Ethbet Whitepaper

Version 1.0 – draft, June 2017

Table of Contents

Abstract

Ethbet is a decentralized and provably-fair Ethereum-based dicing game without a mandatory house edge. Ethbet is able to offer bets without a house edge because players bet directly against other players instead of against a centralized house. The disadvantage of this is that in order to place a bet, there must be another party willing to place the same bet. For this reason it is possible that a player must wait for their desired bet to take place, especially if it is very large. To combat this, an additional feature of an optional player-defined house edge is added, allowing players to offer and take (or 'call') bets with any house edge that they desire. Thus, a player that prioritizes speed over their expected return can agree to a bet that gives him a slight disadvantage (i.e., a bet that gives his opponent a small house edge). Similarly, a player that is patient and prioritizes their expected return can offer bets that the formerly mentioned player may choose to call. This results in a model where players are effectively able to become their own 'casinos', allowing market forces to provide players with bets as quickly as possible at the best possible rates.

Gambling Without a House Edge

A house edge is a statistical bias in favor of the house, so that the house has a slight advantage in every bet. House edges of various games found in physical casinos often range from 2% to 15%, with some games having a low house edge (such as craps) and other games having a higher house edge (such as slot machines). With the advent of online gambling using cryptocurrencies, various websites offer players relatively lower house edges, such as 1%. Although 1% sounds like a low house edge, one must keep in mind that this house edge is applied to every individual bet. Thus, if a player only places one bet, they are expected to lose 1% of it, on average. But it's likely that most players will want to bet more than just once. If a player places 100 bets, they are expected to lose 1% of each of those 100 bets, making it increasingly difficult for the player to turn a profit, inevitably leading to gambler's ruin (the player running out of funds). This is how dice sites are able to consistently generate steady streams of profit for the owners and investors – they slowly but surely make sure that the more people play, the more likely they are to lose all of their money to the house.

Betting without a house edge saves players much more than a trivial amount. Because a player's expected loss can be zero for every bet they make, they can now make hundreds or thousands of bets without statistically being likely to lose more and more of their money over time. With a house edge of 0%, a player's probability of gaining capital is equal to their probability of losing it – they are no longer making an inherently irrational decision with a negative expected gain.

Provable Fairness

Most modern cryptocurrency dicing sites offer provably-fair betting. This is done by having a client seed and a server seed. The client seed is picked by the client, often generated randomly by default. The server seed is picked by the server. The server then hashes its server seed using a secure cryptographic hash function (such as a sha2 or sha3 function) and provides the hash to the client before their roll. Then the client submits their client seed and bet information to the server, and the server combines both seeds, using a public algorithm to generate a random number. After the roll has been made, the client is able to view the server seed that was used, and can confirm that the server did not modify the client seed, the server seed, and therefore also the result of the roll. This results in a roll that is mathematically impossible to bias or otherwise predict by either party, given basic assumptions including that the client does not use a predictable seed, and the hash function used is secure. Although this model of provable fairness is suitable for a client-server model, it cannot be performed in a smart contract, as the blockchain is public information and no unbiased source of entropy exists.

Most solutions put fourth to securely generate a random number on the Ethereum blockchain pose significant downsides, as there are too many actors that are able to influence the blockchain when money is at stake. For example, if the hash of the next Ethereum block was used as a source of randomness, then a miner can choose to modify a block before they publish it, or can decide against publishing a block altogether, depending on if it is favorable to them. Given that there have already been notable instances of miners acting selfishly in a way that hurts other users, this is not an acceptable solution.

RANDAO[1] attempts to solve the problem of untrustable miners by effectively crowd-sourcing entropy. Anyone who wants to participate in RANDAO may contribute to its pool of entropy, and is incentivized to do so as they are paid a small reward, which RANDAO in turn collects from those that call its contract. It would take every participant to collude with one another in order to manipulate the result[2]. Unfortunately it takes a wait time of several blocks for RANDAO to be statistically confident that a miner has not manipulated its pool of entropy. RANDAO is also limited in the amount of entropy that it can provide per unit of time, and potentially per unit of ether.

One solution which is used by Etheroll[3] and others is to use Oraclize[4] and random.org[5] to generate a random number. Oraclize is a service that fetches external (outside of the blockchain) data for use on the blockchain. Oraclize makes a call to random.org, returning the integer roll from random.org, the id associated with it, and a TLSNotary proof[6], showing that Oraclize did not modify the result. As the id associated with the bet (returned from random.org) is supplied as well, it can be shown that Oraclize only made one call to random.org for every call it was requested to make.. This solution has two downsides, the first being that it introduces a liability of depending on Oraclize, which is not desired. The second is that random.org must be trusted to provide a secure random number. This solution is currently implemented in at least one decentralized dice game due to the lack of appealing and efficient

alternatives. Performing statistical analysis on the results that have been returned from Oraclize via random.org, it appears that this solution has thus far succeeded (with high probability) in its goal of providing a source of entropy that is unbiased.

An additional solution, more appealing than the previous, is currently being tested by Oraclize[7]. This solution involves a hardware random data source that is integrated with the Ethereum network. The random bytes generated by the data source are periodically published onto the Ethereum network along with a proof that they have not been modified. Although fully functional, it is currently only available on the testnet. When available on the mainnet, this will likely become the best option to use for Ethbet's source of randomness. Until that period, the aforementioned solution that has an additional liability of random.org is scheduled to be used for Ethbet.

The Optional Player-Defined House Edge

Placing bets with a house edge of 0% does not come without a disadvantage, i.e., a bet can only take place if there are two parties that wish to make it. As bets are significantly more advantageous for players when made with a 0% (or otherwise negligible) house edge, network effects may cause the majority of players to use Ethbet, as it will be more profitable than other betting alternatives. Even with this, however, it may be possible that players are not content with the amount of time they have to wait between bets, especially for larger bets, which fewer players are willing to call. To solve this problem, an optional feature is added: allow players to offer and call bets with a player-defined house edge.

With the ability for players to offer and call bets with an arbitrary player-defined house edge, the problem of large wait times for bets can now be solved with negligible downsides. Players are effectively able to become their own casinos within Ethbet, setting their own house edge. As every player that offers bets is competing against other players to have their bets taken, they are incentivized to set their house edge as low as possible.

For example, if a player wants to make a very large bet, they may be incentivized to offer a house edge to whoever calls the bet, so that they do not have to wait too long for someone to bet against them. This player decides to prioritize speed over their proportional expected gain.

Similarly, if a player has a large amount of ETH and wishes to make a profit over time with it (with high or variable probability), they can offer bets with a small house edge in their favor, making it easier for others to play the game while giving them a small profit over time for their service.

Profit Model

The profit model of Ethbet has several aspects which generate revenue for token holders:

The Ethbet smart contract will take a small portion of the house edge that is offered by players. This only occurs for bets with a nonzero house edge. As an example, suppose that a player offers a bet of 1 ETH with a house edge of 1% in their favor. This player's expected gain would normally be 0.01 ETH. If the Ethbet smart contract were to take a 10% cut of their expected gain, this would change their expected gain to 0.009 ETH. Thus the player would win a total of 1.009 ETH instead of 1.01 ETH, decreasing their profit by slightly less than 0.1%, or less than 1/1000th. The portion of the house edge that Ethbet takes is decided by token holders.

In addition to this, Ethbet charges a small fee on all bets in order to pay for the gas to execute its smart contract. A portion of this fee that is not used for gas can also be allocated to the holders of Ethbet tokens. The token holders can vote on this value as well.

Although token holders can vote on these values, they are incentivized not to set these values to an unreasonably high percentage, or less users would use Ethbet, and the value of their tokens would decrease.

Market Potential

The global online gambling market is estimated to be worth over $50 billion USD by the end of 2017[8] and is forecast to grow by around 10% for years to come[9]. With the advent of cryptocurrencies allowing players to gamble significantly easier and with a lower house edge than previous options, cryptocurrency gambling has already garnered a significant proportion of this market potential. A 2013 estimate suggests that up to 50-60% of all bitcoin transactions were related to gambling at one point[10]. Although previously dominated by Bitcoin, Ethereum has become a major player within the cryptocurrency world, offering significantly more features as well as a shorter block time and lower transaction fees. As Ethereum gains more users it benefits from network effects, which are currently leading many users to invest in and use Ethereum over Bitcoin, leading its market cap to increase to $38 billion USD in June, 2017[11]. Although it is already possible to gamble using Ethereum, even via a smart contract[12], players are still faced against a house of 1% or more, which is significantly detrimental even to casual players, as mentioned above.

Given that Ethbet will be able to provide the most competitive house edge that the market allows for, there is a strong possibility that it will acquire a significant proportion of the cryptocurrency gambling market share, as there is no reason for a user to gamble against a house edge of 1% or higher when they can instead gamble with house edges significantly lower, possibly zero. Ethbet can allow users to bet

any amount that is technically possible, using any house edge that they desire, potentially deprecating all other forms of gambling for users that wish to maximize their expected value.

Bitcoin dicing sites such as PrimeDice and SatoshiDice (among many others) have reported profits of millions of dollars, with SatoshiDice selling for 126,315 BTC in 2013, which was 'only' $11.47 million USD at the time[13]. Ethbet has significant advantages over these websites, including that it is decentralized, transparent, uses Ether over Bitcoin, and, crucially, provides the lowest possible house edge. For the aforementioned reasons, the market potential of a platform such as Ethbet is extremely large.

Ethbet Tokens (EBET)

For the purposes of decentralization, dividend distribution, further developmental funding, and future endeavors of Ethbet, an Ethbet token (EBET) will be created on top of the Ethereum network. This will be a standard ERC20 token, and thus will be secure, easy to store, use, and trade, as wallets and exchanges already have the needed technical infrastructure to interface with tokens that implement the ERC20 interface. For the technical details of the ERC20 specification, see the EIP on Github[14].

Token holders are eligible not only to receive their proportional share of dividends from the profits that Ethbet creates, but are also eligible to vote on Ethbet Improvement Proposals (Ethbet IPs). An Ethbet IP is a proposed change to Ethbet, such as increasing or decreasing the cut of the house edge that is taken. Rather than having a single entity decide on this proposal, the proposal will be voted on by those who hold Ethbet tokens, with their voting weight being linearly proportional to the amount of tokens that they hold. This way the investors of Ethbet are able to optimize it in the direction that they see most desirable. This feature is not yet implemented, however token holders will be able to vote on changing Ethbet's house edge cut and fee before this feature is further implemented.

Crowdsale

Those wishing to invest in Ethbet via purchasing Ethbet tokens will have the opportunity to do so via the Ethbet crowdsale. The funds received from the crowdsale go to fund the further development of Ethbet, including 3rd party contract security audits and further web/application development. The crowdsale will last for 2 weeks and is set to begin on Aug 27th, 2017, 8:00 PM UTC. All information relevant to the crowdsale is available in the below table.

Ethbet description	Ethbet is a decentralized dicing platform with the

	lowest possible house edge
Token Description	Ethbet tokens give their holders the ability to collect dividends and vote on proposals to improve Ethbet
Ticker Symbol	EBET
Start Date	Aug 27th, 2017, 8:00 PM UTC.
Duration	2 weeks
Token Price	1000 EBET = 1 ETH, 1 EBET = 1 / 1000ETH
Token bonus for first day of crowdsale	+10%, i.e., 1100 EBET = 1 ETH
Percentage of all tokens offered via crowdsale	90%
Total Possible Token Supply	50,000,000
Excess Tokens Deleted?	Yes. No additional tokens ever created.
Token Type	ERC-20-compliant

Project Architecture

The structure of the Ethbet code is intended to be highly modularized, clean, and secure, with the full project functionality being split into several smart contracts based off of the principles of high cohesion and low coupling (where applicable). The contract for the crowdsale is separate from the contract for the token, the contract for the game, and others. All contracts will be audited and tested extensively, ensuring that best practices are followed and no major bugs exist.

The first implementation of the Ethbet dice game will be relatively lightweight and is intended as a fully-functioning proof of concept. There are only three types of calls that can be made into the game contract: place_bet, call_bet, and cancel_bet (that the player previously placed, but that has not been called by another player). A bet is composed of several variables: the bet ID, the address of the player placing or calling, the bet amount, and the house edge.

The ability to decide the probability of winning a given bet (such as the ability of a user to set the ‘roll under’ or ‘role over’ values before their roll) will not be available in the initial version of Ethbet. Instead, the win and loss chance will be set to a static value of 50%. This is done for several reasons:

- The original implementation should be as lightweight as possible to encourage a small codebase and fewer potential bugs.
- The user experience should be as smooth and simple as possible, to decrease the overhead involved when users use the Ethbet platform.

- The market will likely have an easier time providing all types of players with a desirable selection of available bets if all bets have the same risk/reward ratio.
- Users are still able to manage their risk profile in an arbitrary fashion; they must instead make several bets with potentially differing amounts if they desire a certain ratio of risk to reward. In practice this causes the risk and reward ratio to be equivalent to one found in a variable-probability bet[15].

With that said, there is no reason why this feature cannot be implemented in some manner if the token holders are in favor of it.

Off-chain Matchmaking

When information is stored on the blockchain, a fee must be paid (refereed to gas) in order to provide an incentive for miners to include the information in the blocks that they mine. The more information that one wishes to store on the blockchain, the higher the fees will be. As the blockchain is immutable and must be stored by all full nodes, storing information on the blockchain is generally a costly transaction, and should be avoided if possible. The blockchain is secure and decentralized, but at the cost of extreme redundancy. For this reason, the blockchain is only needed when we desire a secure, decentralized, and immutable environment.

Offering and canceling bets on the blockchain is highly inefficient: if a player wishes to offer many bets and then cancel them, they will pay high gas fees to have that information stored on the blockchain forever, even if the bets are never actually executed. A solution to this is to match bets off of the blockchain, and then have players confirm and execute their bets by submitting them via a smart contract.

This is a common system used by decentralized exchanges so that every order placement and cancellation does not need to be stored on the blockchain, and instead the blockchain is only used where its advantages of security and immutability are highly relevant, i.e. for the actual transaction.

One example of an off-chain matchmaking system is used by the decentralized exchange protocol 0x[16], where anyone is able to set up a ‘relay’ that allows for efficient communication of intent between exchange users. Users are incentivized to set up honest relays through a fee structure that allows them to profit off of providing this valuable service. Another example is the decentralized exchange known as EtherDelta[17], which hosts their own service that allows for this.

A system similar to this can be implemented within Ethbet: We can have a service that acts as a relay and functions separate from the blockchain which allows users to signal their intent. After a match can be found between the intent of two users, both users can submit their bet to a smart contract, which ensures that their bet is executed fairly and securely. This matchmaking service can be hosted by anyone as the code will be open-source. An official version of the service will be provided even though there is no obligation to use it or to use a matchmaking service at all.

This system offers a significant number of improvements over a more naive implementation in which all information is exchanged only via the blockchain. Aside from the significant reduction in fees for users, it allows bets to be communicated significantly more quickly and makes it much easier for users to cancel their bets safely. Instead of placing and canceling a bet by broadcasting and storing two pieces of information in the blockchain, a bet can be placed and canceled instantly and with zero fees by signaling intent and then revoking this intent afterwards.

Development Timeline

At the time of the crowdsale, the Ethbet token and Ethbet crowdsale contracts will be deployed on the mainnet and fully functional, as necessary for the crowdsale to occur. The code in these smart contracts is a relatively standard and lightweight implementation of the ERC20 standard, and the possibility for critical bugs is small in comparison to that of more complex and novel contracts, such as the primary Ethbet game contract. If a significant problem occurs that is recoverable, the necessary steps will be taken to remedy the situation. For example, if there was somehow a critical flaw in the Token contract, allowing someone to steal all Ethbet Tokens, we could fix the problem, deploy the new token contract (with the problem fixed), and restore the balances of all users, migrating the entire platform to the newer version of the token, similar to what happened with Ethereum and the DAO. An issue like this is is very unlikely to occur unless it is caused by a problem within Ethereum itself, as the Ethbet Token is nearly isomorphic to most Ethereum (ERC20) tokens, so a critical problem with one could indicate the same problem with many others.

After the crowdsale is complete, Ethbet tokens will become unfrozen and can then be sent to other users. At this time the development of the primary game contract will proceed. This is a relatively lengthy process despite the simplicity of the game architecture. The general timeline is as follows:

1. Develop primary contract functionality and tests
2. Extensively test and audit the contract for potential flaws
3. Deploy the contract onto the testnet
4. Allow users to interact with the contract during a beta period
5. Continue to improve the contract as needed
6. Perform final third-party security audit(s)
7. Deploy the contract onto the mainnet
8. Continue to improve non-contract code, such as improving accessibility and user interfaces, only updating the contract to fix critical issues or to later implement new features.

In order to make interaction with the smart contract user-friendly and simple, users will be able to interact with it via the Mist browser, giving them an experience similar to traditional websites, but while still interfacing only with smart contracts.

Timeline

Q1 2017	Market research, feasibility assessment, other planning– completed
Q2 2017	Website and Whitepaper – completed
Q3 2017	Crowdsale, development, and community building
Q4 2017	Continuation of development and other improvements as desired by token holders
Q1 2018	Playerbase building, community growth, further improvements as needed
Q2 2018+	Additional games, projects, and features, decided by token holders and market demand

Future Possibilities

As Ethereum matures as a technology, it will allow decentralized applications such as Ethbet to run more efficiently. Improvements in other technologies such as Web3 browsers (Mist and the Metamask extension) also help to further Ethbet's goals. As Ethbet progresses as a project, there will be opportunities for more features to be added. Examples include a more feature-rich implementation of dicing, other games such as lotteries, and development of a standalone or mobile app. The inclusion of these features depends on the success of the Ethbet crowdsale as well as the opinions (votes) of the Ethbet token holders.

Disclaimer

There are many risks associated with the Ethbet token, just like with Ethereum.

The entire Ethbet project is dependent on Ethereum; a critical issue in Ethereum could prove significantly detrimental or fatal to Ethbet.

There is no guarantee or expectation that Ethbet tokens purchased will increase in value, provide a return, or will have sufficient adoption and liquidity to enable exchange for other assets.

There is no guarantee that blockchain technology and smart contracts, especially those related to gambling, will remain legal, unregulated, and usable within your legal jurisdiction, even if they presently are.

Owning Ethbet tokens does not constitute a share of, equity of, or ownership of the Ethbet platform.

United States citizens are not allowed to participate in the Ethbet crowdsale. The United States regulatory environment regarding token sales is still evolving, and Ethbet has made the decision to avoid this market to help ensure its success. Do not participate in the Ethbet crowdsale if you are a resident of the United States.

There are many risks, both known and unknown, that are involved with cryptographic assets, including Ethereum and Ethbet tokens. These risks include but are not limited to critical bugs, security flaws, difficulty scaling, denial of service, and the risk of new cryptographic breakthroughs.

This document does not constitute a prospectus of any sort, and is not an Initial Public Offering or Share/Equity offering. The tokens involved with Ethbet do not in any way involve any form of ordinary shares in Ethbet, and no dividends are guaranteed on Ethbet tokens. Fiat currency is not accepted in the Ethbet crowdsale.

Ethereum is an experimental technology and all possible future risks cannot be enumerated here. Ethbet is not responsible or any losses that may occur. Please exercise caution with all cryptographic assets and do not invest money that you cannot afford to lose.

More Information

For more information about Ethbet, or if you have any questions, please visit the Ethbet website[18] at https://ethbet.io/ or send an email to team@ethbet.io.

1 https://github.com/randao/randao

2 https://blog.ethereum.org/2015/08/28/on-anti-pre-revelation-games/

3 http://crowdfund.etheroll.com/etheroll-whitepaper.pdf

4 http://www.oraclize.it/#services

5 https://random.org/

6 http://docs.oraclize.it/#security-deep-dive-authenticity-proofs-tlsnotary-proof

7 https://blog.oraclize.it/the-random-datasource-chapter-2-779946e54f49

8 https://www.statista.com/statistics/270728/market-volume-of-online-gaming-worldwide/

9 http://www.businesswire.com/news/home/20161006005678/en/Global-Online-Gambling-Market-Worth-USD-66.59

10 http://lsvp.com/2013/08/23/at-least-half-of-all-bitcoin-transactions-are-for-online-gambling/

11 https://coinmarketcap.com/currencies/ethereum/

12 https://etheroll.com/ and other forks

13 http://www.coindesk.com/bitcoin-company-acquisitions-begin-gambling-site-satoshidice-sells-for-11-5m-126315-btc/

14 https://github.com/ethereum/EIPs/issues/20

15 For example, instead of a user making a bet with a 25% win chance and a 4X payout, the user can make 2 bets with a 50% win chance and a 2X payout on each, resulting in the same risk to reward ratio. The equivalent can be done for those who wish to risk smaller amounts, as they are able to make bets as small as feasible, dictated by network and gas fees and their preferences.

16 https://0xproject.com/

17 https://etherdelta.github.io/

18 https://ethbet.io/