Abstract

The Ethereum Network has proven itself as the world's first ecosystem for permissionless, transparent and immutable software applications. These software applications, typically taking the form of Smart Contracts, can all seamlessly interact with each other. To facilitate this process, various standard protocols have been developed such as the ERC20 standard for a common 'token' format so that these Smart Contracts can pass scarce, owned, and transferable data between one another without a centralized mediator. Up until 2018, every ERC20 token has been distributed in a matter that is generally known to align with 'securities.' The tokens are sold to 'investors' by the 'creator' under the pretenses that the 'creator' will perform some action to make the tokens more valuable. It should be clarified that Bitcoin is distributed via 'bitcoin mining' and therefore aligns itself as a 'commodity' and not a 'security.' This whitepaper will describe the first ERC20 token that aligns itself as a 'commodity' since it is distributed only using 'Proof of Work Mining' identical to the Bitcoin model. This token is also transferred on a blockchain in a method very similar to Bitcoin and so therefore interfaces with other software and with the world in a manner which is effectively identical to Bitcoin. This token has several advances that set it apart from Bitcoin such as the ability to directly interact with Ethereum Smart Contracts and the rest of the Ethereum Ecosytem in a permissionless way.

Background

Yew is the implementation of Solidity and is the first decentralized ERC20 token for Yew Ethereum Revolution. It is an open source community project, not led by an official team or corporation, and therefore does not have ICO capital or other vast amounts of currency/capital that a centralized token project would have. We believe as a community that decentralization is the true flavor of the blockchain and that is the architecture that

provides open and transparent trust for users. We also believe that Ethereum and ERC20 tokens are a significant segment of the future of blockchain technology.
(YEW) token is designed to be used as a decentralized ‘bitcoin-like’ token within the Ethereum ecosystem and beyond. It avoids problems related to centralization and security because it is powered by the Ethereum Network and by globally distributed anonymous miners. Since it follows a standard protocol (ERC20), it is stored in a traditional Ethereum wallet and it is transferred using standard software which supports EIP20/ERC20 tokens. Since every (YEW) token has been mined in a completely decentralized manner, there is no central body or central organization which controls or enforces any aspect of (YEW). The community owns and operates the token in a flat structure and every individual has the same power over the smart contract as any other individual. This is on purpose in order to follow the same model of Bitcoin and to establish (YEW) as a commodity. One of the most effective side effects of Satoshi Nakamoto's desire to secure the original Bitcoin network with Proof of Work hash mining was tethering and bootstrapping the coin to computing power, thereby removing centralized actor jurisdiction. Transitioning the responsibility of work back onto individual miners, government organizations would have no jurisdiction, and indeed visibility, of mined (YEW). Government oversight is removed from an equation whereby miners are providing economic effort in direct exchange of a cryptographic commodity. This facilitates relatively decentralized distribution and establishes all involved parties as stakeholders. (YEW) is a first in class token that allows projects to be funded not by centralized, direct-fiat conversion, but through decentralized computing power.

Name Origin of (YEW)

The name (YEW) is derived from a combination of sports and a sound that’s easy to say. (YEW) has a slogan “IN SPIRIT WE

RIDE”. Made by Jacob. The (YEW) contract is located at Ethereum address 0x0a0624d95020fa8a0c11ec83e14f1e51cea0fa4a and has validated transparent code which can be audited on the Etherscan service.

Ethereum and ICOs

The Ethereum blockchain in its current state exists as a thriving permissionless ecosystem which allows any individual to store immutable records in a permissionless, invulnerable and transparent manner. There is no other database system in the world that has this ability except for Ethereum and other similar blockchains. As blockchain applications become richer and more numerous, there is a need for alternative distribution models than the ICO. Indeed, there have been proposals to mitigate some initial investment risks through the recent introduction of the DAICO model (Cunningham, 2018) that rely on timed and automated value transfers via the DIACO smart contract tapping mechanism. However, this does not align a token smart contract as a non-security and still has the potential to put investors at risk if not implemented carefully. Allowing users of the network direct access to tokens by performing computations as a proof of work supplies allows any smart contract to distribute a token in a safe, slow, and controlled manner similar to the release of a new commodity.

As of 2017, all Ethereum token distribution methods were flawed and able to be Sybil attacked. A Sybil attack is a form of computer security attack in which one human pretends to be many humans with multiple computer accounts in order to manipulate a system in a malicious way. ICOs and airdrops are highly susceptible to Sybil Attacks and since there is no way to verify that all ERC20 tokens distributed by the deployer distributed fairly or unfairly. (YEW), with its unique Proof of Work distribution method, is resistant to Sybil attacks. This means that (YEW) is the chief trustless Ethereum token in the world. It can be argued that the distribution of (YEW) is fair since it was only distributed by mathematical hashing and not by a human.

Current and Proposed Use Cases

As an implementation of the original Bitcoin software as an Ethereum Smart Contract, yew (or YEW) combines advantages from Ethereum. The asset is decentralized, permissionless, mined and scarce just like Bitcoin which means it shares all of Bitcoin's usecases and properties as a transparent and permanent digital record of value. However, above Bitcoin, (YEW) has the speed and scalability of the Ethereum network and is compatible with all ERC20 token services. This means it can be stored in any Ethereum wallet, is as secure as Ethereum, and can act as 'the bitcoin' for the Ethereum ecosystem. This is important because Bitcoin is not able to communicate with or interact with the Ethereum smart contract ecosystem. With (YEW), the Ethereum network is now effectively upgraded with the ability to interface with a commodity which shares all of the same properties as Bitcoin. Now, all Ethereum smart contracts can hold, transfer, and trade YEW-like tokens permissionlessly and can do so based on immutable rules set forth using their own computer code.

To elaborate, the commodity Ether is being used for many purposes within the Ethereum network. The ultimate usability of Ether as a decentralized store of value is unknown. This is because Ether is designed as a medium for securing the Ethereum network and not only as a form of 'bitcoin' for Ethereum. For example, if Proof of Stake is implemented for Ethereum, Ether will no longer be mined using Proof of Work. This will likely leave (YEW) as the only mined asset on Ethereum. In this way and others, Ether may be transformed in such a manner as to make it best for securing the network and not as a good medium of exchange. This message has already been implied by the Ethereum development team in 2017. (YEW) intends to help fulfill a role that Ether currently plays in the

Ethereum network. (YEW) intends to be the primary medium of exchange and store of value for the Ethereum network. This will allow Ether to fulfill its original intended function to secure the network at scale and to be the lifeblood of the Ethereum network.

The Decentralized Token

Since (YEW) is mined like Bitcoin, it acts just like a commodity. The difficulty of 'mining' this commodity automatically adjusts to the total computational power used to mine it. The current state of the Ethereum ICO market with its demonstrable failure rate leaves investors vulnerable to holding pseudo-value backed only by speculation. (YEW) mitigates this problem by providing the Ethereum network with a decentralized bitcoin-like asset which is able to fill the role of a multitude of centralized tokens in a more invulnerable and trustless format.

This powerful mechanism frees individuals from having to use a third party exchange, susceptible to security holes and wallet compromise, and third party escrows. The movement away from centralization is a core tenant of what Satoshi Nakamoto originally intended with classic Bitcoin (Nakamoto, 2009). (YEW) has the facilities to help keep the Ethereum ecosystem open, accountable, trustless and decentralized at every step in the value transfer process. Unlike Bitcoin, (YEW) can interact decentralzied exchanges such as EtherDelta and ForkDelta since it is compatible with Ethereum smart contracts. This means that while Bitcoin can only be traded using centralized means, (YEW) can be traded permissionlessly within immutable permanent smart contracts which are not able to be censored or restricted by central entities. This is another clear advantage and is closer to fulfilling Satoshi's complete vision.

Account System

As an ERC20 token, (YEW) uses a traditional Ethereum account. These accounts are free and are impossible to hack or to steal from, given that the private key has not been exposed. (YEW) can be stored in a Ledger Nano, Trezor or any other wallet that supports ERC20 tokens.

Mining

There have been mintable or mined tokens proposed for Ethereum in the past but none of them have ever successfully implemented Proof of Work or automated difficulty adjustment and so never became pure decentralized currencies. (YEW) is mined using a simple Keccak256 (Sha3) algorithm using the following methodology:

```
   keccak256(nonce, minerEthAddress, challengeNumber) <
difficultyTarget
```

The nonce is a random number selected by the mining software. The mining software mines to try to find a valid nonce. If the above statement evalutates to true, then the nonce is a valid solution to the proof of work. The challengeNumber is just a recent Ethereum block hash. Every round, the challengeNumber updates to the most recent Ethereum block hash so future works cannot be mined in the past. The miner's Ethereum Address is part of the hashed solution so that when a nonce solution is found, it is only valid for that particular miner and man in the middle attacks cannot occur. This also enables pool mining. The difficulty target becomes smaller and smaller automatically as more hashpower is added to the network.

Pool Mining

When mining (YEW), whenever a miner submits a solution, the miner must pay a small gas fee in order to execute the Ethereum smart contract code for the mint() function. If the gas fee is too low, the solution will take too long to be mined and if difficulty is not at equillibrium then another mint() solution from another miner will likely be mined first. This renders the original miners solution invalid and the transaction will revert(). To alleviate gas fees for miners, they can instead mine into a pool. This way, the pool will then submit the solutions to the smart contract and pay a gas fee. Then the pool will typically take a small percent of the rewards and give the rest to the miner for providing the PoW solution.

Since the miner's ethereum address is included in the proof of work, pools require that miners mine using the pool's ethereum address. This way, the miner cannot submit full solutions to the contract while only giving partial solutions to the pool. If the miner is mining on behalf of the pool (using the pools address in the PoW algorithm) then it will not be able to submit any of those solutions to the smart contract without a revert(). This allows pools to operate without being cheated by the miners.

Typically, a pool will accept 'partial solutions' from miners which means the miners will receive 'shares' from the pool for solutions that are close to valid but not quite valid. This follows the same methodology as Bitcoin and Ethereum Proof of Work pool mining. Probability theory states that, given enough close solutions, a full solution will eventually be found.

Smart Contract

Typically, ERC20 tokens will grant all tokens to the owner or will have an ICO which demands that amounts of Ether be sent to the owner for an initial offering of tokens. Instead of granting tokens to the 'contract owner', all 0xBitcoin tokens are locked within the smart contract initially. These tokens are dispensed, 50 at a time, by calling the function 'mint' and using Proof of Work, similar to mining bitcoin classic.