0xVRF

0xVerify: A Faucet Distributed Ethereum Token

Abstract

A major factor in the value of a cryptocurrency is the breadth of its adoption. Too many coins in too few hands create a sense of uncertainty and risk, as the major holders may choose to exit at any time. The true potential value of the token is constrained by a catch-22; value depends on users, but users want to see value before accepting risk.

Attempts at creating a store-of-value, transaction friendly Ethereum token have seen some success in the form of proof-of-work systems like 0xBTC. The ability of crypto-mining based systems to create a wide distribution is limited, however, since access to mining hardware and cheap electricity is relatively centralized. 0xVRF takes decentralization one step farther with the power of the Eth Verify system, allowing all new tokens to be issued to individual people, at no cost and no risk to them.

Introduction and overview of related technologies

0xVerify (0xVRF) is an ERC-20 compliant token on the Ethereum blockchain, similar to many other popular cryptocurrencies. Unlike many of these, 0xVRF is not distributed via an ICO where they are initially sold to the public. Instead, 0xVRF tokens are issued in a manner similar to a ‘faucet’, daily, for free, to valid holders of Eth Verify accounts who send a transaction to the contract. In a similar manner to proof-of-work tokens, this regular distribution is automatically balanced to achieve a targeted average rate of token creation, ensuring a predictable supply and tightly constrained rate of inflation. That is, the more people collecting 0xVRF tokens daily, the fewer tokens will be issued to each individual.

Eth Verify is a service offering free on-chain verification of Ethereum accounts, conferring security against ‘bots’ which utilize hundreds or thousands of accounts to exploit smart contracts. Eth Verify and 0xVRF are made by the same team and are symbiotically connected in several ways:

- Eth Verify prevents mass abuse of 0xVRF, so free tokens go to real users and not to bot operators

- 0xVRF distribution and exchange rate determine the cost for instant registration of Eth Verify accounts
- Eth Verify (optional) registration fees are sent to a 0xVRF exchange contract, directly increasing the value of the token
- As the first decentralized application built using the Eth Verify service, 0xVRF will serve as proof of the effectiveness of Eth Verify by demonstrating resistance to automated attacks in spite of a clear incentive to carry out those attacks.

0xVRF uses a custom token exchange contract to provide an initial, convenient means for users to trade the asset before it is represented on crypto exchanges. This contract is modeled after popular ‘farm’ DApps, and works by holding both Ethereum and tokens, and allowing users to trade one for the other directly, at a rate based on the proportionate balance of each that the contract contains. As mentioned above, the use of this contract also allows for a tighter integration with Eth Verify and a way of directly increasing value for token holders by injecting registration revenue directly into the contract.

Eth Verify enables smart contracts to do things previously infeasible, the clearest use case being to offer something of value for free and know it is going to real users. 0xVRF uses this capability to create a cryptocurrency with a distribution more inherently even than any other coin available. Not only does it derive value from this evenness and its tightly constrained supply growth, but also directly from Eth Verify itself.

Technical outline of the Eth Verify service

Possibly the single biggest limitation facing decentralized applications today is the need to design around the assumption that a single user can create unlimited accounts, and that you do not know whether one thousand Ethereum addresses represent one thousand people or just one. For this reason, crypto games and other systems must carefully limit themselves, lest all value be siphoned away by mass account creators. Eth Verify represents a direct, practical solution to this problem, in the form of what is essentially an address verification oracle. Users sign up off-chain, checks are completed to determine that their registrations are legitimate, and their Ethereum addresses are added to the smart contract. Many users are pre-verified and do not need to sign up, as the system crawls popular contracts and adds addresses that clearly represent legitimate users, accelerating the formation of a network effect and increasing convenience. Other

smart contracts can then query this contract to verify whether a particular address has been vetted by the system.

There are two basic ways to become verified: direct, and free. The process starts with the user completing a captcha and submitting some basic information. Once email verification is complete and the system has acquired all the information it can, the user may wait for the manual verification process to decide whether to verify their address, or send a transaction and pay a fee to register their account instantly. This fee is dynamically adjusted using 0xVRF, with the goal of ensuring that the fee is always higher than the profit that may be immediately extracted from a single verified account. It is determined by the following algorithm:

```
final_cost=base_cost
dynamic_cost=VRF_EXCHANGE.calculateTokenSell(VRF.PER_USER_ISSUANCE))
while(final_cost<2*dynamic_cost):
     final_cost=final_cost*2
return final_cost
```

Where PER_USER_ISSUANCE is the number of tokens a user may claim on the given day, calculateTokenSell is how much Eth those tokens will sell for on the exchange, and base_cost is a fixed value (0.02 Eth at time of writing). This algorithm ensures that it will always cost more to directly verify your account than you can directly obtain with that account on a given day, in terms of 0xVRF tokens. Doubling of values is used rather than a continuous value in order to avoid failing transactions due to fluctuations. As the value of 0xVRF is expected to scale with adoption of Eth Verify, this should serve as a roughly accurate measure of the general value of a verified address.

Following the initial signup, a user's application and the information therein will be reviewed by a regularly scheduled procedure. This system is the heart of Eth Verify, and its design and construction represent the bulk of the effort put into the project as a whole. The details of this procedure are largely confidential. While security by obscurity is often rightly criticized, in systems designed to filter real users from automated processes, it is an unavoidable necessity, and so a strategy founded in uncertainty and concealment of information has become the standard approach to this problem in many industries. The difference between a bot and a real user is subjective; perhaps you can know that a program cannot solve your captcha, but a program could have called on the assistance of a real person solving captchas for a fee. You can know that an IP address originated from

a particular country, but it is difficult to know for sure if that country is the true origin of the traffic. For any precise programmatic definition of a real user, there exists a specific cost at which a perfect counterfeit of a user may be created, and increasing this cost often also increases the barrier to entry for real users. The goal of bot prevention is twofold; increase the effective cost to botters beyond the point of viability, while minimizing the cost to real users. In service of this soft war of attrition, there is great value in concealing your true programmatic definition of a user, and therefore, for Eth Verify, its definition will not be made available to the public, and practical evidence alone must serve to prove its effectiveness.

At the conclusion of the application review process, the system will have made a decision as to which accounts are legitimate and which are not. If an illegitimate account has not paid for registration, no action will be taken. If an illegitimate account has paid and is already registered, it will be deregistered. The converse is true for legitimate accounts; if they paid for verification no action is taken, if they did not the system verifies them on-chain. Once registered you are free to make full use of any DApp that uses Eth Verify.

In terms of how a smart contract may use Eth Verify, it is very straightforward to integrate. See the following example, in which the highlighted lines of code can be copied verbatim in any contract for the same results:

```
pragma solidity ^0.4.18;

contract EthVerifyCore{
  mapping (address => bool) public verifiedUsers;
}
contract FreeNapkins{
  mapping (address => uint256) public napkinCount;
  EthVerifyCore public
ethVerify=EthVerifyCore(0x1ea6fad76886fe0c0bf8ebb3f51678b33d24186c);

  function getFreeNapkins() public{
    //causes transaction to be reverted if user is not verified.
Ensures fair napkin distribution.
    require(ethVerify.verifiedUsers(msg.sender));
    //50 napkin limit per user
    require(napkinCount[msg.sender]<=50);
    //give user 10 free free napkins
    napkinCount[msg.sender]+=10;
  }
}
```

By using the line `require(ethVerify.verifiedUsers(msg.sender));` a function will fail to execute if called by an unverified user. In a similar manner, 0xVRF uses Eth Verify to cause its token issuance function to only succeed when called by verified users.

Eth Verify has potential uses that go beyond the prevention of mass account spam. A very common trend in smart contracts today is to use codesize and transaction origin checks to prevent other contracts from having access. Without these checks, a decentralized application becomes much more vulnerable to attacks that can be very unintuitive and difficult to plan for. There are plans for an upcoming Ethereum update to remove the effectiveness of transaction origin checks, and codesize checks have proven to be flawed. But by conducting checks ahead of time, Eth Verify can ensure that all verified addresses represent wallets and not contracts, providing a simple, enduring method of protecting against contract based exploits.

Issuance and Inflation

0xVRF tokens are issued directly to users on a daily basis. If you have already claimed tokens on the same day, you may not claim more. Once the next day (as defined by an arbitrary point of time in the contract) arrives, everyone can once again claim tokens. Like many cryptocurrencies, there are built in limits on how many coins can be created. The number of tokens a user can claim each day is determined by the following formula:

$$\frac{10{,}000{,}000}{USER\,CLAIMS\,YESTERDAY}$$

That is, the number of tokens you can claim depends on how many people claimed tokens the previous day. So for example, if 1000 people claimed tokens on the previous day, today you can claim 10,000 VRF. If 100 people claimed tokens, today you can claim 100,000 VRF. Notice that this formula does not guarantee that ten million tokens will be distributed daily. For example if the first day only ten people claim tokens, the second day everyone can claim 1,000,000 each, and if 50 people claim tokens this results in a daily total issuance of 50,000,000. However if on the third day there are only 30 claims, only 6,000,000 tokens will be issued in total. The ultimate result will be that, once the user base reaches a peak, the number of tokens issued daily will average out to the target number of ten million. Since the tokens are issued at a roughly constant rate, the total supply growth

will decrease percentage-wise. Proportionally growth is fast at first and eventually tapers off.

Naturally, this issuance mechanism depends on the effectiveness of the Eth Verify system; it cannot be possible to generate unlimited verified addresses, or all value of the coin could be rapidly inflated away by automated adversaries. This is by design. While 0xVRF is an innovative new store of value in its own right, its primary purpose is to instill confidence in the platform on which it is built. It will do this by presenting an attractive target for attack, and by proving highly resistant to those attacks. In this way it will further propagate its own value, given the close connections it has with Eth Verify.

Exchange Contract

Released simultaneously with the 0xVRF token is an exchange contract that can be used to trade between VRF and Eth. This serves three main purposes:

1. As a stopgap measure to allow trading before the coin has achieved much volume on traditional exchanges.
2. As a way to inject value directly into the token.
3. As a way for Eth Verify to use the value of the token to increase the security of the registration price algorithm.

The exchange uses the same algorithm as many popular ‘farm’ games such as Ether Shrimp Farm. Unlike a normal cryptocurrency exchange, it has no order book. Instead, it holds both assets, and offers the ability to either:

- Exchange VRF → ETH
- Exchange ETH → VRF

It does this on a basis of how much of both assets it currently holds, and how much you want to trade. Because the rate of exchange gets worse the more of one asset enters the contract, you might think that it could be somewhat exploited by trading large amounts, but the algorithm accounts for this, giving you a different rate depending on the volume you are trading. The formula for purchasing VRF with Eth is as follows:

$$\frac{VRF\ SUPPLY}{1/2 + \frac{ETH\ SUPPLY + \frac{ETH\ TRADED}{2}}{ETH\ TRADED}}$$

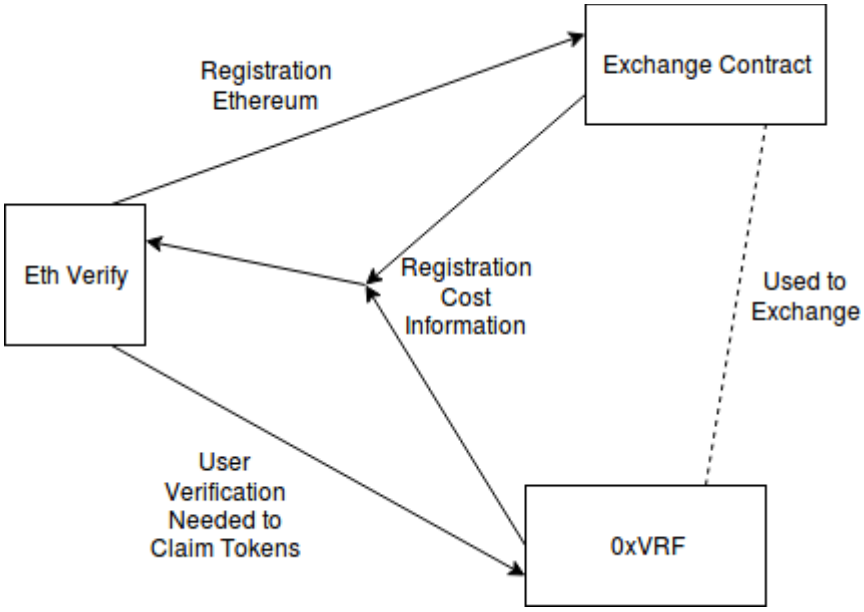
With the result being the number of tokens you will receive for the amount of Ethereum you have spent. To trade in the other direction, the formula is the same, but with the values swapped.

Since the rate of exchange depends on the values already in its contract, there need to be starting values, and this happens in the form of seeding the market with both VRF and Eth. For this reason, the 0xVRF contract will initially generate a few days worth of tokens, most of which will be put into the exchange contract, along with a sum of Eth. While Ethereum can be directly put into the contract, the exchange is verifiably trustless; there is no way for anyone to access the funds without trading for them like everyone else.

The value of VRF in the contract is increased by more Eth being added to it. Therefore, by directing Eth Verify registration fees to the exchange, the value of the token will be increased. As the value fluctuates, both per token and per-day, the cost of immediate verification may also fluctuate; ideally making registration easier while the project is smaller, and more difficult as it becomes progressively more desirable to have access to production of VRF. From a user experience and convenience perspective especially, the exchange will enhance the token by enabling single transaction, zero fee trades that can be carried out directly from the website.

0xVRF contract ecosystem

0xVRF is a separate entity from the Eth Verify service and the VRF exchange contract, but all of these systems interact with and benefit each other. Eth Verify provides the user verification that allows the 0xVRF faucet issuance mechanism to function, and distributes revenue from signups directly to the exchange contract, boosting the token’s value. 0xVRF and the exchange contract together provide pricing information to Eth Verify that is used to set the instant registration cost to a safe level. The exchange contract holds 0xVRF tokens and can be used to trade them.



The combination of these systems results in a cryptocurrency with a highly decentralized distribution, and therefore a clear path to network growth and increasing value.