the state where a mature economy has formed, early users will receive extra daily Bitts during Stage One.

Stage One

In Stage One, income will be generated at an accelerated rate so the economy can grow to maturity within a shorter time period. During this stage, Bit Citizens will receive Bitts dependent on the number of Swift Citizens that are in the ecosystem. The formula to calculate the Income Distribution Multiplier is as follows: (781250 / (5^(log10(users)))) with a maximum value of 100, and minimum value of 1.

Stage Two

After the 70 Billion cap has been reached by following the formula of Stage One, Stage Two will come into effect. During this stage, new Bits will be given out to users at an inflation rate decided by the Delegated Nodes to all users in the ecosystem. It's their responsibility to choose an inflation rate that will avoid devaluing existing currency while ensuring the distribution is sufficiently large.

Referral System

When a new Bit Citizen joins, there's an option to include the public key of the Bit Citizen that referred them. Referral bonuses are calculated using 5 * Income Distribution Multiplier. For example, if there are 100,000 Bit Citizens at the time of a referral, the bonus would be 500 Bits.

DAO Based Governance

Governance is an integral part of the Bit Protocol as it allows for outside data to be safely used for identity verification and economic control. However, the decentralized and autonomous elements of the Bit Protocol allow certain rules to be set in stone. These rules ensure a fair system exists where nobody has the ability to cheat in a way that is possible with centralized systems.

The Bit Protocol features an internal system that simulates a decentralized government. Bit Citizens have the responsibility to elect representatives known as Delegated Nodes that will have various powers within the government. These Delegated Nodes are required to both maintain the blockchain, forge new blocks, and vote on proposals.

Election Duration

Elections will occur every six months for the first five years. Citizens will have a two-week time period in which they may cast their vote for their preferred Delegated Node. After the voting period has ended, a one-month grace period will begin--giving time for newly-elected nodes to prepare for their responsibility, and to prevent any potential splits in the chain.

Delegated Node Voting

Delegated Nodes have the following abilities

- Elect new Identity Providers.
- Ban existing Identity Providers.
- Revert the chain state to some time within the past 72 hours.
- Ban Delegated Nodes.
- Elect replacement Delegated Nodes.
- Choose the inflation rate in Stage Two.
- Vote on the salary for Delegated Nodes.
- Vote on the Salary Multiplier for Identity Providers.
- Vote to approve or disapprove funding proposals.

To perform these abilities, a proposal must be submitted to the blockchain by one Delegated Node. All other Delegated Nodes on the network will then vote on the proposal. Any proposal that receives 50% + 1 votes within 24 hours of submission will be executed.

Transaction Capabilities

The Bit Protocol is built to be a transactional currency. This means that exchanging money in the form of Swifts needs to be at least as convenient and safe as traditional banking systems. Four main factors have been focused on that will allow transferring Bits to be as simple as clicking a button or swiping a credit card.

Transaction Per Second

Due to the controlled nature of the Delegated Node network, nodes can work to forge blocks extremely fast with a targeted time of three seconds per block. Other algorithms that have implemented proof-of-stake algorithms (such as EOS--which has the same functionality of having selected speaker nodes that forge blocks have proven that it's possible to scale such a system to 50,000 transactions per second. For comparison, Visa is able to scale to 24,000 TPS

Low Transaction Fees

Transactions have no inherent cost on SwiftDemand, however Identity Providers have the ability to set transaction fees--allowing them to have funds to resolve transaction disputes. The Bit Protocol reserves 80% of each block to be used exclusively by Identity Providers. The space is further partitioned by Identity Provider--proportional to the number of Bit Citizens each has verified with a minimum of 10 transactions per block. It's therefore the responsibility of Identity Providers to ensure that spam transactions are not added to the chain. The remaining 20% of each block will be open for transactions with a bidding system--in a similar manner to how Bitcoin functions.

Buyer / Seller Protections

Transactions are able to be signed either by a Nit Citizen's private key or the private key of an Identity Provider. This gives Identity Providers the ability to reverse transactions. Non-authorized transactions should only be used to settle disputes between buyer and sellers on the platform. When reversing funds is not possible, Identity Providers have the responsibility to use the money earned from transaction fees to settle any issues.

Transaction Latency

A single confirmation of a transaction will usually occur within three seconds after publishing a transaction. Normal transactions should be signed by Identity Providers on behalf of a Bit Citizen when the citizen initiates an action. Therefore, any transaction signed by an Identity Provider has a high level of trust--as an Identity Provider is very unlikely to attempt a double-spend attack and can be trusted after a single confirmation. Transactions signed by individual citizens should wait for multiple transactions before being treated as final; this follows the same logic laid out in Bitcoin's Whitepaper.

Compensation

Compensation for Delegated Nodes and Identity Providers are a core part of the Bit Protocol. This compensation is used to heavily disincentivize bad behavior as these bad actions would result in heavy financial losses. Compensation also has the added benefit of making sure that the entire economy can continue to run smoothly for an indefinite period of time as funds will never be depleted.

Both Delegated Nodes and Identity Providers receive a salary in Bits for their service. Salary will be paid out on a daily basis at the same time Bit Citizens receive their daily income. The Swifts generated will initially be drawn from the 70% pool dedicated to regular Bit distribution. Once that pool has been fully distributed, Bits for salaries will be created in addition to the Stage Two inflation distribution.

Delegated Node Salary

Delegated Nodes will each receive an equal salary. The Delegated Nodes themselves will vote on their own salary--with the constraint that the salary must stay within a certain percentage of the previous salary. In the event that Delegated Nodes attempt to abuse this power, it's the responsibility of Bit Citizens to vote out the nodes.

Identity Provider Salary

The Salary Multiplier for Identity Providers is decided by the Delegated Nodes. An Identity Provider's salary is determined by multiplying the number of Bits that have been claimed by Citizens under that specific Identity Provider by the Salary Multiplier. For example, if the Salary Multiplier is 0.01 and the Identity Provider has 100,000 active validated citizens that claimed 5,000,000 Bits during that day, the Identity Provider will receive 50,000 Bitts at the first block after midnight UTC.

Reserved Funds

30 Billion Swifts will be reserved; these Bits are not controlled by any central source. Delegated Nodes have the ability to award these funds to proposals with a majority vote. It's the responsibility of the Delegated Nodes to assign these funds on an as-needed basis to Identity Providers, Delegated Nodes, Bits Citizens, or Bit Entities in an effort to further the success of the Bit Protocol.

Funding Proposal

When a Bit Citizen or Identity Provider requires funds to perform some task, they must submit a public funding proposal. This proposal will be written in plain text, signed

with the requester's private key and then added to the blockchain. Nodes will then have one week to vote on the proposal. Non-votes are counted as "No"s. A majority consensus is required for the funds to be transferred.

Consensus Protocol

A new consensus mechanism is used in the Bit Protocol that allows for extremely fast block times while still being trustable. The Bit Protocol uses a new consensus mechanism called DPOI (delegated Proof of Identity). The mechanism works almost identically to DPOS (delegated Proof of Stake). The primary difference is that in DPOS people have a say proportional to the amount of stake they own in the currency. In DPOI, each Swift Citizen has the ability to cast a single vote regardless of the stake they own.

Consensus

Consensus is decided by following the longest chain. Delegated Nodes that attempt to perform a double-spend attack by signing multiple blocks will promptly be banned by other Delegated Nodes.

Protection

Due to the decentralized government system implemented by the Bit Protocol, there are potential attack vectors that should be carefully analyzed. These attacks have been outlined along with their potential impact and preventative measures.

Skip Attack

If nodes are in the order <Bad Node> <Good Node> <Bad Node>, then the two bad nodes can collide to skip over the good node. When it's the first bad node's turn to create a block, it can create a block immediately, and only broadcast to the next bad node in the list. The second bad node can then wait ten seconds, sign the node, and then broadcast it normally. The chain with the two bad nodes will be accepted since it's longer. While this attack is normally harmless, it does allow colluding bad nodes to take control of the network with only 25% +1 of the nodes if the nodes happen to be optimally placed.

Incubation Period

All new Bit Citizens that join the Swift Protocol will be placed into an incubation period of one week. This prevents an Identity Provider from creating fake Bit Citizens to quickly create Bitts for themselves--and gives Delegated Nodes sufficient time to ban the offending Identity Provider.

Sybil Attacks

Identity Providers are disincentivized from performing Sybil attacks as it comes with the risk of getting banned from the platform by Delegated Nodes. Additional safeguards such as the incubation period and the blockchain rollback capability of Delegated Nodes also exist to help mitigate any abuse. Bits Citizens can attempt to submit fake documents to gain additional basic income, however they are disincentivized from doing so since being caught would result in losing both sources of income. It's expected that a few fake accounts may be created, but Identity Providers will be required to have very strict levels of regulation on how they approve new Bit Citizens, which should eliminate most abuse.

Round Robin Order Attacks

A group of colluding bad actors could collude to all try to receive a similar number of votes, allowing them to be placed in similar locations within the round-robin ordering. (See Selecting Forgers.) A double-spend attack could then be completed with only a handful of bad nodes. This attack, however, can only occur once before being detected. Large transactions should wait for a sufficient amount of confirmations to combat this. Small transactions should be insured by Identity Providers.

Deactivation of an Identity Provider

In the event that an Identity Provider attempts to perform fraud, they can be banned by Delegated Nodes. In the event that damage has already been caused by the action of the Identity Provider, Delegated Nodes can vote to revert the chain to a previous state with an Identity Provider banned. This will cause a large amount of economic damage, but is meant as a last resort to enable the Bit Protocol to not be devastated by an attack and to disincentivize Identity Providers from acting poorly. Bit Citizen accounts that belong to that Identity Provider would consequently be orphaned until they were claimed and validated by another Identity Provider.

Connection To Basic Income Token

The Bit Protocol is simply the protocol that has been outlined above. Basic Income Token will be the initial Identity Provider on the Bit Protocol and all Bits that exist on

Basic Income Token at the time of launching the Bit Mainnet will be transferred at a 1:1 ratio. Bits Citizens will be required to undergo stricter Identity Verification requirements at this time to comply with KYC and AML.

Basic Income Token Features

Basic Income Token is designed to be an extremely user-friendly platform that requires no prior knowledge of cryptocurrency--setting the standard for future Identity Providers. Basic Income Token provides an API as well as a marketplace to make it as easy as possible to transfer Bits for goods and services.